CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

Référentiel

Centre gouvernemental de cyberdéfense

Oct. 2026

Votre gouvernement

Québec

Table des matières

AC — Gestion des droits d'accès aux systèmes et données

AC-01 — Politique et procédures de contrôle d'accès 37
AC-02 — Gestion des comptes 38
AC-02(01) — Gestion automatisée des comptes système 40
AC-02(02) — Gestion automatisée des comptes temporaires et des comptes d'urgence 41
AC-02(03) — Désactivation des comptes 42
AC-02(04) — Opérations automatisées de vérification 43
AC-02(05) — Fermeture de session en cas d'inactivité 44
AC-02(06) — Gestion dynamique des droits d'accès 45
AC-02(07) — Comptes d'utilisateur privilégiés 46
AC-02(08) — Gestion dynamique des comptes 47
AC-02(09) — Restrictions liées à l'utilisation de comptes partagés et de groupe 48
AC-02(10) — Changement de justificatifs d'identité de comptes partagés et de groupe 49
AC-02(11) — Conditions d'utilisation 50
AC-02(12) — Surveillance des comptes pour utilisation irrégulière 51
AC-02(13) — Désactivation des comptes des personnes à risque élevé 52
AC-03 — Application de l'accès 53
AC-03(01) — Restriction de l'accès aux fonctions privilégiées 54
AC-03(02) — Double autorisation 55
AC-03(03) — Contrôle d'accès obligatoire 56
AC-03(04) — Contrôle d'accès discrétionnaire 57
AC-03(05) — Information pertinente en matière de sécurité 58
AC-03(06) — Protection de l'information du système, des utilisatrices et utilisateurs 59
AC-03(07) — Contrôle d'accès basé sur les rôles 60
AC-03(08) — Révocation des autorisations d'accès 61
AC-03(09) — Diffusion contrôlée 62
AC-03(10) — Dérogation vérifiée aux mécanismes de contrôle d'accès 63
AC-03(11) — Accès restreint à des types d'information spécifiques 64
AC-03(12) — Assurer et appliquer l'accès aux applications 65
AC-03(13) — Contrôle d'accès basé sur les attributs 66
AC-03(14) — Accès individuel 67
AC-03(15) — Contrôle d'accès discrétionnaire et obligatoire 68
AC-04 — Application du contrôle de flux d'information 69
AC-04(01) — Attributs de sécurité et de protection de la vie privée des objets 70
AC-04(02) — Domaines de traitement 71

AC-04(03) — Contrôle dynamique de flux d'information 72
AC-04(04) — Contrôle de flux de l'information chiffrée 73
AC-04(05) — Types de données intégrés 74
AC-04(06) — Métadonnées 75
AC-04(07) — Mécanismes de flux unidirectionnels 76
AC-04(08) — Filtres de stratégie de sécurité et protection de la vie privée 77
AC-04(09) — Vérifications manuelles 78
AC-04(10) — Activer et désactiver les filtres de stratégie de sécurité et de protection de la vie privée 79
AC-04(11) — Configuration des filtres de stratégie de sécurité et de protection de la vie privée 80
AC-04(12) — Identifiants de type de données 81
AC-04(13) — Décomposition en sous-composantes pertinentes 82
AC-04(14) — Contraintes liées aux filtres de stratégie de sécurité ou de protection de la vie privée 83
AC-04(15) — Détection de l'information non autorisée 84
AC-04(16) — Transferts d'information sur des systèmes interconnectés 85
AC-04(17) — Authentification des domaines 86
AC-04(18) — Liaison d'attribut de sécurité 87
AC-04(19) — Validation des métadonnées 88
AC-04(20) — Solutions approuvées 89
AC-04(21) — Séparation physique ou logique des flux d'information 90
AC-04(22) — Accès seulement 91
AC-04(23) — Modifier l'information non communicable 92
AC-04(24) — Format normalisé interne 93
AC-04(25) — Nettoyage des données 94
AC-04(26) — Mesures de filtrage de vérification 95
AC-04(27) — Mécanismes de filtrage redondants et indépendants 96
AC-04(28) — Pipelines de filtre linéaire 97
AC-04(29) — Moteurs d'orchestration de filtre 98
AC-04(30) — Mécanismes de filtrage à l'aide de plusieurs processus 99
AC-04(31) — Prévenir l'échec d'un transfert de contenu 100
AC-04(32) — Exigences des processus pour le transfert d'information 101
AC-05 — Séparation des tâches 102
AC-06 — Droit d'accès minimal 103
AC-06(01) — Autorisation de l'accès aux fonctions de sécurité 104
AC-06(02) — Accès non privilégié aux fonctions non liées à la sécurité 105
AC-06(03) — Accès réseau aux commandes privilégiées 106
AC-06(04) — Domaines de traitement séparés 107
AC-06(05) — Comptes privilégiés 108
AC-06(06) — Accès privilégié des utilisatrices et utilisateurs ne faisant pas partie de l'organisation 109

AC-06(07) — Examen des privilèges d'utilisateur 110
AC-06(08) — Niveaux de droits d'accès pour une exécution de code 111
AC-06(09) — Journalisation de l'utilisation des fonctions privilégiées 112
AC-06(10) — Interdiction aux utilisatrices et utilisateurs non privilégiés d'exécuter des fonctions privilégiées 113
AC-07 — Tentatives d'ouverture de session infructueuses 114
AC-07(01) — Verrouillage automatique du compte 115
AC-07(02) — Purge ou nettoyage d'appareils mobiles 116
AC-07(03) — Limitation des tentatives par biométrie 117
AC-07(04) — Utilisation d'un autre facteur d'authentification 118
AC-08 — Avis d'utilisation système 119
AC-09 — Avis d'ouverture de session précédente 120
AC-09(01) — Ouvertures de session infructueuses 121
AC-09(02) — Tentatives fructueuses et infructueuses d'ouverture de session 122
AC-09(03) — Avis de changements au compte 123
AC-09(04) — Information supplémentaire sur l'ouverture de session 124
AC-10 — Contrôle de sessions simultanées 125
AC-11 — Verrouillage d'appareil 126
AC-11(01) — Masquage de l'affichage au moyen d'une image 127
AC-12 — Fin de session 128
AC-12(01) — Fermetures de session exécutées par les utilisatrices et utilisateurs 129
AC-12(02) — Message d'interruption 130
AC-12(03) — Message d'avertissement de délai d'expiration 131
AC-13 — Contrôle d'accès 132
AC-14 — Opérations permises sans identification ni authentification 133
AC-14(01) — Usages indispensables 134
AC-15 — Marquage automatique 135
AC-16 — Attributs de sécurité et de protection de la vie privée 136
AC-16(01) — Association dynamique d'attribut 137
AC-16(02) — Changements aux valeurs d'attribut par des personnes autorisées 138
AC-16(03) — Maintenance des associations d'attributs par système 139
AC-16(04) — Association d'attributs par personnes autorisées 140
AC-16(05) — Affichage d'attributs des objets transmis à des dispositifs de sortie 141
AC-16(06) — Maintien des associations d'attributs 142
AC-16(07) — Interprétation uniforme des attributs 143
AC-16(08) — Techniques et technologies d'association 144
AC-16(09) — Réaffectation d'attribut – Mécanismes remaniés 145
AC-16(10) — Configuration d'attribut par des personnes autorisées 146
AC-17 — Accès à distance 147

AC-17(01) — Surveillance et contrôle 148
AC-17(02) — Protection de la confidentialité et de l'intégrité au moyen du chiffrement 149
AC-17(03) — Points de contrôle d'accès gérés 150
AC-17(04) — Commandes et accès privilégiés 151
AC-17(05) — Surveillance pour connexions non autorisées 152
AC-17(06) — Protection de l'information sur les mécanismes 153
AC-17(07) — Protection supplémentaire pour l'accès aux fonctions de sécurité 154
AC-17(08) — Désactiver les protocoles réseau non sécurisés 155
AC-17(09) — Déconnecter ou désactiver l'accès 156
AC-17(10) — Authentification des commandes à distance 157
AC-17(400) — Accès à distance à des comptes privilégiés 158
AC-18 — Accès sans fil 159
AC-18(01) — Authentification et chiffrement 160
AC-18(02) — Surveillance des connexions non autorisées 161
AC-18(03) — Désactivation du réseautage sans fil 162
AC-18(04) — Restriction des configurations par les utilisatrices et utilisateurs 163
AC-18(05) — Antennes et puissance de transmission 164
AC-19 — Contrôle d'accès pour les appareils mobiles 165
AC-19(01) — Utilisation de dispositifs de stockage portatifs et accessibles en écriture 166
AC-19(02) — Utilisation de dispositifs de stockage portatifs appartenant à des particuliers 167
AC-19(03) — Utilisation de dispositifs de stockage portatifs sans propriétaire identifiable 168
AC-19(04) — Restrictions liées à l'information classifiée 169
AC-19(05) — Chiffrement complet des appareils ou chiffrement des contenants 170
AC-19(400) — Appareils sans fil 171
AC-20 — Utilisation de systèmes externes 172
AC-20(01) — Limites relatives à l'utilisation autorisée 173
AC-20(02) — Dispositifs de stockage portatifs – Utilisation restreinte 174
AC-20(03) — Systèmes ne faisant pas partie de l'organisation – Utilisation restreinte 175
AC-20(04) — Dispositifs de stockage accessibles par réseau – Utilisation interdite 176
AC-20(05) — Dispositifs de stockage portatifs – Utilisation interdite 177
AC-21 — Échange d'information 178
AC-21(01) — Application des décisions automatisées 179
AC-21(02) — Recherche et récupération d'information 180
AC-21(400) — Accord d'échange de renseignements 181
AC-21(401) — Entente d'échange de renseignements 182
AC-22 — Contenu accessible au public 183
AC-23 — Protection contre l'exploration de données 184
AC-24 — Décisions de contrôle d'accès 185

AC-24(01) — Transmission de l'information sur l'autorisation d'accès 186
AC-24(02) — Aucune identité d'utilisatrices, utilisateurs ou processus 187
AC-25 — Moniteur de référence 188

AT — Formation du personnel à la cybersécurité

AT-01 — Politique et procédures de sensibilisation et de formation 190
AT-02 — Formation et sensibilisation en matière de sécurité 191
AT-02(01) — Exercices pratiques 192
AT-02(02) — Menace interne 193
AT-02(03) — Piratage psychologique et exploration de données 194
AT-02(04) — Communications suspectes et comportements anormaux de systèmes 195
AT-02(05) — Menaces persistantes avancées 196
AT-02(06) — Environnement de cybermenaces 197
AT-03 — Formation selon le rôle 198
AT-03(01) — Contrôles environnementaux 199
AT-03(02) — Contrôles de sécurité physiques 200
AT-03(03) — Exercices pratiques 201
AT-03(04) — Communications suspectes et comportements anormaux de systèmes 202
AT-03(05) — Traitement des renseignements personnels 203
AT-04 — Dossiers de formation 204
AT-05 — Contacts avec les groupes et associations de sécurité 205
AT-06 — Rétroaction sur les formations suivies 206

AU — Journaux d'audit, traçabilité des actions

AU-01 — Politique et procédures de vérification et de responsabilisation 208
AU-02 — Journalisation d'événements 209
AU-02(01) — Compilation d'enregistrements de vérification provenant de sources multiples 210
AU-02(02) — Sélection d'événements de vérification par composant 211
AU-02(03) — Examens et mises à jour 212
AU-02(04) — Fonctions privilégiées 213
AU-03 — Contenu des enregistrements de vérification 214
AU-03(01) — Information de vérification supplémentaire 215
AU-03(02) — Gestion centralisée du contenu des enregistrements de vérification 216
AU-03(03) — Limitation des éléments liés aux renseignements personnels 217
AU-04 — Capacité de stockage des journaux de vérification 218
AU-04(01) — Transfert vers une capacité de stockage secondaire 219
AU-05 — Intervention en cas d'échec du processus de journalisation des données de vérification 220
AU-05(01) — Avertissement de capacité de stockage 221
AU-05(02) — Alertes en temps réel 222

AU-05(03) — Seuils de volume de trafic configurables 223
AU-05(04) — Interruption en cas d'échec 224
AU-05(05) — Capacité de journalisation des données de vérification secondaire 225
AU-06 — Examen, analyse et production de rapports liés aux enregistrements de vérification 226
AU-06(01) — Intégration de processus automatisés 227
AU-06(02) — Alertes de sécurité automatisées 228
AU-06(03) — Correspondance des référentiels pour les enregistrements de vérification 229
AU-06(04) — Analyses et examens centralisés 230
AU-06(05) — Analyse intégrée des enregistrements de vérification 231
AU-06(06) — Corrélation avec la surveillance physique 232
AU-06(07) — Opérations autorisées 233
AU-06(08) — Analyse plein texte des commandes privilégiées 234
AU-06(09) — Corrélation avec l'information provenant de sources non techniques 235
AU-06(10) — Ajustement du niveau d'examen 236
AU-07 — Réduction des enregistrements de vérification et génération de rapports 237
AU-07(01) — Traitement automatique 238
AU-07(02) — Triage et recherche automatisés 239
AU-08 — Horodatage du contrôle 240
AU-08(01) — Synchronisé avec source de temps qui fait autorité 241
AU-08(02) — Deuxième source de temps qui fait autorité 242
AU-09 — Protection de l'information de vérification 243
AU-09(01) — Supports matériels non réinscriptibles 244
AU-09(02) — Stockage sur des systèmes ou des composants physiques séparés 245
AU-09(03) — Protection cryptographique 246
AU-09(04) — Accès par un sous-ensemble d'utilisateurs privilégiés 247
AU-09(05) — Double autorisation 248
AU-09(06) — Accès en lecture seule 249
AU-09(07) — Stockage sur composant avec un système d'exploitation différent 250
AU-10 — Non-répudiation 251
AU-10(01) — Association avec les identités 252
AU-10(02) — Validité du lien avec l'identité de l'auteure ou auteur de l'information 253
AU-10(03) — Chaîne de possession 254
AU-10(04) — Validité du lien avec l'identité de l'examinatrice ou examinateur de l'information 255
AU-10(05) — Signatures numériques 256
AU-11 — Conservation des enregistrements de vérification 257
AU-11(01) — Capacité de récupération à long terme 258
AU-12 — Génération d'enregistrements de vérification 259
AU-12(01) — Piste de vérification à l'échelle du système et corrélée dans le temps 260

AU-12(02) — Formats normalisés 261
AU-12(03) — Modifications par des personnes autorisées 262
AU-12(04) — Vérifications des paramètres d'interrogation des renseignements personnels 263
AU-13 — Surveillance de la divulgation d'information 264
AU-13(01) — Utilisation d'outils automatisés 265
AU-13(02) — Examen des sites surveillés 266
AU-13(03) — Duplication non autorisée d'information 267
AU-14 — Vérification des sessions 268
AU-14(01) — Démarrage du système 269
AU-14(02) — Contenu de la saisie et de l'enregistrement 270
AU-14(03) — Visualisation et écoute à distance 271
AU-15 — Capacité de journalisation des données de vérification secondaire 272
AU-16 — Journalisation des données de vérification transorganisationnelle 273
AU-16(01) — Préservation de l'identité 274
AU-16(02) — Échange d'information de vérification 275
AU-16(03) — Dissociabilité 276

CA — Évaluation des systèmes et autorisation

CA-01 — Politique et procédures d'évaluation, d'autorisation et de surveillance 278
CA-02 — Évaluations de contrôle 279
CA-02(01) — Évaluatrices et évaluateurs indépendants 281
CA-02(02) — Évaluations spécialisées 282
CA-02(03) — Tirer parti des résultats d'évaluation provenant d'organisations externes 283
CA-03 — Échange d'information 284
CA-03(01) — Connexions à des systèmes de sécurité nationaux non classifiés 285
CA-03(02) — Connexions à des systèmes de sécurité nationaux classifiés 286
CA-03(03) — Connexions à des systèmes de sécurité non nationaux non classifiés 287
CA-03(04) — Connexions aux réseaux publics 288
CA-03(05) — Connexions restreintes à des systèmes externes 289
CA-03(06) — Autorisations de transfert 290
CA-03(07) — Échanges d'information éphémère 291
CA-04 — Certification de sécurité 292
CA-05 — Plan d'action et des jalons 293
CA-05(01) — Automatisation du soutien aux fins d'exactitude et d'actualité 294
CA-06 — Autorisation 295
CA-06(01) — Autorisation conjointe (au sein de l'organisation) 296
CA-06(02) — Autorisation conjointe (interorganisation) 297
CA-07 — Surveillance continue 298
CA-07(01) — Évaluation indépendante 299

CA-07(02) — Types d'évaluations 300
CA-07(03) — Analyses des tendances 301
CA-07(04) — Surveillance des risques 302
CA-07(05) — Analyse de la cohérence 303
CA-07(06) — Soutien automatisé pour la surveillance 304
CA-08 — Tests d'intrusion 305
CA-08(01) — Équipe, agente ou agent indépendant chargé des tests d'intrusion 306
CA-08(02) — Exercices effectués par l'équipe de testeuses et testeurs 307
CA-08(03) — Tests d'intrusion des installations 308
CA-09 — Connexions des systèmes internes 309
CA-09(01) — Vérifications de la conformité 310

CM — Gestion sécurisée des configurations système

CM-01 — Politique et procédures de gestion des configurations 312
CM-02 — Configuration de référence 313
CM-02(01) — Examens et mises à jour 314
CM-02(02) — Automatisation du soutien aux fins d'exactitude et d'actualité 315
CM-02(03) — Conservation des configurations antérieures 316
CM-02(04) — Logiciels non autorisés 317
CM-02(05) — Logiciels autorisés 318
CM-02(06) — Environnements de test et de développement 319
CM-02(07) — Configuration des systèmes et des composants pour des zones à risque élevé 320
CM-03 — Contrôle des changements de configuration 321
CM-03(01) — Automatisation concernant la documentation, les avis et les interdictions de changements 322
CM-03(02) — Tests, validation et documentation des changements 323
CM-03(03) — Mise en oeuvre automatisée des changements 324
CM-03(04) — Représentantes et représentants de la sécurité et de la protection de la vie privée 325
CM-03(05) — Mesures de sécurité automatisées 326
CM-03(06) — Gestion de la cryptographie 327
CM-03(07) — Examen des changements apportés au système 328
CM-03(08) — Empêcher ou limiter les changements de configuration 329
CM-04 — Analyses des répercussions 330
CM-04(01) — Environnements de test distincts 331
CM-04(02) — Vérification des contrôles 332
CM-05 — Restrictions d'accès associées aux changements 333
CM-05(01) — Enregistrements de vérification et d'application des restrictions d'accès automatisées 334
CM-05(02) — Examen des changements apportés au système 335
CM-05(03) — Composants signés 336

CM-05(04) — Double autorisation 337
CM-05(05) — Limite des privilèges pour la production et l'opération 338
CM-05(06) — Privilèges de bibliothèque limités 339
CM-05(07) — Automatisation de la mise en oeuvre de mécanismes de sécurité 340
CM-06 — Paramètres de configuration 341
CM-06(01) — Gestion, application et vérification automatisées 342
CM-06(02) — Intervention lorsque des changements non autorisés sont apportés 343
CM-06(03) — Détection de changement non autorisé 344
CM-06(04) — Démonstration de conformité 345
CM-07 — Fonctionnalité minimale 346
CM-07(01) — Examen périodique 347
CM-07(02) — Prévention de l'exécution des programmes 348
CM-07(03) — Conformité aux exigences d'enregistrement 349
CM-07(04) — Logiciel non autorisé – Interdire par exception 350
CM-07(05) — Logiciels autorisés – Autorisation par exception 351
CM-07(06) — Environnements clos aux privilèges restreints 352
CM-07(07) — Exécution de code dans des environnements protégés 353
CM-07(08) — Code binaire ou exécutable sur machine 354
CM-07(09) — Empêcher l'utilisation de composants matériels non autorisés 355
CM-08 — Inventaire des composants de système 356
CM-08(01) — Mises à jour durant l'installation et le retrait 357
CM-08(02) — Automatisation de la maintenance 358
CM-08(03) — Détection automatisée de composants non autorisés 359
CM-08(04) — Information sur la responsabilisation 360
CM-08(05) — Aucune comptabilisation en double des composants 361
CM-08(06) — Configurations évaluées et écarts approuvés 362
CM-08(07) — Référentiel centralisé 363
CM-08(08) — Localisation automatisée 364
CM-08(09) — Attribution de composants à des systèmes 365
CM-09 — Plan de gestion des configurations 366
CM-09(01) — Attribution des responsabilités 367
CM-10 — Restrictions relatives à l'utilisation des logiciels 368
CM-10(01) — Logiciels ouverts 369
CM-11 — Logiciels installés par les utilisatrices et utilisateurs 370
CM-11(01) — Alertes pour les installations non autorisées 371
CM-11(02) — Installation de logiciels avec statut privilégié 372
CM-11(03) — Application et surveillance automatisées 373
CM-12 — Localisation de l'information 374

CM-12(01) — Outils automatisés associés à la localisation de l'information 375
CM-13 — Mappage des actions de données 376
CM-14 — Composants signés 377

CP — Planification de la continuité d'activité

CP-01 — Politique et procédures de planification d'urgence 379
CP-02 — Plan d'urgence 380
CP-02(01) — Coordination avec les plans connexes 381
CP-02(02) — Planification de la capacité 382
CP-02(03) — Reprise de la mission et des activités 383
CP-02(04) — Reprise de toutes les fonctions liées à la mission et aux activités de l'organisation 384
CP-02(05) — Continuer les fonctions liées à la mission et aux activités 385
CP-02(06) — Sites de traitement et de stockage auxiliaires 386
CP-02(07) — Coordination avec les fournisseurs de services externes 387
CP-02(08) — Désignation des biens essentiels 388
CP-03 — Formation en mesure d'urgence 389
CP-03(01) — Événements simulés 390
CP-03(02) — Mécanismes utilisés dans des environnements de formation 391
CP-04 — Mise à l'essai du plan d'urgence 392
CP-04(01) — Coordination avec les plans connexes 393
CP-04(02) — Site de traitement auxiliaires 394
CP-04(03) — Tests automatisés 395
CP-04(04) — Reprise et reconstitution complètes 396
CP-04(05) — Se mettre au défi 397
CP-05 — Mise à jour du plan d'urgence 398
CP-06 — Site de stockage auxiliaire 399
CP-06(01) — Séparation du site principal 400
CP-06(02) — Objectifs de délai de rétablissement et de point de rétablissement 401
CP-06(03) — Accessibilité 402
CP-07 — Site de traitement auxiliaire 403
CP-07(01) — Séparation du site principal 404
CP-07(02) — Accessibilité 405
CP-07(03) — Priorité de service 406
CP-07(04) — Préparation en vue de l'utilisation 407
CP-07(05) — Protections équivalentes de sécurité de l'information 408
CP-07(06) — Impossibilité de retourner au site principal 409
CP-08 — Services de télécommunications 410
CP-08(01) — Dispositions de priorité de service 411
CP-08(02) — Points de défaillance uniques 412

CP-08(03) — Séparation des fournisseurs principaux et auxiliaires 413
CP-08(04) — Plan d'urgence des fournisseurs 414
CP-08(05) — Test des services de télécommunications de secours 415
CP-09 — Sauvegarde du système 416
CP-09(01) — Tests de fiabilité et d'intégrité 417
CP-09(02) — Essai de restauration au moyen de l'échantillonnage 418
CP-09(03) — Stockage distinct pour l'information essentielle 419
CP-09(04) — Protection contre une modification non autorisée 420
CP-09(05) — Transfert vers un site de stockage auxiliaire 421
CP-09(06) — Système secondaire redondant 422
CP-09(07) — Double autorisation pour la suppression ou la destruction 423
CP-09(08) — Protection cryptographique 424
CP-10 — Reprise et reconstitution du système 425
CP-10(01) — Tests relatifs au plan d'urgence 426
CP-10(02) — Reprise des transactions 427
CP-10(03) — Contrôles de sécurité compensatoires 428
CP-10(04) — Restauration dans les délais précisés 429
CP-10(05) — Capacité de basculement 430
CP-10(06) — Protection des composants 431
CP-11 — Protocoles de communications de secours 432
CP-12 — Mode sans échec 433
CP-13 — Mécanismes de sécurité de secours 434

IA — Contrôle de l'identité et de l'authentification

IA-01 — Politique et procédures d'identification et d'authentification 436
IA-02 — Identification et authentification (utilisatrices et utilisateurs de l'organisation) 437
IA-02(01) — AMF robustes pour les comptes privilégiés 438
IA-02(02) — AMF pour comptes non privilégiés 439
IA-02(03) — Accès local aux comptes privilégiés 440
IA-02(04) — local aux comptes non privilégiés 441
IA-02(05) — Authentification individuelle avec authentification de groupe 442
IA-02(06) — Accès aux comptes – Dispositif distinct 443
IA-02(07) — Accès réseau aux comptes non privilégiés – Dispositif distinct 444
IA-02(08) — Accès aux comptes – Résistant à la réinsertion 445
IA-02(09) — Accès réseau aux comptes non privilégiés – Résistance à la réinsertion 446
IA-02(10) — Authentification unique 447
IA-02(11) — Accès à distance – Dispositif distinct 448
IA-02(12) — Utilisation de jeton matériel basé sur des justificatifs d'identité d'ICP 449
IA-02(13) — Authentification hors bande 450

IA-02(400) — AMF pour accès à distance aux comptes privilégiés 451
IA-03 — Identification et authentification des dispositifs 452
IA-03(01) — Authentification bidirectionnelle cryptographique 453
IA-03(02) — Authentification réseau bidirectionnelle cryptographique 454
IA-03(03) — Attribution dynamique des adresses 455
IA-03(04) — Attestation de dispositifs 456
IA-04 — Gestion des identifiants 457
IA-04(01) — Interdire l'utilisation d'identifiants de compte en tant qu'identifiants publics 458
IA-04(02) — Autorisation de superviseure ou superviseur 459
IA-04(03) — Multiples formes de certification 460
IA-04(04) — Établissement du statut d'une utilisatrice ou d'un utilisateur 461
IA-04(05) — Gestion dynamique 462
IA-04(06) — Gestion interorganisationnelle 463
IA-04(07) — Inscription en personne 464
IA-04(08) — Identifiants pseudonymes par paires 465
IA-04(09) — Maintenance et protection d'attributs 466
IA-04(400) — Protection de la biométrie 467
IA-04(401) — Intégrité de la biométrie 468
IA-05 — Gestion des authentifiants 469
IA-05(01) — Authentification basée sur mot de passe 470
IA-05(02) — Authentification basée sur clé publique 471
IA-05(03) — Enregistrement par tierce partie externe de confiance 472
IA-05(04) — Soutien automatisé aux fins de détermination de la robustesse du mot de passe 473
IA-05(05) — Changement des authentifiants avant la livraison 474
IA-05(06) — Protection des authentifiants 475
IA-05(07) — Aucun authentifiant statique intégré non chiffré 476
IA-05(08) — Comptes multiples des systèmes 477
IA-05(09) — Gestion des justificatifs d'identité fédérés 478
IA-05(10) — Liaison dynamique des justificatifs d'identité 479
IA-05(11) — Authentification basée sur un jeton matériel 480
IA-05(12) — Rendement de l'authentification biométrique 481
IA-05(13) — Expiration d'authentifiants en mémoire cache 482
IA-05(14) — Gestion du contenu des magasins de confiance d'ICP 483
IA-05(15) — Produits et services conformes aux niveaux d'assurance de l'identité, des justificatifs et de l'authentification 484
IA-05(16) — Émission d'un authentifiant en personne ou par tierce partie externe de confiance 485
IA-05(17) — Détection des attaques de présentation pour les authentifiants biométriques 486
IA-05(18) — Gestionnaires de mots de passe 487
IA-06 — Réinjection d'authentification 488

IA-07 — Authentification du module cryptographique 489

IA-08 — Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) 490

IA-08(01) — Acceptation des justificatifs d'identité d'ICP d'autres organismes 491

IA-08(02) — Acceptation des authentifiants externes 492

IA-08(03) — Utilisation de produits approuvés par l'architecture FICAM 493

IA-08(04) — Utilisation de profils définis 494

IA-08(05) — Acceptation des justificatifs de vérification de l'identité personnelle interopérables (PIV-I) 495

IA-08(06) — Dissociabilité 496

IA-08(400) — Identité et assurance des justificatifs 497

IA-09 — Identification et authentification des services 498

IA-09(01) — Échange d'information 499

IA-09(02) — Transmission des décisions 500

IA-10 — Authentification adaptative 501

IA-11 — Réauthentification 502

IA-12 — Confirmation de l'identité 503

IA-12(01) — Autorisation de superviseure ou superviseur 504

IA-12(02) — Preuve d'identité 505

IA-12(03) — Validation et vérification de preuve d'identité 506

IA-12(04) — Validation et vérification en personne 507

IA-12(05) — Confirmation d'adresse 508

IA-12(06) — Accepter les identités confirmées externes 509

IA-13 — Fournisseurs d'identité et serveurs d'autorisation 510

IA-13(01) — Protection des clés cryptographiques 511

IA-13(02) — Vérification des assertions d'identité et des jetons d'accès 512

IA-13(03) — Gestion des jetons 513

IR — Gestion des incidents de cybersécurité

IR-01 — Politique et procédures d'intervention en cas d'incident 515

IR-02 — Formation sur les interventions en cas d'incident 516

IR-02(01) — Événements simulés 517

IR-02(02) — Environnements de formation automatisée 518

IR-02(03) — Atteinte à la vie privée 519

IR-03 — Tests d'intervention en cas d'incident 520

IR-03(01) — Tests automatisés 521

IR-03(02) — Coordination avec les plans connexes 522

IR-03(03) — Amélioration continue 523

IR-04 — Traitement des incidents 524

IR-04(01) — Processus de traitement des incidents automatisés 525
IR-04(02) — Reconfiguration dynamique 526
IR-04(03) — Continuité des opérations 527
IR-04(04) — Corrélation de l'information 528
IR-04(05) — Désactivation automatique du système 529
IR-04(06) — Menace interne 530
IR-04(07) — Menace interne – Coordination au sein de l'organisation 531
IR-04(08) — Corrélation avec les organisations externes 532
IR-04(09) — Capacités d'intervention dynamique 533
IR-04(10) — Coordination relative à la chaîne d'approvisionnement 534
IR-04(11) — Équipe intégrée d'intervention en cas d'incident 535
IR-04(12) — Programme malveillant et analyse criminalistique 536
IR-04(13) — Analyse comportementale 537
IR-04(14) — Centre des opérations de sécurité 538
IR-04(15) — Relations publiques, réparation de réputation et notification 539
IR-05 — Surveillance des incidents 540
IR-05(01) — Suivi, collecte de données et analyses automatisés 541
IR-06 — Signalement des incidents 542
IR-06(01) — Signalement automatisé 543
IR-06(02) — Vulnérabilités liées aux incidents 544
IR-06(03) — Coordination avec la chaîne d'approvisionnement 545
IR-07 — Assistance en cas d'incident 546
IR-07(01) — Soutien automatisé concernant la disponibilité de l'information et du soutien 547
IR-07(02) — Coordination avec les fournisseurs externes 548
IR-08 — Plan d'intervention en cas d'incident 549
IR-08(01) — Atteintes à la vie privée 550
IR-09 — Intervention en cas de fuite d'information 551
IR-09(01) — Personnel responsable 552
IR-09(02) — Formation 553
IR-09(03) — Opérations à la suite d'une fuite 554
IR-09(04) — Exposition au personnel non autorisé 555
IR-10 — Équipe d'analyse de la sécurité de l'information intégrée 556

MA — Sécurité des opérations de maintenance

MA-01 — Politique et procédures de maintenance 558
MA-02 — Maintenance contrôlée 559
MA-02(01) — Contenu des enregistrements 560
MA-02(02) — Activités de maintenance automatisées 561
MA-03 — Outils de maintenance 562

MA-03(01) — Inspection des outils 563
MA-03(02) — Inspection des supports 564
MA-03(03) — Prévention des retraits non autorisés 565
MA-03(04) — Utilisation restreinte des outils 566
MA-03(05) — Exécution avec privilège 567
MA-03(06) — Mises à jour logicielles et correctifs 568
MA-04 — Maintenance non locale 569
MA-04(01) — Journalisation et examen 570
MA-04(02) — Documenter la maintenance non locale 571
MA-04(03) — Sécurité et nettoyage comparables 572
MA-04(04) — Authentification et séparation des sessions de maintenance 573
MA-04(05) — Approbations et avis 574
MA-04(06) — Protection cryptographique 575
MA-04(07) — Vérification de la déconnexion 576
MA-05 — Personnel de maintenance 577
MA-05(01) — Personnes ne détenant pas l'accès approprié 578
MA-05(02) — Habilitations de sécurité pour les systèmes classifiés 579
MA-05(03) — Exigences relatives à la citoyenneté pour les systèmes classifiés 580
MA-05(04) — Ressortissantes ou ressortissants étrangers 581
MA-05(05) — Maintenance non liée aux systèmes 582
MA-06 — Maintenance opportune 583
MA-06(01) — Maintenance préventive 584
MA-06(02) — Maintenance prévisionnelle 585
MA-06(03) — Soutien automatisé pour la maintenance prévisionnelle 586
MA-07 — Maintenance sur site 587

MP — Protection des supports d'information

MP-01 — Politique et procédures de protection des supports 589
MP-02 — Accès aux supports 590
MP-02(01) — Accès limité automatisé 591
MP-02(02) — Protection cryptographique 592
MP-03 — Marquage des supports 593
MP-04 — Entreposage des supports 594
MP-04(01) — Protection cryptographique 595
MP-04(02) — Accès limité automatisé 596
MP-05 — Transport des supports 597
MP-05(01) — Protection à l'extérieur des zones contrôlées 598
MP-05(02) — Documentation des activités 599
MP-05(03) — Gardiennes et gardiens 600

MP-05(04) — Protection cryptographique 601
MP-06 — Nettoyage des supports 602
MP-06(01) — Examen, approbation, suivi, documentation et vérification 603
MP-06(02) — Mise à l'essai du matériel 604
MP-06(03) — Techniques non destructives 605
MP-06(04) — Information protégée 606
MP-06(05) — Information classifiée 607
MP-06(06) — Destruction de supports 608
MP-06(07) — Double autorisation 609
MP-06(08) — Purge ou nettoyage à distance de l'information 610
MP-07 — Utilisation des supports 611
MP-07(01) — Interdire l'utilisation sans propriétaire 612
MP-07(02) — Interdire l'utilisation de supports résistant au nettoyage 613
MP-08 — Déclassement des supports 614
MP-08(01) — Documentation du processus 615
MP-08(02) — Mise à l'essai du matériel 616
MP-08(03) — Information protégée 617
MP-08(04) — Information classifiée 618

PE — Sécurité physique des installations

PE-01 — Politique et procédures de protection physique et environnementale 620
PE-02 — Autorisations d'accès physique 621
PE-02(01) — Accès par poste ou rôle 622
PE-02(02) — Deux formes d'identification 623
PE-02(03) — Accès restreint sans escorte 624
PE-02(400) — Exigences des cartes d'identité 625
PE-03 — Contrôle d'accès physique 626
PE-03(01) — Accès au système 627
PE-03(02) — Installation et systèmes 628
PE-03(03) — Garde continue 629
PE-03(04) — Contenants verrouillables 630
PE-03(05) — Protection antitrafiquage 631
PE-03(06) — Tests d'intrusion des installations 632
PE-03(07) — Barrières physiques 633
PE-03(08) — Vestibules de contrôle d'accès 634
PE-03(400) — Inspections de sécurité 635
PE-04 — Contrôle d'accès pour la transmission 636
PE-05 — Contrôle d'accès aux dispositifs de sortie 637
PE-05(01) — Accès à la sortie par personnes autorisées 638

PE-05(02) — Associer l'identité des individus 639
PE-05(03) — Marquage des dispositifs de sortie 640
PE-06 — Surveillance de l'accès physique 641
PE-06(01) — Alarmes de détection d'intrusion et équipement de surveillance 642
PE-06(02) — Automatisation de la reconnaissance des intrusions et des interventions 643
PE-06(03) — Surveillance vidéo 644
PE-06(04) — Surveillance de l'accès physique aux systèmes 645
PE-07 — Contrôle des visiteuses et visiteurs 646
PE-08 — Registre des accès des visiteuses et visiteurs 647
PE-08(01) — Tenue et examen automatisés du registre 648
PE-08(02) — Registre des accès physiques 649
PE-08(03) — Limitation des éléments liés aux renseignements personnels 650
PE-09 — Équipement et câblage d'alimentation 651
PE-09(01) — Câblage redondant 652
PE-09(02) — Contrôles de tension automatisés 653
PE-10 — Arrêt d'urgence 654
PE-10(01) — Activation accidentelle et non autorisée 655
PE-11 — Alimentation d'urgence 656
PE-11(01) — Source d'alimentation de secours – Capacité opérationnelle minimale 657
PE-11(02) — Source d'alimentation de secours – Autonome 658
PE-12 — Éclairage de sécurité 659
PE-12(01) — Fonctions opérationnelles et de mission essentielles 660
PE-13 — Protection contre les incendies 661
PE-13(01) — Activation et avis automatiques 662
PE-13(02) — Systèmes d'extinction – Activation et avis automatiques 663
PE-13(03) — Extinction automatique d'incendie 664
PE-13(04) — Inspections 665
PE-13(400) — Services d'urgence 666
PE-14 — Contrôles environnementaux 667
PE-14(01) — Contrôles automatisés 668
PE-14(02) — Surveillance avec des alarmes et des notifications 669
PE-15 — Protection contre les dégâts d'eau 670
PE-15(01) — Soutien automatisé 671
PE-16 — Livraison et retrait 672
PE-17 — Autres lieux de travail 673
PE-18 — Emplacement des composants du système 674
PE-18(01) — Site de l'installation 675
PE-19 — Fuite d'information 676

PE-19(01) — Stratégies et procédures nationales en matière d'émission 677
PE-20 — Surveillance et suivi des biens 678
PE-21 — Protection contre les impulsions électromagnétiques 679
PE-22 — Marquage des composants 680
PE-23 — Emplacement de l'installation 681
PE-400 — Environnements à distance et de télétravail 682
PE-400(01) — Rangement physique d'information et de biens 683
PE-400(02) — Travail à distance et télétravail à l'étranger 684
PE-401 — Centre des opérations de sécurité 685

PL — Planification de la cybersécurité

PL-01 — Politique et procédures de planification 687
PL-02 — Plans de sécurité et de protection de la vie privée des systèmes 688
PL-02(01) — Concept d'opérations 690
PL-02(02) — Architecture fonctionnelle 691
PL-02(03) — Planifier et coordonner avec d'autres entités organisationnelles 692
PL-03 — Mise à jour du plan de sécurité des systèmes 693
PL-04 — Règles de conduite 694
PL-04(01) — Restriction d'utilisation des médias sociaux et des sites et applications externes 695
PL-05 — Évaluation des facteurs relatifs à la vie privée 696
PL-06 — Planification des activités relatives à la sécurité 697
PL-07 — Concepts d'opérations 698
PL-08 — Architecture de sécurité et de protection de la vie privée 699
PL-08(01) — Défense en profondeur 700
PL-08(02) — Diversité des fournisseurs 701
PL-09 — Gestion centrale 702
PL-10 — Sélection de la base de référence 703
PL-11 — Adaptation de la base de référence 704

PM — Gestion de programme à l'échelle organisationnelle

PM-01 — Plan du programme de sécurité de l'information 706
PM-02 — Rôle de leadership du programme de sécurité de l'information 707
PM-03 — Ressources de sécurité et de protection de la vie privée de l'information 708
PM-04 — Processus du plan d'action et des jalons 709
PM-05 — Inventaire des systèmes et des programmes 710
PM-05(01) — Inventaire des renseignements personnels 711
PM-06 — Mesures du rendement 712
PM-07 — Architecture d'entreprise 713
PM-07(01) — Déchargement 714

PM-08 — Plan des infrastructures essentielles 715
PM-09 — Stratégie de gestion des risques 716
PM-10 — Processus d'autorisation 717
PM-11 — Définition des processus liés à la mission et aux activités 718
PM-12 — Programme de protection contre la menace interne 719
PM-13 — Personnel affecté à la sécurité et à la protection de la vie privée 720
PM-14 — Tests, formation et surveillance 721
PM-15 — Groupes et associations de sécurité et de protection de la vie privée 722
PM-16 — Programme de sensibilisation aux menaces 723
PM-16(01) — Moyens automatisés pour l'échange de renseignement sur les menaces 724
PM-17 — Protection de l'information contrôlée sur les systèmes externalisés 725
PM-18 — Plan du programme de protection de la vie privée 726
PM-19 — Rôle de leadership du programme de protection de la vie privée 727
PM-20 — Communication des principaux services de protection de la vie privée 728
PM-20(01) — Politiques de protection de la vie privée pour les sites Web, les applications et les services numériques 729
PM-21 — Maintien d'un registre des divulgations 730
PM-22 — Gestion de la qualité des renseignements personnels 731
PM-23 — Comité de gouvernance des données 732
PM-24 — Comité de l'intégrité des données 733
PM-25 — Réduction des renseignements personnels utilisés aux fins de tests, de formation et de recherche 734
PM-26 — Gestion des plaintes 735
PM-27 — Génération de rapports concernant la protection de la vie privée 736
PM-28 — Cadrage des risques 737
PM-29 — Rôles de leadership pour le programme de gestion des risques 738
PM-30 — Stratégie de gestion des risques liés à la chaîne d'approvisionnement 739
PM-30(01) — Fournisseurs d'articles critiques ou essentiels à la mission 740
PM-31 — Stratégie de surveillance continue 741
PM-32 — Établissement des objectifs 742

PS — Sécurité du personnel (vérifications, accès, etc.)

PS-01 — Politique et procédures de sécurité du personnel 744
PS-02 — Analyse de sécurité des postes 745
PS-03 — Filtrage de sécurité du personnel 746
PS-03(01) — Information classifiée 747
PS-03(02) — Endoctrinement officiel 748
PS-03(03) — Information exigeant des mesures de protection spéciales 749
PS-03(04) — Exigences relatives à la citoyenneté 750

PS-04 — Cessation d'emploi du personnel 751
PS-04(01) — Exigences régissant l'après-mandat 752
PS-04(02) — Opérations automatisées 753
PS-04(400) — Astreint au secret à perpétuité 754
PS-05 — Transfert du personnel 755
PS-05(400) — Autorisation de sécurité 756
PS-06 — Ententes d'accès 757
PS-06(01) — Information exigeant une protection spéciale 758
PS-06(02) — Information classifiée exigeant une protection spéciale 759
PS-06(03) — Exigences régissant l'après-mandat 760
PS-07 — Sécurité du personnel externe 761
PS-08 — Sanctions imposées au personnel 762
PS-09 — Descriptions de poste 763

PT — Traitement des renseignements personnels identifiables et transparence

PT-01 — Politique et procédures de traitement des renseignements personnels et de transparence 765
PT-02 — Pouvoir en matière de collecte et d'utilisation de renseignements personnels 766
PT-02(01) — Étiquetage des données 767
PT-02(02) — Automatisation 768
PT-03 — Traitement, utilisation et divulgation de renseignements personnels 769
PT-03(01) — Étiquetage des données 770
PT-03(02) — Automatisation 771
PT-04 — Consentement 772
PT-04(01) — Consentement adapté au gouvernement du Canada 773
PT-04(02) — Consentement opportun 774
PT-04(03) — Révocation 775
PT-04(400) — Consentement adapté au secteur privé 776
PT-05 — Énoncé de confidentialité 777
PT-05(01) — Énoncés de confidentialité opportuns 778
PT-05(02) — Avis et énoncés de confidentialité 779
PT-06 — Fichiers de renseignements personnels 780
PT-06(01) — Usages et divulgations compatibles 781
PT-06(02) — Fichiers inconsultables 782
PT-07 — Renseignements personnels particulièrement sensibles 783
PT-07(01) — Numéros d'assurance sociale 784
PT-07(02) — Charte canadienne des droits et libertés 785
PT-07(400) — Secteur privé 786
PT-08 — Exigences de couplage de données 787

RA — Évaluation des risques

RA-01 — Politique et procédures d'évaluation des risques 789
RA-01(400) — Évaluations des facteurs relatifs à la vie privée 790
RA-02 — Catégorisation de la sécurité 791
RA-02(01) — Hiérarchisation des répercussions 792
RA-03 — Évaluation des risques 793
RA-03(01) — Évaluation des risques liés à la chaîne d'approvisionnement 794
RA-03(02) — Utilisation du renseignement de toutes sources 795
RA-03(03) — Sensibilisation aux menaces dynamiques 796
RA-03(04) — Cybernanalyse prédictive 797
RA-04 — Mise à jour de l'évaluation des risques 798
RA-05 — Surveillance et analyse des vulnérabilités 799
RA-05(01) — Mise à jour de la capacité des outils 801
RA-05(02) — Mise à jour de la liste de vulnérabilités à analyser 802
RA-05(03) — Étendue et profondeur de la couverture 803
RA-05(04) — Information découvrable 804
RA-05(05) — Accès privilégiés 805
RA-05(06) — Automatisation des analyses de tendances 806
RA-05(07) — Automatisation de la détection et du signalement des composants non autorisés 807
RA-05(08) — Examiner les journaux de vérification historiques 808
RA-05(09) — Tests d'intrusion et analyses 809
RA-05(10) — Corrélation de l'information tirée des analyses 810
RA-05(11) — Programme de divulgation publique 811
RA-06 — Dépistage des contre-mesures de surveillance technique 812
RA-07 — Réponse aux risques 813
RA-08 — Évaluations des facteurs relatifs à la vie privée 814
RA-09 — Analyse de criticité 815
RA-10 — Chasse aux cybermenaces 816

SA — Acquisition sécurisée des systèmes/services

SA-01 — Politique et procédures d'acquisition des systèmes et des services 818
SA-02 — Affectation des ressources 819
SA-03 — Cycle de développement des systèmes 820
SA-03(01) — Gestion de l'environnement de préproduction 821
SA-03(02) — Utilisation de données opérationnelles et en temps réel 822
SA-03(03) — Mise à jour technologique 823
SA-04 — Processus d'acquisition 824
SA-04(01) — Propriétés fonctionnelles des contrôles 825

SA-04(02) — Renseignements relatifs à la conception et à la mise en œuvre des contrôles 826
SA-04(03) — Méthodes, techniques et pratiques en matière de développement 827
SA-04(04) — Attribution de composants à des systèmes 828
SA-04(05) — Configurations de systèmes, de composants et de services 829
SA-04(06) — Utilisation de produits de cybersécurité 830
SA-04(07) — Profils de protection reconnus par le Programme canadien lié aux Critères communs 831
SA-04(08) — Plan de surveillance continue des contrôles 832
SA-04(09) — Fonctions, ports, protocoles et services utilisés 833
SA-04(10) — Utilisation de produits de justificatifs d'identité numériques approuvés 834
SA-04(11) — Système d'enregistrement 835
SA-04(12) — Propriété des données 836
SA-05 — Documentation relative aux systèmes 837
SA-05(01) — Propriétés fonctionnelles des contrôles de sécurité 838
SA-05(02) — Interfaces des systèmes externes servant à la sécurité 839
SA-05(03) — Conception de haut niveau 840
SA-05(04) — Conception de bas niveau 841
SA-05(05) — Code source 842
SA-06 — Restrictions relatives à l'utilisation des logiciels 843
SA-07 — Logiciels installés par les utilisatrices et utilisateurs 844
SA-08 — Principes d'ingénierie de la sécurité et de la protection de la vie privée 845
SA-08(01) — Abstractions claires 846
SA-08(02) — Mécanisme moindre commun 847
SA-08(03) — Modularité et structuration en couches 848
SA-08(04) — Dépendances partiellement hiérarchisées 849
SA-08(05) — Accès avec médiation efficace 850
SA-08(06) — Échange minimal 851
SA-08(07) — Complexité réduite 852
SA-08(08) — Évolutivité sécurisée 853
SA-08(09) — Composants fiables 854
SA-08(10) — Confiance hiérarchique 855
SA-08(11) — Seuil de modification inverse 856
SA-08(12) — Protection hiérarchique 857
SA-08(13) — Éléments de sécurité minimisés 858
SA-08(14) — Droit d'accès minimal 859
SA-08(15) — Autorisation des prédicats 860
SA-08(16) — Fiabilité autonome 861
SA-08(17) — Composition distribuée sécurisée 862
SA-08(18) — Voies de communication fiables 863

SA-08(19) — Protection continue 864
SA-08(20) — Gestion sécurisée des métadonnées 865
SA-08(21) — Auto-analyse 866
SA-08(22) — Responsabilisation et traçabilité 867
SA-08(23) — Valeurs par défaut sécurisées 868
SA-08(24) — Défaillance et reprise sécurisées 869
SA-08(25) — Sécurité économique 870
SA-08(26) — Sécurité des performances 871
SA-08(27) — Sécurité tenant compte du facteur humain 872
SA-08(28) — Sécurité acceptable 873
SA-08(29) — Procédures reproduisibles et documentées 874
SA-08(30) — Rigueur procédurale 875
SA-08(31) — Modification de systèmes sécurisés 876
SA-08(32) — Documentation adéquate 877
SA-08(33) — Minimisation 878
SA-08(400) — Ingénieures et ingénieurs brevetés et agréés 879
SA-09 — Services de systèmes externes 880
SA-09(01) — Évaluations des risques et approbations organisationnelles 881
SA-09(02) — Établissement des fonctions, des ports, des protocoles et des services 882
SA-09(03) — Établissement et maintien d'une relation de confiance avec les fournisseurs de services 883
SA-09(04) — Concordance des intérêts des clients et des fournisseurs 884
SA-09(05) — Lieux de traitement, de stockage et de service 885
SA-09(06) — Clés cryptographiques contrôlées par l'organisation 886
SA-09(07) — Vérification de l'intégrité contrôlée par l'organisation 887
SA-09(08) — Lieu de stockage et de traitement (au Canada) 888
SA-10 — Gestion des configurations par les développeuses et développeurs 889
SA-10(01) — Vérification de l'intégrité des logiciels et des micrologiciels 890
SA-10(02) — Processus de gestion des configurations de rechange 891
SA-10(03) — Vérification de l'intégrité du matériel 892
SA-10(04) — Génération fiable 893
SA-10(05) — Intégrité du mappage pour le contrôle des versions 894
SA-10(06) — Distribution fiable 895
SA-10(07) — Représentantes et représentants de la sécurité et de la protection de la vie privée 896
SA-11 — Évaluations et tests effectués par les développeuses et développeurs 897
SA-11(01) — Analyse statique du code 898
SA-11(02) — Modélisation des menaces et analyses des vulnérabilités 899
SA-11(03) — Vérification indépendante des plans d'évaluation et des preuves 900
SA-11(04) — Revues manuelles du code 901

SA-11(05) — Tests d'intrusion 902
SA-11(06) — Examens de la surface d'attaque 903
SA-11(07) — Vérification de la portée des tests et des évaluations 904
SA-11(08) — Analyse dynamique du code 905
SA-11(09) — Tests de sécurité des applications interactives 906
SA-12 — Protection de la chaîne d'approvisionnement 907
SA-12(01) — Stratégies, outils et méthodes d'acquisition 908
SA-12(02) — Examen des fournisseurs 909
SA-12(03) — Expédition et entreposage sécurisés 910
SA-12(04) — Diversité des fournisseurs 911
SA-12(05) — Limitation des dommages 912
SA-12(06) — Réduction du temps d'approvisionnement 913
SA-12(07) — Évaluation préalable à la sélection, à l'acceptation et à la mise à jour 914
SA-12(08) — Utilisation du renseignement de toutes sources 915
SA-12(09) — Sécurité opérationnelle 916
SA-12(10) — Attestation de l'authenticité et de la non-altérité 917
SA-12(11) — Tests d'intrusion et analyse d'éléments, de processus et des parties prenantes 918
SA-12(12) — Accords interorganisationnels 919
SA-12(13) — Composants de systèmes d'information essentiels 920
SA-12(14) — Identité et traçabilité 921
SA-12(15) — Processus visant à réagir aux faiblesses et aux lacunes 922
SA-13 — Fiabilité 923
SA-14 — Analyse de criticité 924
SA-14(01) — Composants essentiels sans autre source d'approvisionnement viable 925
SA-15 — Processus, normes et outils de développement 926
SA-15(01) — Mesure de la qualité 927
SA-15(02) — Outils de traçabilité des contrôles de sécurité et de protection de la vie privée 928
SA-15(03) — Analyse de criticité 929
SA-15(04) — Modélisation des menaces et analyse des vulnérabilités 930
SA-15(05) — Réduction de la surface d'attaque 931
SA-15(06) — Amélioration continue 932
SA-15(07) — Analyse automatisée des vulnérabilités 933
SA-15(08) — Réutilisation de l'information sur les menaces et les vulnérabilités 934
SA-15(09) — Utilisation de données en temps réel 935
SA-15(10) — Plan d'intervention en cas d'incident 936
SA-15(11) — Système ou composant d'archivage 937
SA-15(12) — Réduction des renseignements personnels 938
SA-15(13) — Syntaxe de journalisation 939

SA-16 — Formation offerte par la développeuse ou le développeur 940
SA-17 — Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur 941
SA-17(01) — Modèle formel de stratégie 942
SA-17(02) — Composants servant à la sécurité 943
SA-17(03) — Correspondance formelle 944
SA-17(04) — Correspondance informelle 945
SA-17(05) — Conception simple 946
SA-17(06) — Structure de mise à l'essai 947
SA-17(07) — Structure relative au droit d'accès minimal 948
SA-17(08) — Orchestration 949
SA-17(09) — Diversité de la conception 950
SA-18 — Résistance au trafiquage et détection 951
SA-18(01) — Multiples phases du cycle de développement de systèmes 952
SA-18(02) — Inspection des systèmes ou des composants 953
SA-19 — Authenticité des composants 954
SA-19(01) — Formation anticontrefaçon 955
SA-19(02) — Contrôle des configurations pour l'entretien et la réparation des composants 956
SA-19(03) — Mise hors service des composants 957
SA-19(04) — Analyse anticontrefaçon 958
SA-20 — Développement sur mesure des composants essentiels 959
SA-21 — Filtrage de sécurité des développeuses et développeurs 960
SA-21(01) — Validation du filtrage de sécurité 961
SA-22 — Composants de systèmes non pris en charge 962
SA-22(01) — Solution de rechange visant à assurer la continuité du soutien 963
SA-23 — Spécialisation 964
SA-24 — Conception aux fins de cyberrésilience 965
SA-400 — Souveraineté et juridiction 966
SA-400(01) — Évaluation des menaces et des risques 967
SA-400(02) — Évaluation d'ordre juridique et contractuel 968
SA-400(03) — Marquage des attributs liés aux processus opérationnels 969
SA-400(04) — Protection des données au repos 970
SA-400(05) — Protection des données en transit 971
SA-400(06) — Protection des données en cours d'utilisation 972
SA-400(07) — Protection contre les contraintes extraterritoriales 973
SA-400(08) — Protection du cycle de vie des activités 974
SA-400(09) — Propriété publique 975

SC — Sécurité des communications et des systèmes

SC-01 — Politique et procédures de protection des systèmes et des communications 977
SC-02 — Séparation des fonctionnalités d'utilisateur et du système 978
SC-02(01) — Interfaces pour les utilisatrices et utilisateurs non privilégiés 979
SC-02(02) — Dissociabilité 980
SC-03 — Isolation des fonctions de sécurité 981
SC-03(01) — Séparation du matériel 982
SC-03(02) — Accès et fonctions de contrôle des flux 983
SC-03(03) — Réduction des fonctionnalités n'ayant pas trait à la sécurité 984
SC-03(04) — Jumelage et cohésion des modules 985
SC-03(05) — Structures en couches 986
SC-04 — Information dans les ressources système partagées 987
SC-04(01) — Niveaux de sécurité 988
SC-04(02) — Traitement multiniveau ou des périodes 989
SC-05 — Protection contre les dénis de service 990
SC-05(01) — Restreindre la capacité de mener des attaques sur d'autres systèmes 991
SC-05(02) — Capacité, bande passante et redondance 992
SC-05(03) — Détection et surveillance 993
SC-06 — Disponibilité des ressources 994
SC-07 — Protection des frontières 995
SC-07(01) — Sous-réseaux séparés physiquement 996
SC-07(02) — Accès public 997
SC-07(03) — Points d'accès 998
SC-07(04) — Services de télécommunications externes 999
SC-07(05) — Refus par défaut – Autorisation par exception 1000
SC-07(06) — Réponse aux échecs reconnus 1001
SC-07(07) — Tunnellisation partagée pour les appareils distants 1002
SC-07(08) — Acheminement du trafic vers des serveurs mandataires authentifiés 1003
SC-07(09) — Restriction du trafic de communications malveillant sortant 1004
SC-07(10) — Prévention de l'exfiltration 1005
SC-07(11) — Restrictions du trafic de communications entrant 1006
SC-07(12) — Protection au niveau de l'hôte 1007
SC-07(13) — Isolation des outils de sécurité, des mécanismes et des composants de soutien 1008
SC-07(14) — Protection contre les connexions physiques non autorisées 1009
SC-07(15) — Accès privilégiés aux réseaux 1010
SC-07(16) — Prévention de la découverte de composants de systèmes 1011
SC-07(17) — Application automatisée des formats de protocoles 1012
SC-07(18) — Fonctionnement à sécurité intégrée 1013
SC-07(19) — Blocage des communications provenant d'hôtes non configurés par l'organisme 1014

SC-07(20) — Isolation dynamique et séparation 1015
SC-07(21) — Isolation des composants de systèmes 1016
SC-07(22) — Sous-réseaux distincts pour la connexion à des domaines de sécurité différents 1017
SC-07(23) — Désactivation de la rétroaction à l'expéditrice ou expéditeur après l'échec de validation d'un protocole 1018
SC-07(24) — Renseignements personnels 1019
SC-07(25) — Connexions à des systèmes de sécurité nationaux non classifiés 1020
SC-07(26) — Connexions à des systèmes de sécurité nationaux classifiés 1021
SC-07(27) — Connexions à des systèmes de sécurité non nationaux non classifiés 1022
SC-07(28) — Connexions aux réseaux publics 1023
SC-07(29) — Séparation des sous-réseaux pour l'isolation des fonctions 1024
SC-08 — Confidentialité et intégrité des transmissions 1025
SC-08(01) — Protection cryptographique 1026
SC-08(02) — Traitement pré-transmission et post-transmission 1027
SC-08(03) — Protection cryptographique pour les éléments complémentaires des messages 1028
SC-08(04) — Dissimulation et distribution aléatoire des communications 1029
SC-08(05) — Système de distribution protégé 1030
SC-09 — Confidentialité des transmissions 1031
SC-10 — Déconnexion du réseau 1032
SC-11 — Chemin de confiance 1033
SC-11(01) — Chemin de communication irréfutable 1034
SC-12 — Établissement et gestion des clés cryptographiques 1035
SC-12(01) — Disponibilité 1036
SC-12(02) — Clés symétriques 1037
SC-12(03) — Clés asymétriques 1038
SC-12(04) — Certificats d'ICP 1039
SC-12(05) — Certificats d'ICP et jetons matériels 1040
SC-12(06) — Contrôle physique des clés 1041
SC-13 — Protection cryptographique 1042
SC-13(01) — Cryptographie homologuée FIPS 1043
SC-13(02) — Cryptographie approuvée par la National Security Agency (NSA) 1044
SC-13(03) — Personnes ne disposant pas des approbations formelles d'accès 1045
SC-13(04) — Signatures numériques 1046
SC-13(400) — Données en transit PROTÉGÉ A 1047
SC-13(401) — Données en transit PROTÉGÉ B 1048
SC-13(402) — Données en transit PROTÉGÉ C 1049
SC-14 — Protection de l'accès public 1050
SC-15 — Applications et dispositifs d'informatique collaborative 1051
SC-15(01) — Déconnexion physique ou logique 1052

SC-15(02) — Blocage du trafic de communications entrant et sortant 1053
SC-15(03) — Désactivation et retrait dans les zones de travail sécurisées 1054
SC-15(04) — Indication explicite des participantes et participants 1055
SC-16 — Transmission des attributs de sécurité et de protection de la vie privée 1056
SC-16(01) — Vérification de l'intégrité 1057
SC-16(02) — Mécanismes anti-usurpation 1058
SC-16(03) — Liaison cryptographique 1059
SC-17 — Certificats d'infrastructure à clé publique 1060
SC-18 — Code mobile 1061
SC-18(01) — Établissement du code inadéquat et application de mesures correctives 1062
SC-18(02) — Acquisition, développement et utilisation 1063
SC-18(03) — Prévention du téléchargement et de l'exécution 1064
SC-18(04) — Prévention de l'exécution automatique 1065
SC-18(05) — Autoriser l'exécution dans les environnements clos seulement 1066
SC-19 — Voix sur IP 1067
SC-19(400) — Conversion de protocole 1068
SC-19(401) — Aucun accès au réseau public 1069
SC-20 — Service sécurisé de résolution de nom ou d'adresse (source faisant autorité) 1070
SC-20(01) — Zones enfants 1071
SC-20(02) — Intégrité et origine des données 1072
SC-21 — Service sécurisé de résolution de nom ou d'adresse (résolveur récursif ou cache) 1073
SC-21(01) — Intégrité et origine des données 1074
SC-22 — Architecture et prestation de services de résolution de nom ou d'adresse 1075
SC-23 — Authenticité des sessions 1076
SC-23(01) — Annulation de la validation des identificateurs de session lors de la fermeture de session 1077
SC-23(02) — Fermetures de session exécutées par les utilisatrices et utilisateurs et affichage de messages 1078
SC-23(03) — Identificateurs de session uniques générés par le système 1079
SC-23(04) — Identificateurs de session uniques avec randomisation 1080
SC-23(05) — Autorités de certification homologuées 1081
SC-24 — Défaillance dans un état connu 1082
SC-25 — Nœuds légers 1083
SC-26 — Leurres 1084
SC-26(01) — Détection de code malveillant 1085
SC-27 — Applications indépendantes des plateformes 1086
SC-28 — Protection de l'information au repos 1087
SC-28(01) — Protection cryptographique 1088
SC-28(02) — Stockage hors ligne 1089

SC-28(03) — Clés cryptographiques 1090
SC-29 — Hétérogénéité 1091
SC-29(01) — Techniques de virtualisation 1092
SC-30 — Dissimulation et détournement 1093
SC-30(01) — Techniques de virtualisation 1094
SC-30(02) — Facteur aléatoire 1095
SC-30(03) — Changement des lieux de traitement et de stockage 1096
SC-30(04) — Information trompeuse 1097
SC-30(05) — Dissimulation des composants de systèmes 1098
SC-31 — Analyse des voies clandestines 1099
SC-31(01) — Test d'exploitabilité des voies clandestines 1100
SC-31(02) — Bande passante maximale 1101
SC-31(03) — Mesure de la bande passante dans les environnements opérationnels 1102
SC-32 — Partitionnement des systèmes 1103
SC-32(01) — Séparation des domaines physiques pour les fonctions privilégiées 1104
SC-33 — Intégrité de la préparation des transmissions 1105
SC-34 — Programmes exécutables non modifiables 1106
SC-34(01) — Dispositif de stockage non inscriptible 1107
SC-34(02) — Protection de l'intégrité et des supports non inscriptibles 1108
SC-34(03) — Protection matérielle 1109
SC-35 — Identification des programmes malveillants externes 1110
SC-36 — Traitement et stockage répartis 1111
SC-36(01) — Techniques de scrutation 1112
SC-36(02) — Synchronisation 1113
SC-37 — Voies d'acheminement hors bande 1114
SC-37(01) — Assurance de la distribution et de la transmission 1115
SC-38 — Sécurité des opérations 1116
SC-39 — Isolation des processus 1117
SC-39(01) — Séparation du matériel 1118
SC-39(02) — Domaine d'exécution distinct pour chaque fil d'exécution 1119
SC-40 — Protection des liaisons sans fil 1120
SC-40(01) — Interférence électromagnétique 1121
SC-40(02) — Atténuation du potentiel de détection 1122
SC-40(03) — Déception des communications par imitation ou par manipulation 1123
SC-40(04) — Identification des paramètres de signaux 1124
SC-400 — Authentification de la source de l'entité 1125
SC-400(01) — Authentification de l'identifiant présumé 1126
SC-400(02) — Signature numérique 1127

SC-400(03) — Mise en œuvre de l'authentification 1128
SC-401 — Systèmes de télécommunications non classifiés dans les installations sécurisées 1129
SC-41 — Accès des ports et des périphériques d'entrée et de sortie 1130
SC-42 — Capacité des capteurs et données 1131
SC-42(01) — Signalement auprès du personnel ou des rôles autorisés 1132
SC-42(02) — Utilisation autorisée 1133
SC-42(03) — Dispositifs interdits d'utilisation 1134
SC-42(04) — Avis de collecte 1135
SC-42(05) — Minimisation de la collecte 1136
SC-42(400) — Désactivation des zones de sécurité et de haute sécurité 1137
SC-43 — Restrictions relatives à l'utilisation 1138
SC-44 — Chambres de détonation 1139
SC-45 — Synchronisation temporelle des systèmes 1140
SC-45(01) — Synchronisation avec une source de temps faisant autorité 1141
SC-45(02) — Deuxième source de temps faisant autorité 1142
SC-46 — Application des stratégies interdomaines 1143
SC-46(400) — Transfert manuel de données 1144
SC-47 — Chemins de communications secondaires 1145
SC-48 — Relocalisation des capteurs 1146
SC-48(01) — Relocalisation dynamique des capteurs ou des capacités de surveillance 1147
SC-49 — Application de la séparation et des stratégies matérielles 1148
SC-50 — Séparation imposée par logiciel et application de la stratégie 1149
SC-51 — Protection matérielle 1150

SI — Intégrité des systèmes et des données

SI-01 — Politique et procédures d'intégrité de l'information et des systèmes 1152
SI-02 — Correction des défauts 1153
SI-02(01) — Gestion centrale 1154
SI-02(02) — État automatisé de la correction des défauts 1155
SI-02(03) — Délais de correction des défauts et repères liés aux mesures correctives 1156
SI-02(04) — Outils automatisés de gestion des correctifs 1157
SI-02(05) — Mises à jour logicielles ou micrologicielles automatiques 1158
SI-02(06) — Retrait des versions antérieures des logiciels et des micrologiciels 1159
SI-02(07) — Analyse des causes fondamentales 1160
SI-03 — Protection contre les programmes malveillants 1161
SI-03(01) — Gestion centrale 1162
SI-03(02) — Mises à jour automatiques 1163
SI-03(03) — Utilisatrices ou utilisateurs non privilégiés 1164
SI-03(04) — Mises à jour effectuées seulement par des utilisatrices et utilisateurs privilégiés 1165

SI-03(05) — Dispositifs de stockage portatifs 1166
SI-03(06) — Tests et vérifications 1167
SI-03(07) — Détection non axée sur les signatures 1168
SI-03(08) — Détection des commandes non autorisées 1169
SI-03(09) — Authentification des commandes à distance 1170
SI-03(10) — Analyse des programmes malveillants 1171
SI-04 — Surveillance des systèmes 1172
SI-04(01) — Système de détection d'intrusion dans l'ensemble du système 1173
SI-04(02) — Outils et mécanismes automatisés aux fins d'analyse en temps réel 1174
SI-04(03) — Intégration d'outils et de mécanismes automatisés 1175
SI-04(04) — Trafic de communications entrant et sortant 1176
SI-04(05) — Alertes générées par le système 1177
SI-04(06) — Restriction des utilisatrices et utilisateurs non privilégiés 1178
SI-04(07) — Réponse automatisée à des événements suspects 1179
SI-04(08) — Protection de l'information de surveillance 1180
SI-04(09) — Mise à l'essai des outils et des mécanismes de surveillance 1181
SI-04(10) — Visibilité des communications chiffrées 1182
SI-04(11) — Analyse des anomalies du trafic de communications 1183
SI-04(12) — Alertes automatisées générées par l'organisation 1184
SI-04(13) — Analyse des modèles de trafic et d'événements 1185
SI-04(14) — Détection d'intrusion sans fil 1186
SI-04(15) — Communications entre un réseau sans fil et un réseau filaire 1187
SI-04(16) — Corrélations entre les résultats des activités de surveillance 1188
SI-04(17) — Connaissance intégrée de la situation 1189
SI-04(18) — Analyse du trafic et exfiltrations masquées 1190
SI-04(19) — Risque envers les personnes 1191
SI-04(20) — Utilisatrice ou utilisateur privilégié 1192
SI-04(21) — Périodes d'essai 1193
SI-04(22) — Services réseau non autorisés 1194
SI-04(23) — Dispositifs au niveau de l'hôte 1195
SI-04(24) — Indicateurs de compromission 1196
SI-04(25) — Optimisation de l'analyse du trafic réseau 1197
SI-05 — Alertes, avis et directives de sécurité 1198
SI-05(01) — Alertes et avis automatisés 1199
SI-06 — Vérification des fonctions de sécurité et de protection de la vie privée 1200
SI-06(01) — Notification des tests de sécurité infructueux 1201
SI-06(02) — Soutien automatisé pour les tests distribués 1202
SI-06(03) — Rapports sur les résultats des vérifications 1203

SI-07 — Intégrité des logiciels, des micrologiciels et de l'information 1204
SI-07(01) — Contrôles d'intégrité 1205
SI-07(02) — Automatisation des avis d'atteinte à l'intégrité 1206
SI-07(03) — Outils de vérification de l'intégrité gérés centralement 1207
SI-07(04) — Emballage avec sceau d'inviolabilité 1208
SI-07(05) — Automatisation des interventions en cas d'atteinte à l'intégrité 1209
SI-07(06) — Protection cryptographique 1210
SI-07(07) — Intégration de la détection et de l'intervention 1211
SI-07(08) — Vérification des capacités en cas d'événements importants 1212
SI-07(09) — Vérification du processus de démarrage 1213
SI-07(10) — Protection des micrologiciels de démarrage 1214
SI-07(11) — Environnements clos aux privilèges restreints 1215
SI-07(12) — Vérification de l'intégrité 1216
SI-07(13) — Exécution de code dans des environnements protégés 1217
SI-07(14) — Code binaire ou exécutable sur machine 1218
SI-07(15) — Authentification du code 1219
SI-07(16) — Limite temporelle sur l'exécution des processus sans supervision 1220
SI-07(17) — Autoprotection des applications d'exécution 1221
SI-08 — Protection contre les pourriels 1222
SI-08(01) — Gestion centrale 1223
SI-08(02) — Mises à jour automatiques 1224
SI-08(03) — Capacité de perfectionnement continu 1225
SI-09 — Restrictions relatives à la saisie d'information 1226
SI-10 — Validation de la saisie d'information 1227
SI-10(01) — Fonction de correction manuelle 1228
SI-10(02) — Examen et résolution des erreurs 1229
SI-10(03) — Comportements prévisibles 1230
SI-10(04) — Chronométrage des interactions 1231
SI-10(05) — Restriction des saisies provenant de sources de confiance et de formats approuvés 1232
SI-10(06) — Prévention de l'injection 1233
SI-11 — Traitement des erreurs 1234
SI-12 — Gestion et conservation de l'information 1235
SI-12(01) — Limitation des éléments liés aux renseignements personnels 1236
SI-12(02) — Réduction des renseignements personnels utilisés aux fins de tests, de formation et de recherche 1237
SI-12(03) — Élimination de l'information 1238
SI-13 — Prévention des pannes prévisibles 1239
SI-13(01) — Transfert des responsabilités d'un composant 1240
SI-13(02) — Limite temporelle sur l'exécution des processus sans supervision 1241

SI-13(03) — Transfert manuel entre les composants 1242
SI-13(04) — Installation des composants passifs et notification 1243
SI-13(05) — Capacité de basculement 1244
SI-14 — Non-persistance 1245
SI-14(01) — Restauration à partir de sources de confiance 1246
SI-14(02) — Information non persistante 1247
SI-14(03) — Connectivité non persistante 1248
SI-15 — Filtrage des sorties d'information 1249
SI-16 — Protection de la mémoire 1250
SI-17 — Procédures de sécurité intégrée 1251
SI-18 — Opérations liées à la qualité des renseignements personnels 1252
SI-18(01) — Soutien à l'automatisation 1253
SI-18(02) — Étiquetage des données 1254
SI-18(03) — Collecte 1255
SI-18(04) — Demandes individuelles 1256
SI-18(05) — Avis de correction ou de suppression 1257
SI-19 — Dépersonnalisation 1258
SI-19(01) — Collecte 1259
SI-19(02) — Archivage 1260
SI-19(03) — Diffusion 1261
SI-19(04) — Suppression, masquage, chiffrement, hachage ou remplacement des identificateurs directs 1262
SI-19(05) — Contrôle de la divulgation de statistiques 1263
SI-19(06) — Confidentialité différentielle 1264
SI-19(07) — Algorithmes et logiciels validés 1265
SI-19(08) — Intrus motivé 1266
SI-20 — Contamination 1267
SI-21 — Actualisation de l'information 1268
SI-22 — Diversité de l'information 1269
SI-23 — Fragmentation de l'information 1270
SI-400 — Station de travail administrative dédiée 1271
SI-400(01) — Station de travail administrative dédiée avec client léger 1272
SI-400(02) — RPV sur réseau privé d'opérateur 1273
SI-400(03) — Réseau local 1274
SI-400(04) — Accès par console seulement 1275
SI-400(05) — Station de travail physique dédiée 1276
SI-400(06) — Accès administratif hétérogène 1277

SR — Gestion des risques liés à la chaîne d'approvisionnement

SR-01 — Politique et procédures de gestion des risques liés à la chaîne d'approvisionnement 1279
SR-02 — Plan de gestion des risques liés à la chaîne d'approvisionnement 1280
SR-02(01) — Établissement d'une équipe de GRCA 1281
SR-03 — Contrôles et processus de la chaîne d'approvisionnement 1282
SR-03(01) — Base d'approvisionnement diversifiée 1283
SR-03(02) — Limitation des dommages 1284
SR-03(03) — Transfert d'exigences à des sous-traitants 1285
SR-04 — Provenance 1286
SR-04(01) — Identité 1287
SR-04(02) — Suivi et localisation 1288
SR-04(03) — Attestation de l'authenticité et de la non-altérité 1289
SR-04(04) — Intégrité de la chaîne d'approvisionnement – Pedigree 1290
SR-05 — Stratégies, outils et méthodes d'acquisition 1291
SR-05(01) — Approvisionnement adéquat 1292
SR-05(02) — Évaluation préalable à la sélection, à l'acceptation, à la modification ou à la mise à jour 1293
SR-06 — Évaluations et examens des fournisseurs 1294
SR-06(01) — Tests et analyse 1295
SR-07 — Sécurité opérationnelle de la chaîne d'approvisionnement 1296
SR-08 — Ententes de notification 1297
SR-09 — Résistance au trafiquage et détection 1298
SR-09(01) — Phases multiples du cycle de développement de systèmes 1299
SR-10 — Inspection des systèmes ou des composants 1300
SR-11 — Authenticité des composants 1301
SR-11(01) — Formation anticontrefaçon 1302
SR-11(02) — Contrôle des configurations pour l'entretien et la réparation des composants 1303
SR-11(03) — Analyse anticontrefaçon 1304
SR-12 — Mise hors service des composants 1305

AC

Gestion des droits d'accès aux systèmes et données

Access Control

AC-01 — Politique et procédures de contrôle d'accès (PaF-)

Énoncés :

a. Développer, consigner et diffuser à [Affectation : personnel ou rôles définis par l'organisation]
- **1.** une politique de contrôle d'accès [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, à la jurisprudence, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables
- **2.** des procédures pour faciliter la mise en oeuvre de la politique de contrôle d'accès et des contrôles d'accès connexes

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées au contrôle d'accès

c. Passer en revue et mettre à jour, par rapport au contrôle d'accès :
- **1.** la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]
- **2.** les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Paramètres :

a. tout le personnel a.
- **1.** organisationnel

b. chef de la sécurité de l'information organisationnelle c.
- **1.** triennale; lors de changements significatifs c.
- **2.** annuelle; lors de changements significatifs

Responsable : OP

Discussion :

Les politiques de contrôle d'accès abordent les contrôles de la famille AC qui ont été mis en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les fonctions de sécurité et de protection de la vie privée collaborent à l'élaboration de la politique et des procédures de contrôle d'accès. En règle générale, les politiques et les cadres liés au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin pour des politiques et des procédures propres à la mission ou au système. Les politiques de contrôle d'accès peuvent être intégrées au cadre général de la sécurité et de la protection de la vie privée ou, inversement, être représentées par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour la sécurité et la protection de la vie privée, pour les processus opérationnels ou liés à la mission, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les procédures liées à la protection de la vie privée ne devraient pas avoir un caractère ad hoc. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures de contrôle d'accès comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, à la jurisprudence, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.

AC-02 — Gestion des comptes (PaF-) (Obligatoire)

Énoncés :

a. Définir et consigner les types de comptes permis et dont l'utilisation est interdite dans le système
b. Affecter des gestionnaires de comptes et des responsables des données
c. Exiger [Affectation : prérequis et critères ayant été définis par l'organisation] en ce qui concerne l'appartenance au groupe et au rôle
d. Préciser :
- **1.** les utilisatrices et utilisateurs autorisés du système;
- **2.** les membres des groupes et des rôles;
- **3.** les autorisations d'accès (par exemple, droits d'accès ou privilèges) et [Affectation : attributs définis par l'organisation (selon les besoins)] pour chaque compte

e. Obtenir l'approbation de [Affectation : personnel ou rôles définis par l'organisation] pour les demandes de création de comptes
f. Créer, activer, modifier, désactiver et retirer les comptes du système conformément aux [Affectation : politiques, procédures, conditions préalables et critères définis par l'organisation]
g. Surveiller l'utilisation des comptes
h. Aviser les gestionnaires de compte et [Affectation : personnel ou rôles définis par l'organisation] dans :
- **1.** [Affectation : délais définis par l'organisation] lorsque les comptes ne sont plus requis ou en état de latence
- **2.** [Affectation : délais définis par l'organisation] lorsque les utilisatrices et utilisateurs quittent leur emploi ou sont transférés
- **3.** [Affectation : délais définis par l'organisation] lorsque l'utilisation du système ou le besoin de connaître d'une personne change

i. Autoriser l'accès au système en fonction de ce qui suit :
- **1.** une autorisation d'accès valide
- **2.** l'utilisation prévue du système
- **3.** [Affectation : attributs définis par l'organisation (selon les besoins)]

j. Examiner périodiquement les comptes pour s'assurer qu'ils sont conformes aux exigences en matière de gestion des comptes tous les [Affectation : fréquence définie par l'organisation]
k. Établir et mettre en oeuvre un processus de changement des authentifiants de compte partagé ou de groupe (s'ils sont déployés) lorsque des utilisatrices et utilisateurs sont retirés du groupe
l. Aligner les processus de gestion des comptes avec les processus de cessation d'emploi et de mutation de personnel

Paramètres :

c. à définir par l'organisme d.
- **3.** à définir par l'organisme

e. détenteur de l'actif informationnel
f. à définir par l'organisme
h. détenteur de l'actif informationnel h.
- **1.** à définir par l'organisme en fonction du contexte h.
- **2.** à définir par l'organisme en fonction du contexte h.
- **3.** à définir par l'organisme en fonction du contexte i.
- **3.** à définir par l'organisme

j. au minimum 1 fois par année

Responsable : OP

Date limite de mise en oeuvre : 2021-06-30

Discussion :

Les types de comptes de système comprennent les comptes individuels, partagés, temporaires, anonymes ou d'invité, de groupe, de système, d'urgence, de développeuse ou développeur et de service. L'identification des utilisatrices et utilisateurs autorisés du système et la spécification des privilèges d'accès reflètent les exigences que l'on retrouve dans d'autres contrôles de sécurité et de protection de la vie privée. Les utilisatrices et utilisateurs nécessitant des privilèges administratifs sur les comptes du système font l'objet d'un examen plus approfondi de la part des responsables du personnel de l'organisation pour l'approbation des comptes et de l'accès privilégié. Il peut s'agir entre autres de la ou du propriétaire du système, de la mission ou des activités, d'une ou un cadre supérieur de la gouvernance en matière de sécurité du ministère, d'une ou un responsable des données ou d'une haute ou un haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée. Les types de comptes que les organisations peuvent interdire en raison d'un risque de sécurité accru incluent les comptes partagés, anonymes, temporaires, de groupe, d'urgence et d'invité. Dans la mesure où l'accès comporte des renseignements personnels, les cadres supérieures et supérieurs responsables de la sécurité et de la protection de la vie privée collaborent avec la ou le responsable des données pour déterminer les conditions particulières de l'appartenance aux groupes et aux rôles, identifier les utilisatrices et utilisateurs autorisés,

l'appartenance aux groupes et aux rôles, et les autorisations d'accès pour chaque compte, ainsi que créer, ajuster ou supprimer les comptes du système conformément aux stratégies organisationnelles. Les stratégies peuvent comprendre de l'information telle que les dates d'expiration des comptes ou d'autres facteurs qui déclenchent la désactivation des comptes. Les organisations peuvent choisir de définir les droits d'accès ou d'autres attributs en fonction du compte, du type de compte ou d'une combinaison des deux. Les exemples d'autres attributs requis pour autoriser l'accès incluent les restrictions en fonction du moment de la journée, du jour de la semaine et du point d'origine. Au moment de définir les autres attributs des comptes de système, les organisations considèrent les exigences liées au système et celles liées à la mission ou aux activités. Si les organisations ne considèrent pas ces facteurs, la disponibilité des systèmes risque d'en subir les conséquences. Les comptes temporaires et d'urgence devraient être utilisés à court terme. Les organisations établissent des comptes temporaires dans leurs procédures standard d'activation de compte s'il convient d'utiliser les comptes à court terme et que leur activation n'est pas urgente. Les organisations établissent des comptes d'urgence à la suite de situations de crise et lorsqu'il faut activer des comptes rapidement. Par conséquent, l'activation de compte d'urgence risque de contourner les processus standard d'autorisation de compte. Il ne faut pas confondre les comptes temporaires et d'urgence avec les comptes utilisés peu fréquemment, notamment les comptes d'ouverture de session locaux utilisés pour réaliser des tâches particulières ou lorsque les ressources réseau ne sont pas disponibles (communément appelés des comptes de dernier recours). Ces comptes demeurent activés et ne sont pas assujettis aux dates de retrait ou de désactivation automatique. Les conditions de désactivation des comptes peuvent inclure ce qui suit : lorsque les comptes temporaires, les comptes d'urgence ou les comptes partagés ou de groupe ne sont plus requis; ou lorsque des utilisatrices ou utilisateurs quittent leur poste ou font l'objet d'un transfert. Changer des authentifiants partagés ou de groupe vise à s'assurer que d'anciennes ou anciens membres du groupe ne puissent pas conserver des accès au compte partagé ou de groupe. Les utilisatrices et utilisateurs de certains types de comptes de système pourraient être appelés à suivre une formation spécialisée.

AC-02(01) — Gestion automatisée des comptes système (PbM-)

Énoncés :

Appuyer la gestion des comptes système au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Paramètres :

à définir par l'organisme

Responsable : OP

Discussion :

La gestion automatisée des comptes système comprend le recours à des mécanismes automatisés pour : • créer, activer, modifier, désactiver et supprimer les comptes; • aviser les gestionnaires des comptes lorsqu'un compte est créé, activé, modifié, désactivé ou supprimé, ou lorsque des utilisatrices ou utilisateurs sont congédiés ou transférés; • surveiller l'usage du compte de système; et signaler une utilisation irrégulière de celui-ci. Les mécanismes automatisés peuvent comprendre des fonctions de systèmes internes ainsi que des notifications téléphoniques, de courriels et de messages texte.

AC-02(02) — Gestion automatisée des comptes temporaires et des comptes d’urgence (PbM-)

Énoncés :

Automatiquement, le système [Sélection (un choix) : supprime; désactive] les comptes temporaires et d’urgence après [Affectation : délais définis par l’organisation pour chaque type de compte].

Responsable : Aucun

Discussion :

La gestion de comptes temporaires et d’urgence comprend la suppression ou la désactivation automatique de ces comptes après un délai prédéfini plutôt qu’à la convenance de l’administratrice ou administrateur de système. Une suppression ou une désactivation automatique des comptes assure une mise en œuvre plus cohérente.

AC-02(03) — Désactivation des comptes (PaF-)

Énoncés :

Désactiver les comptes dans [Affectation : délais définis par l'organisation] lorsque les comptes :
a. ont expiré
b. ne sont plus associés à une utilisatrice ou un utilisateur, ou à une personne
c. contreviennent à une politique organisationnelle
d. sont inactifs depuis [Affectation : délais définis par l'organisation]

Responsable : Aucun

Discussion :

Désactiver des comptes expirés, inactifs ou comportant des anomalies soutient les concepts du principe de droit d'accès et du principe de fonctionnalité minimale qui permettent de réduire la surface d'attaque du système.

AC-02(04) — Opérations automatisées de vérification (---)

Énoncés :

Vérification automatique des activités de création, de modification, d'activation, de désactivation et de retrait des comptes.

Responsable : Aucun

Discussion :

Les dossiers de vérification de gestion des comptes sont définis conformément au contrôle AU-02 et ils sont examinés, analysés et signalés conformément au contrôle AU-06.

AC-02(05) — Fermeture de session en cas d'inactivité (---)

Énoncés :

Exiger des utilisatrices et utilisateurs qu'ils ferment leur session après [Affectation : délai d'inactivité prévu ou description du moment de la fermeture de session définis par l'organisation].

Responsable : Aucun

Discussion :

La fermeture de session en cas d'inactivité peut être basée sur des comportements ou sur des stratégies, et nécessite que les utilisatrices et utilisateurs effectuent une opération physique afin de fermer leur session s'ils prévoient d'être inactifs sur le système pendant une période dépassant la période définie. L'application automatique de la fermeture de session en cas d'inactivité est abordée dans le contrôle AC-11.

AC-02(06) — Gestion dynamique des droits d’accès (---)

Énoncés :

Mettre en œuvre des [Affectation : capacités de gestion dynamique des droits d’accès définies par l’organisation].

Responsable : Aucun

Discussion :

Contrairement aux approches de contrôle d’accès qui emploient des comptes statiques et des droits d’accès d’utilisatrice et utilisateur prédéfinis, les approches de contrôle d’accès dynamique reposent sur des décisions d’exécution de contrôle d’accès facilitées par une gestion dynamique des droits d’accès, comme le contrôle d’accès basé sur les attributs. Quoique les identités d’utilisateur demeurent relativement constantes au fil du temps, les droits d’accès changent généralement plus fréquemment selon les exigences de la mission et des opérations ainsi que selon les besoins opérationnels de l’organisation. Un exemple de la gestion dynamique des droits d’accès est la révocation immédiate des droits d’accès des utilisatrices et utilisateurs, par opposition à forcer les utilisatrices et utilisateurs à mettre fin à leur session et à en ouvrir une nouvelle pour refléter les changements de droits d’accès. La gestion dynamique des droits d’accès peut également comprendre les mécanismes qui modifient les droits d’accès des utilisatrices et utilisateurs en fonction de règles dynamiques, au lieu de modifier les profils d’utilisatrice ou utilisateur particuliers. Des exemples peuvent comprendre des ajustements automatiques des droits d’accès si les utilisatrices et utilisateurs travaillent en dehors de leurs heures normales de travail, leurs fonctions ou affectations changent, ou si les systèmes sont dans des situations contraignantes ou de maintenance d’urgence. La gestion dynamique des droits d’accès peut également inclure les effets des changements de droits d’accès, lorsqu’il y a des changements aux clés de chiffrement utilisées pour les communications.

AC-02(07) — Comptes d'utilisateur privilégiés (Nc--)

Énoncés :

a. Établir et administrer des comptes d'utilisateur privilégiés conformément à un [Sélection (un choix) : plan de contrôle d'accès basé sur les rôles; plan d'accès basés sur les attributs]
b. Surveiller les attributions de rôles privilégiés ou d'attributs
c. Surveiller les changements aux rôles ou aux attributs
d. Révoquer l'accès lorsque les attributions de rôles privilégiés ou d'attributs ne conviennent plus

Responsable : Aucun

Discussion :

Les rôles privilégiés sont des rôles définis par l'organisation qui sont attribués aux utilisatrices et utilisateurs pour leur permettre d'exécuter certaines fonctions de sécurité qu'ils ne sont pas habituellement autorisés à exécuter. Les rôles privilégiés comprennent la gestion des clés, la gestion des comptes, l'administration des bases de données, l'administration des réseaux et des systèmes, et l'administration Web. Un plan d'accès basé sur les rôles regroupe l'accès et les droits d'accès permis au système par rôle. À l'inverse, un plan d'accès basé sur des attributs précise les droits d'accès au système en fonction des attributs.

AC-02(08) — Gestion dynamique des comptes (---)

Énoncés :

Créer, activer, gérer et désactiver [Affectation : comptes du système définis par l'organisation] de manière dynamique.

Responsable : Aucun

Discussion :

Les approches permettant de créer, d'activer, de gérer et de désactiver de manière dynamique les comptes du système reposent sur l'attribution automatique des comptes au moment de leur exécution en temps réel dans le cas des entités jusque-là inconnues. Les organisations planifient la gestion, la création, l'activation et la désactivation dynamiques de comptes de système en établissant des relations de confiance, des règles opérationnelles et des mécanismes avec les autorités appropriées pour valider les autorisations et droits d'accès connexes.

AC-02(09) — Restrictions liées à l'utilisation de comptes partagés et de groupe (---)

Énoncés :

Autoriser uniquement l'utilisation des comptes partagés et de groupe qui répondent aux [Affectation : conditions relatives à l'établissement de comptes partagés et de groupe définies par l'organisation].

Responsable : Aucun

Discussion :

Avant d'autoriser l'utilisation de comptes partagés ou de groupe, les organisations tiennent compte du risque accru engendré par le manque de responsabilisation associé à de tels comptes.

AC-02(10) — Changement de justificatifs d'identité de comptes partagés et de groupe (---)

Énoncés :

Annulé : Intégré au contrôle AC-02.

Responsable : Aucun

AC-02(11) — Conditions d'utilisation (---)

Énoncés :

Appliquer [Affectation : circonstances et/ou conditions d'utilisation définies par l'organisation] aux [Affectation : comptes du système définis par l'organisation].

Responsable : Aucun

Discussion :

Le fait de préciser et d'appliquer des conditions d'utilisation aide à appliquer le principe de droit d'accès minimal, à accroître l'imputabilité de l'utilisatrice ou utilisateur et à permettre une surveillance efficace des comptes. La surveillance des comptes implique que des alertes sont générées si l'utilisation d'un compte contrevient aux paramètres organisationnels. Les organisations peuvent décrire les conditions ou les circonstances particulières selon lesquelles les comptes du système peuvent être utilisés, comme en limitant l'utilisation à certains jours de la semaine, à certaines heures du jour ou à une durée précise.

AC-02(12) — Surveillance des comptes pour utilisation irrégulière (Nc--)

Énoncés :

a. Surveiller les comptes de système afin de détecter [Affectation : utilisation irrégulière définie par l'organisation]
b. Signaler une utilisation irrégulière des comptes de système à [Affectation : personnel ou rôles définis par l'organisation]

Responsable : Aucun

Discussion :

L'utilisation irrégulière peut comprendre l'accès à des systèmes à des heures précises de la journée ou à partir d'endroits qui ne correspondent pas aux habitudes d'utilisation régulières des employées et employés. La surveillance des comptes pour utilisation irrégulière peut révéler un comportement malhonnête de certaines personnes ou une attaque en cours. La surveillance des comptes peut créer par inadvertance des risques pour ce qui touche les renseignements personnels étant donné que les données recueillies pour repérer une utilisation irrégulière peuvent exposer de l'information précédemment inconnue concernant le comportement de personnes. Les organisations évaluent et documentent les risques pour les renseignements personnels en surveillant les comptes afin de déceler une utilisation irrégulière en ce qui a trait à l'évaluation des facteurs relatifs à la vie privée (EFVP), et prennent des décisions conformément à leur plan du programme de protection de la vie privée.

AC-02(13) — Désactivation des comptes des personnes à risque élevé (---)

Énoncés :

Désactiver des comptes du personnel dans les [Affectation : délais définis par l'organisation] après la découverte des [Affectation : risques importants définis par l'organisation].

Responsable : Aucun

Discussion :

Les utilisatrices et utilisateurs qui présentent un risque important pour la sécurité et/ou l'atteinte à la vie privée comprennent les personnes pour lesquelles des preuves fiables indiquent l'intention d'utiliser un accès autorisé aux systèmes afin de causer des dommages ou de permettre à des adversaires de causer des dommages. Ces dommages comprennent des incidences négatives aux activités et aux biens organisationnels, aux employées et employés, à d'autres organisations ou au gouvernement. Une collaboration étroite entre les administratrices et administrateurs de système, le personnel juridique, les gestionnaires des ressources humaines et les autorités responsables est essentielle à la désactivation des comptes système des personnes présentant un risque élevé.

AC-03 — Application de l’accès (---)

Énoncés :

Appliquer les autorisations approuvées pour l’accès logique à l’information et aux ressources système conformément aux stratégies de contrôle d’accès applicables.

Responsable : Aucun

Discussion :

Les stratégies de contrôle d’accès contrôlent ou documentent l’accès entre les entités ou sujets actifs (c’est-à-dire les utilisatrices et utilisateurs ou les processus système agissant en leur nom) et les entités ou objets passifs (c’est-à-dire les dispositifs, les fichiers, les documents et les domaines) dans les systèmes organisationnels. En plus de consigner et d’appliquer l’accès autorisé au système et de reconnaître que les systèmes peuvent héberger de nombreuses applications et services à l’appui des fonctions liées à la mission et aux activités, les mécanismes d’application de l’accès peuvent également servir aux applications et aux services en vue de renforcer la sécurité et la protection de la vie privée de l’information. Contrairement aux contrôles d’accès logiques qui sont mis en oeuvre dans le système, les contrôles d’accès physiques relèvent des contrôles appartenant à la famille Protection physique et environnementale (PE).

AC-03(01) — Restriction de l’accès aux fonctions privilégiées (---)

Énoncés :

Annulé : Intégré au contrôle AC-06.

Responsable : Aucun

AC-03(02) — Double autorisation (---)

Énoncés :

Appliquer une double autorisation pour [Affectation : commandes privilégiées ou autres mesures définies par l'organisation].

Responsable : Aucun

Discussion :

La double autorisation, également appelée le contrôle par deux personnes, réduit le risque lié aux menaces internes. L'exécution des mécanismes de double autorisation exige l'approbation de deux personnes autorisées. Pour réduire le risque de collusion, les organisations considèrent la rotation des tâches à double autorisation. Les organisations tiennent compte du risque associé à la mise en oeuvre de mécanismes de double autorisation lorsqu'il faut agir immédiatement pour assurer la sécurité publique et environnementale.

AC-03(03) — Contrôle d'accès obligatoire (---)

Énoncés :

Appliquer la [Affectation : stratégie de contrôle d'accès obligatoire définie par l'organisation] à l'ensemble de sujets et objets couverts qui sont définis dans la stratégie, quand la stratégie :
a. est appliquée de façon uniforme pour tous les sujets et objets dans le système
b. précise qu'un sujet ayant reçu l'accès à l'information est contraint :
1. d'acheminer l'information à des sujets ou à des objets non autorisés
2. d'octroyer ses droits d'accès à d'autres sujets
3. de changer un ou plusieurs attributs de sécurité (précisés par la stratégie) pour des sujets, des objets, le système ou des composants du système
4. de choisir les attributs de sécurité et les valeurs d'attribut (précisés par la stratégie) qui seront associés aux objets nouvellement créés ou modifiés
5. de changer les règles régies par le contrôle d'accès
c. précise que les [Affectation : sujets définis par l'organisation] peuvent accorder explicitement [Affectation : droits d'accès définis par l'organisation], de façon à ce qu'ils ne soient pas limités par les contraintes ci-dessus

Responsable : Aucun

Discussion :

Le contrôle d'accès obligatoire est un type de contrôle non discrétionnaire des accès. Les stratégies de contrôle d'accès obligatoire limitent les opérations que peuvent exécuter les sujets par rapport à l'information obtenue des objets auxquels l'accès leur a déjà été accordé. C'est ce qui empêche les sujets de transmettre de l'information à des sujets ou à des objets non autorisés. Les stratégies de contrôle d'accès obligatoire limitent les opérations que peuvent exécuter les sujets en ce qui a trait à la propagation des privilèges de contrôle d'accès, à savoir qu'un sujet ayant un privilège ne peut pas le transmettre à d'autres sujets. La stratégie est appliquée de façon uniforme pour tous les sujets et objets que contrôle le système. Autrement, la politique de contrôle d'accès peut être contournée. Cette application est assurée par une mise en oeuvre qui répond au concept de contrôleur de référence décrit dans le contrôle AC-
25. La stratégie est délimitée par les frontières du système (c'est-à-dire une fois que l'information sort du contrôle du système, des moyens additionnels seront peut-être nécessaires pour s'assurer que les contraintes imposées sur l'information demeurent en vigueur). Les droits d'accès accordés aux sujets de confiance décrits ci-dessus sont conformes au concept du droit d'accès minimal (voir AC-06). Les sujets de confiance reçoivent seulement les droits d'accès minimaux qui sont nécessaires afin de satisfaire les besoins de l'organisation liés à la mission et aux opérations associées à la stratégie ci-dessus. Le contrôle s'applique particulièrement lorsqu'il existe un mandat qui établit une politique concernant l'accès à l'information protégée ou classifiée, où certaines utilisatrices ou certains utilisateurs du système ne sont pas autorisés à accéder à toute l'information sensible ou classifiée contenue dans le système d'information. Un contrôle d'accès obligatoire peut être appliqué en conjonction avec le contrôle d'accès discrétionnaire décrit dans le contrôle AC-03(04). Un sujet dont les activités sont limitées par les stratégies d'accès obligatoire peut quand même être en mesure de réaliser ses activités en vertu des contraintes moins rigoureuses du contrôle AC-03(04), mais les stratégies d'accès obligatoire ont préséance sur les contraintes moins rigoureuses du contrôle AC-03(04). Par exemple, bien qu'une stratégie de contrôle d'accès obligatoire impose une contrainte empêchant un sujet de transmettre de l'information à un sujet menant des activités à un niveau d'incidence ou de classification différent, le contrôle AC-03(04) permet au sujet de transmettre de l'information à des sujets ayant le même niveau d'incidence ou de classification que celui du sujet. Des exemples de stratégies de contrôle d'accès obligatoire comprennent la stratégie Bell-LaPadula pour protéger la confidentialité de l'information et la stratégie Biba pour protéger l'intégrité de l'information.

AC-03(04) — Contrôle d'accès discrétionnaire (---)

Énoncés :

Appliquer la [Affectation : stratégie de contrôle d'accès discrétionnaire définie par l'organisation] aux ensembles de sujets et d'objets couverts qui ont été précisés dans la stratégie, et quand la stratégie précise qu'un sujet à qui l'accès à l'information a été accordé peut réaliser l'un ou l'autre des aspects suivants :
a. acheminer l'information à d'autres sujets ou objets
b. octroyer ses droits d'accès à d'autres sujets
c. changer des attributs de sécurité de sujets, d'objets, du système ou de composants du système
d. choisir les attributs de sécurité qui seront associés aux objets nouvellement créés ou modifiés; par le contrôle d'accès
e. changer les règles régies par le contrôle d'accès

Responsable : Aucun

Discussion :

Lors de la mise en oeuvre des stratégies de contrôle d'accès discrétionnaire, les sujets ne sont pas limités quant aux opérations qu'ils peuvent exécuter par rapport à l'information de l'organisation à laquelle ils ont déjà reçu l'accès. Toutefois, ils sont limités quant à l'utilisation ou la divulgation de renseignements personnels. Un avis d'utilisation est fourni à la personne au point de collecte et les seules utilisations autorisées de l'information sont communiquées dans un énoncé de confidentialité, et les limites d'utilisation sont détaillées dans la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. Pour les dossiers opérationnels, les sujets ayant déjà obtenu l'accès à l'information sont autorisés à transmettre (c'est-à-dire qu'ils peuvent choisir de transmettre) l'information à d'autres sujets ou à d'autres objets. Un contrôle d'accès discrétionnaire peut être appliqué en conjonction avec le contrôle d'accès obligatoire décrit dans les contrôles AC-03(03) et AC-03(15). Un sujet dont les activités sont limitées par les stratégies de contrôle d'accès obligatoire peut toujours effectuer ses activités selon les contraintes moins rigoureuses du contrôle d'accès discrétionnaire. Par conséquent, bien que le contrôle AC-03(03) impose des contraintes empêchant un sujet de transmettre de l'information à un sujet travaillant à un niveau d'incidence ou de classification différent, le contrôle AC-03(04) permet au sujet de transmettre de l'information à des sujets ayant le même niveau d'incidence ou de classification que celui du sujet. La politique est délimitée par le système. Une fois que l'information sort du contrôle du système, des moyens additionnels seront peut-être nécessaires pour s'assurer que les contraintes imposées demeurent en vigueur. Alors que les définitions traditionnelles du contrôle d'accès discrétionnaire exigeaient le contrôle d'accès basé sur l'identité, il n'est pas nécessaire d'appliquer cette limite à l'utilisation du contrôle d'accès discrétionnaire.

AC-03(05) — Information pertinente en matière de sécurité (---)

Énoncés :

Empêcher l'accès à [Affectation : information pertinente en matière de sécurité définie par l'organisation] sauf lorsque le système est en état de non-fonctionnement sécurisé.

Responsable : Aucun

Discussion :

L'information pertinente en matière de sécurité désigne l'information dans les systèmes susceptibles d'influer sur l'exécution des fonctions de sécurité ou sur la prestation des services de sécurité, de telle façon qu'elle nuirait à l'application des stratégies de sécurité du système ou à la séparation du code et des données. L'information liée à la sécurité comprend les listes de contrôle d'accès, les règles de filtrage pour les routeurs et les pare-feu, les paramètres de configuration pour les services de sécurité et l'information de gestion des clés cryptographiques. Les systèmes dans un état de non-fonctionnement sécurisé comprennent également les périodes où ils n'effectuent aucun traitement lié à la mission ou aux opérations, comme lorsqu'un système a été mis hors ligne aux fins de maintenance, de dépannage, d'amorçage ou d'arrêt.

AC-03(06) — Protection de l'information du système, des utilisatrices et utilisateurs (---)

Énoncés :

Annulé : Intégré aux contrôles MP-04 et SC-28.

Responsable : Aucun

AC-03(07) — Contrôle d’accès basé sur les rôles (---)

Énoncés :

Appliquer une stratégie de contrôle d’accès basé sur les rôles à des sujets et objets définis, et il contrôle l’accès en fonction des [Affectation : rôles et du personnel autorisé à assumer ces rôles définis par l’organisation].

Responsable : Aucun

Discussion :

Le contrôle d’accès basé sur les rôles (RBAC pour Role-Based Access Control) est une stratégie de contrôle d’accès qui applique l’accès à des objets et à des fonctions de système en se basant sur le rôle défini (par exemple, les fonctions) du sujet. Les organisations peuvent créer des rôles précis selon les fonctions du poste et les autorisations (c’est-à-dire les droits d’accès) nécessaires en vue d’exécuter les opérations requises sur les systèmes associés aux rôles définis par l’organisation. Lorsque des rôles particuliers sont attribués aux utilisatrices et utilisateurs, ceux-ci héritent des autorisations ou des privilèges définis pour ces rôles. Le RBAC simplifie l’administration des droits d’accès des organisations puisque les droits d’accès ne sont pas attribués directement à chaque utilisatrice ou utilisateur (ce qui peut représenter beaucoup d’utilisatrices et utilisateurs), mais plutôt à des rôles. Le RBAC peut également accroître les risques liés à la protection de la vie privée et à la sécurité si des personnes à qui un rôle a été attribué obtiennent l’accès à de l’information qui excède ce dont elles ont besoin pour appuyer les fonctions liées à la mission et aux activités de l’organisation. Le RBAC peut être mis en oeuvre de façon discrétionnaire ou non. Pour les organisations mettant en oeuvre le RBAC avec des contrôles d’accès non discrétionnaire, les exigences du contrôle AC-03(03) définissent la portée des sujets et des objets couverts par la stratégie.

AC-03(08) — Révocation des autorisations d’accès (---)

Énoncés :

Appliquer la révocation des autorisations d’accès à la suite de changements apportés aux attributs de sécurité des sujets et des objets en fonction des [Affectation : règles régissant le moment de la révocation des autorisations d’accès définies par l’organisation].

Responsable : Aucun

Discussion :

La révocation des règles d’accès peut être différente selon les types d’accès révoqué. Par exemple, si un sujet (c’est-à-dire une utilisatrice ou un utilisateur, ou un processus agissant au nom d’une utilisatrice ou d’un utilisateur) est retiré d’un groupe, il se peut que l’accès ne soit pas révoqué jusqu’à ce que l’objet soit ouvert de nouveau ou jusqu’à ce que le sujet tente d’accéder de nouveau à l’objet. La révocation fondée sur les changements aux étiquettes de sécurité peut entrer en vigueur sur-le-champ. Les organisations fournissent d’autres approches pour l’application immédiate des révocations dans les cas où les systèmes sont incapables d’offrir cette capacité si elle est obligatoire.

AC-03(09) — Diffusion contrôlée (---)

Énoncés :

Diffuser de l'information hors du système uniquement si :
a. le [Affectation : système ou composant du système désigné par l'organisation] destinataire fournit les [Affectation : contrôles définis par l'organisation]
b. les [Affectation : contrôles définis par l'organisation] sont utilisés pour valider la pertinence de l'information désignée à des fins de diffusion

Responsable : Aucun

Discussion :

Les organisations peuvent uniquement protéger l'information directement lorsqu'elle réside dans le système. Des contrôles additionnels pourraient être nécessaires pour veiller à ce que l'information organisationnelle soit protégée de façon adéquate une fois qu'elle a été transmise hors du système. Dans les cas où le système est incapable de déterminer la convenance des mesures de protection fournies par des entités externes, à titre de contrôle d'atténuation, les organisations établissent, en fonction des procédures, si les systèmes externes fournissent des contrôles adéquats. Les moyens servant à déterminer la convenance des contrôles assurée par les systèmes externes comprennent la conduite d'évaluations périodiques (inspections ou tests), l'établissement d'ententes entre l'organisation et les organisations homologues ou d'autres processus. Les mécanismes qu'utilisent les entités externes pour protéger l'information reçue peuvent être différents de ceux qu'emploie l'organisation, mais ils doivent être suffisants afin de statuer sur la stratégie sur la sécurité et la protection de la vie privée pour protéger l'information et la vie privée des individus. La diffusion contrôlée de l'information exige que les systèmes mettent en oeuvre des mécanismes techniques ou procéduraux pour valider l'information avant de la diffuser à des systèmes externes. Par exemple, si le système transmet l'information à un autre système contrôlé par une autre organisation, les mécanismes techniques servent à confirmer que les attributs de sécurité et de protection de la vie privée associés à l'information exportée sont appropriés pour le système destinataire. Autrement, si le système transmet de l'information à une imprimante dans un espace contrôlé par l'organisation, des mécanismes procéduraux peuvent être mis en oeuvre pour s'assurer que seules les personnes autorisées peuvent accéder à l'imprimante.

AC-03(10) — Dérogation vérifiée aux mécanismes de contrôle d'accès (---)

Énoncés :

Utiliser une dérogation vérifiée aux mécanismes automatisés de contrôle d'accès en vertu des [Affectation : conditions définies par l'organisation] par les [Affectation : rôles définis par l'organisation].

Responsable : Aucun

Discussion :

Dans certains cas, comme lorsque la vie humaine est menacée ou qu'un événement menace la capacité de l'organisation à mener des missions prioritaires ou des fonctions opérationnelles, une fonction de correction pour les mécanismes de contrôle d'accès peut s'avérer nécessaire. Les fonctions de correction sont définies par les organisations et utilisées seulement dans des cas restreints. Les événements vérifiables sont définis dans le contrôle AU-
02. Les enregistrements de vérification sont générés dans le contrôle AU-12.

AC-03(11) — Accès restreint à des types d'information spécifiques (---)

Énoncés :

Accès restreint à des référentiels contenant des [Affectation : types d'information définis par l'organisation].

Responsable : Aucun

Discussion :

Limiter l'accès à de l'information spécifique permet d'offrir une certaine souplesse quant au contrôle d'accès de types spécifiques d'information dans un système. Par exemple, un accès basé sur les rôles peut être employé pour permettre l'accès à seulement un type spécifique de renseignements personnels dans une base de données plutôt que d'autoriser l'accès à l'intégralité de la base de données. D'autres exemples comprennent de limiter l'accès à des clés cryptographiques, à de l'information d'authentification et à de l'information sélectionnée de système.

AC-03(12) — Assurer et appliquer l'accès aux applications (---)

Énoncés :

a. Exiger des applications pour assurer, dans le cadre du processus d'installation, l'accès nécessaire aux applications et fonctions de systèmes suivantes : [Affectation : applications et fonctions de systèmes définies par l'organisation]
b. Fournir un mécanisme d'application de l'accès pour empêcher les accès non autorisés
c. Approuver les changements d'accès après l'installation initiale de l'application

Responsable : Aucun

Discussion :

Assurer et appliquer l'accès aux applications permet d'aborder la question des applications qui doivent accéder à des applications et fonctions existantes de systèmes, notamment les contacts des utilisatrices et utilisateurs, le système mondial de localisation, les caméras, les claviers, les microphones, les réseaux, les téléphones ou autres fichiers.

AC-03(13) — Contrôle d’accès basé sur les attributs (---)

Énoncés :

Appliquer une stratégie de contrôle d’accès basé sur les attributs des sujets et objets définis, et contrôler l’accès en fonction des [Affectation : attributs définis par l’organisation pour assumer les autorisations d’accès].

Responsable : Aucun

Discussion :

Le contrôle d’accès basé sur les attributs est une stratégie de contrôle d’accès qui limite l’accès aux systèmes aux utilisatrices et utilisateurs autorisés en fonction des attributs particuliers de l’organisation (par exemple, les fonctions, l’identité), des attributs d’intervention (par exemple, lecture, écriture, suppression), des attributs environnementaux (par exemple, l’heure ou l’emplacement) et des attributs des ressources (par exemple, la classification d’un document). Les organisations peuvent créer des règles selon des attributs et les autorisations (c’est-à-dire des droits d’accès) nécessaires en vue d’exécuter les opérations requises sur les systèmes associés aux règles et attributs définis par l’organisation. Lorsque des attributs définis dans des règles ou des stratégies de contrôle d’accès basé sur des attributs sont attribués, sont attribués aux utilisatrices et utilisateurs, ils peuvent être provisionnés à un système doté des privilèges requis, ou obtenir de manière dynamique accès à une ressource protégée. Le contrôle d’accès basé sur les attributs peut être mis en oeuvre de façon obligatoire ou discrétionnaire. Lorsqu’elles sont mises en oeuvre avec des contrôles d’accès obligatoire, les exigences du contrôle AC-03(03) définissent la portée des sujets et des objets couverts par la stratégie.

AC-03(14) — Accès individuel (---)

Énoncés :

Fournir les [Affectation : mécanismes définis par l'organisation] pour permettre aux personnes d'avoir accès aux éléments suivants des renseignements personnels : [Affectation : éléments définis par l'organisation].

Responsable : Aucun

Discussion :

Un accès individuel permet aux gens d'accéder et de possiblement corriger des inexactitudes liées aux renseignements personnels qui se trouvent dans les dossiers organisationnels, indépendamment de leur format. L'accès aide les gens à mieux comprendre comment les organisations gouvernementales recueillent, utilisent ou divulguent leurs renseignements personnels. Cet accès peut également aider les gens à s'assurer que leurs renseignements personnels utilisés pour prendre des décisions administratives sont exacts. Les mécanismes d'accès comprennent les formulaires de demande et les interfaces d'applications.

AC-03(15) — Contrôle d’accès discrétionnaire et obligatoire (---)

Énoncés :

a. Appliquer la [Affectation : stratégie de contrôle d’accès obligatoire définie par l’organisation] à l’ensemble de sujets et objets couverts qui sont définis dans la stratégie
b. Appliquer la [Affectation : stratégie de contrôle d’accès discrétionnaire définie par l’organisation] à l’ensemble de sujets et objets couverts qui sont définis dans la stratégie

Responsable : Aucun

Discussion :

En mettant en oeuvre simultanément une stratégie de contrôle d’accès obligatoire et une stratégie de contrôle d’accès discrétionnaire, il est possible d’offrir une protection supplémentaire contre une exécution non autorisée de code de la part d’utilisatrices ou utilisateurs, ou provenant de processus agissant au nom de ceux-ci. Il est ainsi possible d’empêcher qu’une seule utilisatrice ou un seul utilisateur compromis ou qu’un seul processus compromette tout le système.

AC-04 — Application du contrôle de flux d'information (---)

Énoncés :

Appliquer des autorisations approuvées pour contrôler le flux d'information dans le système et entre les systèmes reconnectés en fonction des [Affectation : stratégies de contrôle de flux d'information définies par l'organisation].

Responsable : Aucun

Discussion :

Le contrôle de flux d'information régit le cheminement de l'information au sein d'un système et entre des systèmes (par opposition aux personnes autorisées à y accéder), quels que soient les accès subséquents à cette information. Les restrictions relatives au contrôle du flux d'information consistent notamment à bloquer le trafic externe qui prétend provenir de l'intérieur de l'organisation, éviter que l'information contrôlée pour exportation ne soit transmise en clair sur Internet, limiter les requêtes Web qui ne sont pas acheminées par l'intermédiaire du serveur mandataire Web interne et limiter les transferts d'information entre les organisations selon les structures et le contenu des données. Le transfert d'information entre des organisations peut nécessiter une entente indiquant comment le flux d'information sera appliqué (voir le contrôle CA-03). Le transfert d'information entre des systèmes associés à des domaines de sécurité ou de protection de la vie privée différents et faisant l'objet de stratégies de sécurité ou de protection de la vie privée différentes présente un risque qu'un tel transfert contrevienne à une ou à plusieurs stratégies de sécurité ou de protection de la vie privée des domaines. Dans de telles situations, les gardiennes et gardiens de l'information fournissent des directives aux points désignés d'application des stratégies entre les systèmes interconnectés. Les organisations considèrent le recours à des solutions architecturales particulières pour appliquer des stratégies de sécurité et de protection de la vie privée en particulier. L'application des contrôles comprend l'interdiction des transferts d'information entre les systèmes connectés (c'est-à-dire autoriser l'accès seulement), la vérification des autorisations en écriture avant d'accepter l'information provenant d'un autre domaine de sécurité ou de protection de la vie privée ou d'un système connecté, le recours à des mécanismes matériels pour appliquer des flux d'information dans une seule direction et la mise en place de mécanismes remaniés de confiance pour réassigner les attributs et les étiquettes de sécurité et de protection de la vie privée. Les responsables des fonds de renseignements personnels devraient s'assurer que la quantité minimale de renseignements personnels requis est échangée d'un système à l'autre et, dans la mesure du possible, veiller à ce que l'échange des renseignements personnels soit documenté dans un accord. Les organisations utilisent couramment les mécanismes d'application et les stratégies de contrôle de flux d'information pour contrôler le flux d'information entre des sources et des destinations précises à l'intérieur des systèmes et entre les systèmes interconnectés. Le contrôle de flux est fondé sur les caractéristiques de l'information et/ou sur son chemin. Il est appliqué, par exemple, aux dispositifs de protection des frontières qui font appel à des ensembles de règles ou qui mettent en place des paramètres de configuration qui restreignent les services de systèmes et permettent de filtrer les paquets de données en fonction de l'information comprise dans les en-têtes ou de filtrer les messages en fonction du contenu du message. Les organisations doivent également considérer la robustesse des mécanismes de filtrage et d'inspection (c'est-à-dire les composants matériels, micrologiciels et logiciels) qui sont essentiels à l'application du contrôle de flux d'information. Les améliorations 3 à 32 portent principalement sur les besoins en matière de solutions interdomaines, qui sont axés sur des techniques de filtrage avancées, une analyse approfondie et des mécanismes robustes d'application du contrôle de flux d'information mis en oeuvre dans les produits interdomaines, comme les mécanismes de protection à assurance élevée. De telles capacités ne sont généralement pas offertes dans des produits commerciaux sur étagère (COTS pour Commercial Off-The-Shelf). L'application du contrôle de flux d'information vise également le trafic du plan de contrôle (par exemple, le routage et le système de noms de domaine (DNS pour Domain Name System)).

AC-04(01) — Attributs de sécurité et de protection de la vie privée des objets (---)

Énoncés :

Utiliser des [Affectation : attributs de sécurité et de protection de la vie privée définis par l'organisation] associés aux [Affectation : objets d'information, de source et de destination définis par l'organisation] pour appliquer les [Affectation : stratégies de contrôle de flux d'information définies par l'organisation] comme base pour les décisions concernant le contrôle de flux.

Responsable : Aucun

Discussion :

Les mécanismes d'application du contrôle de flux d'information comparent les attributs de sécurité associés à l'information (contenu et structure de données) avec des objets de source et de destination, et interviennent de manière appropriée lorsqu'ils identifient des flux d'information non explicitement autorisés par les politiques de contrôle de flux d'information. Par exemple, un objet d'information étiqueté Secret serait autorisé à être transmis à un objet de destination étiqueté Secret, mais un objet d'information étiqueté Très secret ne serait pas autorisé à être transmis à un objet de destination étiqueté Secret. Un jeu de données comportant des renseignements personnels peut porter une étiquette avec des restrictions pour empêcher une combinaison avec d'autres types de jeux de données et, ainsi, ce jeu de données ne serait pas autorisé à circuler vers le jeu de données à diffusion restreinte. Les attributs de sécurité et de protection de la vie privée peuvent inclure également les adresses source et destination utilisées dans les pare-feu qui filtrent le trafic. L'application du contrôle de flux d'information basée sur des attributs de sécurité et de protection de la vie privée explicites peut servir, par exemple, à contrôler la diffusion de certains types d'information.

AC-04(02) — Domaines de traitement (---)

Énoncés :

Utiliser des domaines de traitement protégés pour appliquer les [Affectation : stratégies de contrôle de flux d'information définies par l'organisation] comme base pour les décisions concernant le contrôle de flux.

Responsable : Aucun

Discussion :

Les domaines de traitement protégés sont des espaces de traitement ayant des interactions contrôlées avec d'autres espaces de traitement, permettant le contrôle des flux d'information entre les espaces, de même qu'en provenance et à destination des objets de données ainsi que des objets d'information. Un domaine de traitement protégé peut être établi, par exemple, en mettant en oeuvre un domaine et une application type. Dans le domaine et l'application type, les processus du système sont attribués aux domaines; l'information est identifiée par type; les flux d'information sont contrôlés selon les accès autorisés à l'information (c'est-à-dire déterminés par domaine et type), selon la signalisation autorisée entre les domaines et selon les transitions de processus autorisées vers d'autres domaines.

AC-04(03) — Contrôle dynamique de flux d'information (---)

Énoncés :

Appliquer les [Affectation : stratégies de contrôle de flux d'information définies par l'organisation].

Responsable : Aucun

Discussion :

Les stratégies organisationnelles liées au contrôle dynamique de flux d'information comprennent la permission ou l'interdiction des flux d'information en fonction de conditions changeantes ou de motifs liés à la mission et aux opérations. Les conditions changeantes peuvent être des changements dans la tolérance au risque en raison de changements dans l'immédiateté des besoins relatifs à la mission et aux opérations, des changements dans l'environnement de menace et la détection d'événements potentiellement préjudiciables et néfastes.

AC-04(04) — Contrôle de flux de l'information chiffrée (---)

Énoncés :

Le système empêche l'information chiffrée de contourner les [Affectation : mécanismes de vérification de contenu] en [Sélection (un choix ou plus) : déchiffrant l'information; bloquant le flux d'information chiffrée; en mettant fin aux sessions de communication qui tentent d'acheminer l'information chiffrée; {Affectation : procédure ou méthode définie par l'organisation}].

Responsable : Aucun

Discussion :

Les mécanismes de contrôle de flux comprennent la vérification de contenu, les filtres de stratégie de sécurité et les identifiants de type de données. Le terme « chiffrement » est élargi pour couvrir les données codées qui ne sont pas reconnues par les mécanismes de filtrage.

AC-04(05) — Types de données intégrés (---)

Énoncés :

Appliquer [Affectation : restrictions définies par l'organisation] concernant l'intégration de types de données dans d'autres types de données.

Responsable : Aucun

Discussion :

L'intégration de types de données dans d'autres types de données pourrait réduire l'efficacité du contrôle de flux. L'intégration de types de données comprend l'insertion de fichiers à titre d'objets dans d'autres fichiers et l'utilisation de types de données comprimées ou archivées qui peuvent contenir de multiples types de données intégrés. Les limites relatives à l'intégration de types de données considèrent les niveaux d'intégration et interdisent les niveaux d'intégration qui dépassent les capacités des outils d'inspection.

AC-04(06) — Métadonnées (---)

Énoncés :

Appliquer le contrôle de flux d'information en fonction des [Affectation : métadonnées définies par l'organisation].

Responsable : Aucun

Discussion :

Les métadonnées désignent de l'information qui décrit les caractéristiques des données. Elles comprennent les métadonnées structurales décrivant des structures de données ou les métadonnées descriptives décrivant du contenu de données. Les métadonnées peuvent également déduire des caractéristiques personnelles d'une personne. L'application des flux d'information permis en fonction des métadonnées simplifie et améliore le contrôle de flux. Les organisations considèrent la fiabilité des métadonnées selon l'exactitude des données (c'est-à-dire la connaissance que les valeurs de métadonnées sont correctes par rapport aux données), l'intégrité des données (c'est-à-dire la protection contre les changements non autorisés aux étiquettes de métadonnées) et la liaison entre les métadonnées et les données utiles (c'est-à-dire des techniques solides et suffisantes de liaison ainsi que l'assurance appropriée).

AC-04(07) — Mécanismes de flux unidirectionnels (---)

Énoncés :

Appliquer des flux unidirectionnels d'information par des mécanismes de contrôle de flux matériel.

Responsable : Aucun

Discussion :

Les mécanismes de flux unidirectionnels peuvent aussi être appelés réseau unidirectionnel, passerelle de sécurité unidirectionnelle ou diode réseau. Les mécanismes de flux unidirectionnels peuvent aider à empêcher que des données soient exportées d'un domaine ou d'un système classifié ou à incidence élevée tout en autorisant l'importation de données d'un domaine ou d'un système non classifié ou à faible incidence.

AC-04(08) — Filtres de stratégie de sécurité et protection de la vie privée (Nc--)

Énoncés :

a. Appliquer le contrôle de flux d'information en utilisant des [Affectation : filtres de stratégie de sécurité ou de protection de la vie privée définis par l'organisation] comme base pour les décisions de contrôle de flux pour les [Affectation : flux d'information définis par l'organisation]
b. [Sélection (un choix ou plus) : Bloquer; retirer; modifier; mettre en quarantaine] les données après l'échec d'un traitement de filtre conformément à [Affectation : stratégie de sécurité ou de protection de la vie privée définie par l'organisation]

Responsable : Aucun

Discussion :

Les filtres de stratégie de sécurité ou de protection de la vie privée définis par l'organisation peuvent s'appliquer au contenu et aux structures de données. Par exemple, les filtres de stratégie de sécurité ou de protection de la vie privée pour les structures de données peuvent chercher la taille maximale des fichiers, la taille maximale des champs ainsi que les types de données et de fichiers (pour les données structurées et non structurées). Les filtres de stratégie de sécurité ou de protection de la vie privée pour le contenu des données peuvent chercher des mots précis, des valeurs énumérées ou des intervalles de valeur de données et du contenu caché. Ils peuvent être utilisés pour améliorer la précision des données utilisées dans le cadre d'un processus de prise de décision; par exemple, les numéros de téléphone doivent comprendre 10 chiffres. Les organisations peuvent mettre en oeuvre plus d'un filtre de stratégie de sécurité ou de protection de la vie privée pour répondre aux objectifs liés au contrôle de flux d'information. Les données structurées permettent l'interprétation du contenu des données par application. Les données non structurées désignent l'information numérique sans structure de données ou avec une structure de données qui ne permet pas d'élaborer des ensembles de règles pour traiter le niveau d'incidence ou de classification de l'information contenue dans les données ou les décisions relatives à l'application du contrôle de flux. Les données non structurées consistent en des objets binaires, essentiellement indépendants de tout langage (c'est-à-dire les fichiers d'images, les fichiers vidéo ou les fichiers audio) et des objets textuels associés à des langages écrits ou imprimés.

AC-04(09) — Vérifications manuelles (---)

Énoncés :

Appliquer l'utilisation de vérifications manuelles pour les [Affectation : flux d'information définis par l'organisation] selon les modalités suivantes : [Affectation : modalités définies par l'organisation].

Responsable : Aucun

Discussion :

Les organisations définissent les filtres de stratégie de sécurité ou de protection de la vie privée pour toutes les situations dans lesquelles des décisions automatisées liées au contrôle de flux peuvent être prises. Lorsqu'une décision entièrement automatisée liée au contrôle de flux ne peut être prise, on peut faire appel à un examen humain au lieu du filtrage automatisé de stratégie de sécurité ou de protection de la vie privée, ou à titre de complément au filtrage automatisé. Les organisations peuvent faire appel aux vérifications manuelles lorsqu'elles le jugent nécessaire.

AC-04(10) — Activer et désactiver les filtres de stratégie de sécurité et de protection de la vie privée (---)

Énoncés :

Permettre à une administratrice ou à un administrateur privilégié d'activer ou de désactiver les [Affectation : filtres de la stratégie de sécurité définis par l'organisation] selon les modalités suivantes : [Affectation : modalités définies par l'organisation].

Responsable : Aucun

Discussion :

Par exemple, comme le permet le système, les administratrices et administrateurs peuvent activer les filtres de stratégie de sécurité ou de protection de la vie privée pour les types de données approuvés. Les administratrices et administrateurs peuvent sélectionner les filtres qui sont exécutés sur un flux spécifique de données en fonction du type de données à transférer, des domaines de sécurité de source et de destination, et d'autres fonctions pertinentes de sécurité ou de protection de la vie privée, selon les besoins.

AC-04(11) — Configuration des filtres de stratégie de sécurité et de protection de la vie privée (---)

Énoncés :

Permettre à des administratrices et administrateurs privilégiés de configurer [Affectation : filtres de la stratégie de sécurité ou de protection de la vie privée définis par l'organisation] pour appuyer les différentes stratégies de sécurité ou de protection de la vie privée.

Responsable : Aucun

Discussion :

Les documents contiennent de l'information détaillée pour configure les filtres de stratégie de sécurité ou de protection de la vie privée. Par exemple, les administratrices et administrateurs peuvent configurer des filtres de stratégie de sécurité ou de protection de la vie privée pour inclure la liste des mots à proscrire vérifiée par les mécanismes de stratégie de sécurité ou de protection de la vie privée, conformément aux définitions fournies par les organisations.

AC-04(12) — Identifiants de type de données (---)

Énoncés :

Lors du transfert d'information entre différents domaines de sécurité, utiliser des [Affectation : identifiants de type de données définis par l'organisation] pour valider les données essentielles aux décisions liées au flux d'information.

Responsable : Aucun

Discussion :

Les identifiants de type de données comprennent les noms de fichier, les types de fichiers, les signatures et jetons de fichier ainsi que les signatures ou jetons multiples de fichier interne. Les systèmes peuvent autoriser seulement le transfert de données qui est conforme aux spécifications du format de type de données. L'identification et la validation de types de données sont fondées sur des spécifications définies associées à chaque format de données permis. Le nom et le numéro de fichier à eux seuls ne sont pas utilisés pour l'identification de type de données. Le contenu est validé de manière syntaxique et sémantique par rapport à ses spécifications pour assurer qu'il s'agit du bon type de données. Cela peut améliorer l'intégrité des données, plus particulièrement les renseignements personnels, qui sont à transmettre entre les systèmes.

AC-04(13) — Décomposition en sous-composantes pertinentes (---)

Énoncés :

Lors du transfert d'information entre différents domaines de sécurité, décomposer l'information en [Affectation : sous-composantes pertinentes définies par l'organisation] pour la présenter aux mécanismes d'application de la stratégie.

Responsable : Aucun

Discussion :

Décomposer l'information en sous-composants pertinents avant le transfert de l'information facilite les décisions relatives aux stratégies concernant la source, la destination, les certificats, la classification, les pièces jointes et les autres différenciateurs de composants liés à la sécurité et à la protection de la vie privée. Les mécanismes d'application des stratégies appliquent des règles de filtrage, d'inspection et/ou de nettoyage aux sous-composants d'information pertinents afin de faciliter l'application du contrôle de flux avant de transférer l'information à des domaines de sécurité différents.

AC-04(14) — Contraintes liées aux filtres de stratégie de sécurité ou de protection de la vie privée (---)

Énoncés :

Lors du transfert d'information entre différents domaines de sécurité, appliquer des [Affectation : filtres de stratégie de sécurité ou de protection de la vie privée définis par l'organisation] qui exigent des formats entièrement énumérés limitant le contenu et la structure des données.

Responsable : Aucun

Discussion :

Les restrictions relatives au contenu et à la structure des données réduisent l'éventail de contenu potentiellement malveillant ou illicite dans les transactions interdomaines. Les filtres de stratégie de sécurité ou de protection de la vie privée qui restreignent les structures de données comprennent la restriction de la taille des fichiers et des champs. Limiter la taille et le champ des fichiers à des champs de données ouverts peut réduire le risque de collecte excessive de renseignements personnels. Les filtres de stratégie de contenu des données comprennent le codage des formats pour les jeux de caractères, la restriction des champs de caractère pour qu'ils comportent uniquement des caractères alphanumériques, l'interdiction des caractères spéciaux et la validation des structures de schéma.

AC-04(15) — Détection de l'information non autorisée (---)

Énoncés :

Lors du transfert d'information entre différents domaines de sécurité, examiner l'information afin de détecter la présence de [Affectation : information non autorisée définie par l'organisation] et interdire le transfert de cette information, conformément à la [Affectation : stratégie de sécurité ou de conformité définie par l'organisation].

Responsable : Aucun

Discussion :

L'information non autorisée inclut le code malveillant, l'information qui n'est pas adéquate pour une publication provenant du réseau source, ou le code exécutable qui pourrait perturber ou nuire aux services ou systèmes sur le réseau de destination. Limiter la collecte d'information non autorisée spécifique peut réduire le risque de collecte de renseignements personnels inappropriés.

AC-04(16) — Transferts d’information sur des systèmes interconnectés (---)

Énoncés :

Annulé : Intégré au contrôle AC-04.

Responsable : Aucun

AC-04(17) — Authentification des domaines (---)

Énoncés :

Identifier de façon unique et authentifier les points source et destination par [Sélection (un choix ou plus) : organisation; système; application; service; personne] à des fins de transfert d'information.

Responsable : Aucun

Discussion :

L'attribution est une composante essentielle d'un concept d'opération de la sécurité et de la protection de la vie privée. La capacité d'identifier les points source et destination de l'information circulant dans des systèmes permet de reconstruire les événements à des fins judiciaires et d'encourager le respect des politiques en attribuant à des organisations ou à des personnes précises les infractions à la politique. Pour que l'authentification du domaine réussisse, les étiquettes des systèmes doivent faire la distinction entre les systèmes, les organisations et les personnes qui participent à la préparation, à l'envoi, à la réception ou à la diffusion de l'information. L'attribution permet également aux organisations de mieux gérer l'extraction du traitement des renseignements personnels circulant dans les systèmes et elle peut faciliter le suivi du consentement, ainsi que la correction, la suppression ou les demandes d'accès des gens.

AC-04(18) — Liaison d’attribut de sécurité (---)

Énoncés :

Annulé : Intégré au contrôle AC-16.

Responsable : Aucun

AC-04(19) — Validation des métadonnées (---)

Énoncés :

Lors du transfert de l'information entre différents domaines de sécurité, mettre en oeuvre les [Affectation : filtres de stratégie de sécurité ou de protection de la vie privée définis par l'organisation] en fonction des métadonnées.

Responsable : Aucun

Discussion :

Toute l'information (y compris les métadonnées de même que les données auxquelles les métadonnées s'appliquent) est assujettie au filtrage et à l'inspection. Certaines organisations font une distinction entre les métadonnées et les données utiles (c'est-à-dire seules les données auxquelles sont liées les métadonnées). D'autres organisations ne font pas cette distinction et considèrent plutôt que les métadonnées ainsi que les données auxquelles les métadonnées s'appliquent font partie des données utiles.

AC-04(20) — Solutions approuvées (---)

Énoncés :

Utiliser des [Affectation : solutions définies par l'organisation dans les configurations approuvées] pour contrôler le flux de [Affectation : l'information définie par l'organisation] dans les domaines de sécurité.

Responsable : Aucun

Discussion :

Les organisations définissent les configurations et solutions approuvées dans les stratégies et directives interdomaines conformément aux types de flux d'information dans les limites de la classification.

AC-04(21) — Séparation physique ou logique des flux d'information (---)

Énoncés :

Séparer les flux d'information de façon logique ou physique au moyen de [Affectation : mécanismes et/ou techniques définis par l'organisation] pour accomplir les [Affectation : séparations requises par type d'information définies par l'organisation].

Responsable : Aucun

Discussion :

L'application de la séparation des flux d'information associés à des types définis de données peut renforcer la protection en garantissant que l'information n'est pas mélangée en transit et en permettant le contrôle de flux par chemin de transmission qui ne serait pas faisable autrement. Les types d'information séparable comprennent le trafic de communication entrant et sortant, les demandes de services et les réponses, ainsi que l'information de catégories de sécurité ou de niveaux de classification différents.

AC-04(22) — Accès seulement (---)

Énoncés :

Fournir à un seul dispositif l'accès aux plateformes informatiques, aux applications ou aux données contenues dans des domaines de sécurité différents tout en empêchant le flux d'information entre les différents domaines de sécurité.

Responsable : Aucun

Discussion :

Le système fournit un bureau afin que les utilisatrices et utilisateurs puissent accéder à chaque domaine de sécurité connecté sans fournir de mécanismes de transfert de données ou d'information entre les différents domaines de sécurité. Un exemple de solution d'accès seulement est un terminal qui offre à une utilisatrice ou un utilisateur accès à de l'information avec différentes classifications de sécurité tout en gardant l'information séparée.

AC-04(23) — Modifier l'information non communicable (---)

Énoncés :

Lors du transfert d'information entre différents domaines de sécurité, modifier l'information non communicable en mettant en oeuvre une [Affectation : mesure modifiable définie par l'organisation].

Responsable : Aucun

Discussion :

Modifier ou anonymiser de l'information non communicable peut aider à prévenir une fuite de données ou une attaque lorsque l'information est transférée dans les domaines de sécurité. Parmi les mesures de modification, il faut noter le masquage, la permutation, la modification comme l'embrouillage de l'élimination de données ou le caviardage.

AC-04(24) — Format normalisé interne (---)

Énoncés :

Lors du transfert d'information entre différents domaines de sécurité, analyser des données entrantes dans un format normalisé interne et régénérer les données pour qu'elles soient conformes aux spécifications prévues.

Responsable : Aucun

Discussion :

Convertir des données en formulaires normalisés est l'un des mécanismes les plus efficaces pour arrêter les attaques malveillantes et les classes importantes d'exfiltration de données.

AC-04(25) — Nettoyage des données (---)

Énoncés :

Lors du transfert d'information entre différents domaines de sécurité, nettoyer les données pour minimiser la [Sélection (un choix ou plus) : livraison de contenu malveillant, la commande et le contrôle de code malveillant, l'augmentation de code malveillant, et les données codées par stéganographie; fuite d'information sensible] conformément à la [Affectation : stratégie définie par l'organisation].

Responsable : Aucun

Discussion :

Le nettoyage des données est le processus irréversible qui consiste à supprimer ou à détruire les données stockées sur un dispositif de stockage (par exemple, disques durs, disques à mémoire flash ou à circuits intégrés, appareils mobiles, CD, DVD et disques Blu-ray) ou sous forme d'imprimé.

AC-04(26) — Mesures de filtrage de vérification (---)

Énoncés :

Lors du transfert d'information entre différents domaines de sécurité, enregistrer et vérifier les mesures de filtrage de contenu ainsi que les résultats pour l'information faisant l'objet du filtrage.

Responsable : Aucun

Discussion :

Le filtrage de contenu est le processus qui consiste à inspecter l'information alors qu'elle traverse une solution interdomaines (SID) et détermine si l'information respecte une stratégie prédéfinie. Les mesures de filtrage de contenu et les résultats de ces mesures de filtrage sont enregistrés pour différents messages pour assurer l'application des bonnes mesures de filtrage. Les rapports sur les filtres de contenu sont utilisés pour aider au dépannage des mesures, par exemple, en déterminant pourquoi le contenu du message a été modifié ou pourquoi il a échoué au processus de filtrage. Les événements vérifiables sont définis dans le contrôle AU-

02. Les enregistrements de vérification sont générés dans le contrôle AU-12.

AC-04(27) — Mécanismes de filtrage redondants et indépendants (---)

Énoncés :

Lors du transfert d'information entre différents domaines de sécurité, mettre en oeuvre des solutions de filtrage de contenu qui offrent des mécanismes de filtrage de contenu redondants et indépendants pour chaque type de données.

Responsable : Aucun

Discussion :

Le filtrage de contenu est le processus qui consiste à inspecter l'information alors qu'elle traverse une solution interdomaines (SID) et détermine si l'information respecte une stratégie prédéfinie. Le filtrage de contenu redondant et indépendant permet d'éliminer un système de filtrage à point de défaillance unique. L'indépendance se définit comme étant la mise en oeuvre d'un filtre de contenu qui utilise un code de base différent et différentes bibliothèques de soutien (par exemple, 2 filtres JPEG utilisant différentes bibliothèques JPEG de fournisseurs) et plusieurs processus de systèmes indépendants.

AC-04(28) — Pipelines de filtre linéaire (---)

Énoncés :

Lors du transfert d'information entre différents domaines de sécurité, mettre en oeuvre un pipeline de filtre de contenu linéaire qui est appliqué avec contrôle d'accès discrétionnaire et obligatoire.

Responsable : Aucun

Discussion :

Le filtrage de contenu est le processus qui consiste à inspecter l'information alors qu'elle traverse une solution interdomaines (SID) et détermine si l'information respecte une stratégie prédéfinie. L'utilisation de pipelines de filtre de contenu linéaire permet de s'assurer que les processus du filtre sont incontournables et automatiquement invoqués. En général, le recours à des architectures de filtrage en parallèle pour le filtrage de contenu d'un seul type de données crée des problèmes de contournement ou de non-exécution.

AC-04(29) — Moteurs d’orchestration de filtre (---)

Énoncés :

Lors du transfert d’information entre différents domaines de sécurité, utiliser des moteurs d’orchestration de filtre de contenu pour s’assurer de ce qui suit :
a. les mécanismes de filtrage de contenu ont réussi l’exécution sans présenter d’erreurs
b. les opérations de filtrage de contenu sont exécutées dans le bon ordre et sont conforment à la [Affectation : stratégie définie par l’organisation]

Responsable : Aucun

Discussion :

Le filtrage de contenu est le processus qui consiste à inspecter l’information alors qu’elle traverse une solution interdomaines (SID) et détermine si l’information respecte une stratégie de sécurité prédéfinie. Un moteur d’orchestration coordonne l’ordre des activités (manuelles et automatisées) dans le cadre d’un processus de filtrage de contenu. Les erreurs sont définies comme des actions anormales ou une interruption inattendue du processus de filtres de contenu. Il ne s’agit pas ici d’un contenu filtre défaillant en raison d’une non-conformité à la stratégie. Les rapports sur les filtres de contenu relèvent d’un mécanisme fréquemment utilisé pour s’assurer que les mesures de filtrages prévues sont exécutées avec succès.

AC-04(30) — Mécanismes de filtrage à l'aide de plusieurs processus (---)

Énoncés :

Lors du transfert d'information entre différents domaines de sécurité, mettre en oeuvre des mécanismes de filtrage de contenu à l'aide de plusieurs processus.

Responsable : Aucun

Discussion :

Le recours à plusieurs processus pour mettre en oeuvre les mécanismes de filtrage de contenu permet de réduire la probabilité d'un point de défaillance unique.

AC-04(31) — Prévenir l’échec d’un transfert de contenu (---)

Énoncés :

Lors du transfert d’information entre différents domaines de sécurité, prévenir l’échec d’un transfert de contenu vers le domaine destinataire.

Responsable : Aucun

Discussion :

Tout contenu ayant échoué aux vérifications de filtrage peut corrompre le système s’il est transféré au domaine destinataire.

AC-04(32) — Exigences des processus pour le transfert d'information (---)

Énoncés :

Lors du transfert d'information entre différents domaines de sécurité, le processus qui transfert l'information entre les pipelines de filtre :
a. ne filtre pas le contenu du message
b. valide les métadonnées de filtration
c. assure que le contenu associé aux métadonnées de filtrage a effectué avec succès le filtrage
d. transfert le contenu au pipeline de filtre de destination

Responsable : Aucun

Discussion :

Les processus qui transfèrent l'information entre les pipelines de filtre sont associés à une complexité et une fonctionnalité minimales pour assurer que les processus fonctionnent correctement.

AC-05 — Séparation des tâches (---)

Énoncés :

a. Identifier et consigner les [Affectation : tâches assumées par le personnel définies par l'organisation nécessitant une séparation]
b. Définir les autorisations d'accès au système afin d'appuyer la séparation des tâches

Responsable : Aucun

Discussion :

La séparation des tâches gère l'abus possible des droits d'accès autorisés et aide à réduire le risque d'activités malveillantes sans collusion. Les mécanismes de séparation des tâches comprennent notamment : la division des fonctions liées à la mission ou aux activités et des fonctions de soutien entre les personnes ou rôles, l'exécution de fonctions de soutien liées au système par différentes personnes et l'assurance que le personnel de sécurité qui administre les fonctions de contrôle d'accès n'administre pas également les fonctions de vérification. Puisque les violations de séparation des tâches peuvent s'étendre sur plusieurs systèmes et domaines d'application, les organisations doivent prendre en considération l'ensemble des systèmes et des composants de système lors de l'élaboration de la stratégie sur la séparation des tâches. La séparation des tâches s'applique dans le cadre des activités de gestion des comptes du contrôle AC-02, tandis que les mécanismes de contrôle de l'accès relèvent du contrôle AC-03 et les activités relatives à la gestion des identités relèvent des contrôles IA-02, IA-04 et IA-12.

AC-06 — Droit d’accès minimal (---)

Énoncés :

Utiliser le principe du droit d’accès minimal, ce qui autorise l’accès uniquement aux utilisatrices et utilisateurs (ou aux processus exécutés en leur nom) qui en ont besoin pour accomplir les tâches qui leur ont été assignées par l’organisation.

Responsable : Aucun

Discussion :

Les organisations font appel au principe du droit d’accès minimal pour des tâches et systèmes précis. Ce principe est également appliqué aux processus de système et assure que les processus ont accès aux systèmes et fonctionnent au niveau de droits d’accès appropriés pour la réalisation des fonctions liées à la mission ou aux activités de l’organisation. Les organisations considèrent la création de processus, de rôles et de comptes de système additionnels, au besoin, pour adhérer au principe du droit d’accès minimal. Elles appliquent également ce principe au développement, à la mise en oeuvre et à l’exploitation de leurs systèmes.

AC-06(01) — Autorisation de l’accès aux fonctions de sécurité (---)

Énoncés :

Autoriser l’accès à [Affectation : personnel et rôles définis par l’organisation] pour :
a. les [Affectation : fonctions de sécurité définies par l’organisation (déployées dans le matériel, les logiciels et les micrologiciels)]
b. [Affectation : information liée à la sécurité définie par l’organisation]

Responsable : Aucun

Discussion :

Les fonctions de sécurité comprennent l’établissement des comptes de système, la configuration des autorisations d’accès (c’est-à-dire les permissions et droits d’accès), la configuration des paramètres pour les événements à vérifier et l’établissement des paramètres de détection d’intrusion. L’information liée à la sécurité comprend les règles de filtrage pour les routeurs et les pare-feu, les paramètres de configuration pour les services de sécurité, l’information de gestion des clés cryptographiques et les listes de contrôle d’accès. Le personnel autorisé comprend les administratrices et administrateurs de la sécurité, les administratrices et administrateurs de système, les agentes et agents de sécurité de système, les programmeuses et programmeurs de système et d’autres utilisatrices et utilisateurs disposant d’un accès privilégié.

AC-06(02) — Accès non privilégié aux fonctions non liées à la sécurité (---)

Énoncés :

Exiger que les utilisatrices et utilisateurs de comptes ou de rôles de système qui ont accès aux [Affectation : fonctions de sécurité et informations sur la sécurité définies par l'organisation] utilisent des comptes ou des rôles non privilégiés pour accéder à des fonctions qui ne sont pas liées à la sécurité.

Responsable : Aucun

Discussion :

L'exigence d'utiliser des comptes non privilégiés pour accéder à des fonctions ou à des fonctions qui ne sont pas liées à la sécurité limite l'exposition lors de l'utilisation de comptes privilégiés ou des rôles. Les rôles sont inclus pour tenir compte des situations où les organisations mettent en oeuvre des stratégies de contrôle d'accès, comme le contrôle d'accès basé sur les rôles, et où un changement de rôle fournit le même degré d'assurance, dans le changement des autorisations d'accès de l'utilisatrice ou utilisateur et les processus exécutés en son nom, que celui qui serait fourni dans un changement apporté entre un compte privilégié et un compte non privilégié.

AC-06(03) — Accès réseau aux commandes privilégiées (---)

Énoncés :

Autoriser l'accès réseau aux [Affectation : commandes privilégiées définies par l'organisation] seulement pour [Affectation : répondre à des besoins opérationnels urgents définis par l'organisation] et consigner les motifs d'un tel accès dans le plan de sécurité pour le système.

Responsable : Aucun

Discussion :

L'accès réseau désigne tout accès dans une connexion réseau par opposition à l'accès local (c'est-à-dire utilisatrice ou utilisateur sur place).

AC-06(04) — Domaines de traitement séparés (---)

Énoncés :

Fournir des domaines de traitement séparés pour permettre une granularité plus fine dans l'attribution des droits d'accès d'utilisatrice et utilisateur.

Responsable : Aucun

Discussion :

Fournir des domaines de traitement séparés pour permettre une granularité plus fine dans l'attribution des droits d'accès d'utilisatrice et utilisateur comprend l'utilisation de techniques de virtualisation pour accorder des droits d'accès additionnels dans une machine virtuelle tout en limitant ceux accordés à d'autres machines virtuelles ou à la machine réelle sous-jacente; la mise en oeuvre de domaines physiques séparés et l'utilisation de mécanismes de séparation des domaines logiciels ou matériels.

AC-06(05) — Comptes privilégiés (---)

Énoncés :

Restreindre les comptes privilégiés sur le système à [Affectation : personnel ou rôles définis par l'organisation].

Responsable : Aucun

Discussion :

Les comptes privilégiés, y compris les comptes de superutilisateur, sont habituellement décrits comme des administratrices et administrateurs système dans les différents types de systèmes d'exploitation commerciaux sur étagère (COTS). La restriction des comptes privilégiés à des employées et employés ou à des rôles précis empêche les utilisatrices et utilisateurs normaux d'accéder aux fonctions et à l'information privilégiées. Lorsqu'elles appliquent des restrictions, les organisations peuvent faire une distinction entre les droits d'accès attribués aux comptes locaux et ceux attribués aux comptes de domaine pour autant qu'elles restent en mesure de contrôler les configurations des systèmes en ce qui a trait aux paramètres clés et, le cas échéant, d'atténuer suffisamment les risques.

AC-06(06) — Accès privilégié des utilisatrices et utilisateurs ne faisant pas partie de l'organisation (---)

Énoncés :

Interdire tout accès privilégié au système aux utilisatrices et utilisateurs ne faisant pas partie de l'organisation.

Responsable : Aucun

Discussion :

Une utilisatrice ou un utilisateur organisationnel est une employée ou un employé ou encore une personne dont le statut est considéré par son organisation comme étant équivalent à celui d'une employée ou un employé. Les utilisatrices et utilisateurs organisationnels comprennent les entrepreneures et entrepreneurs, chercheuses et chercheurs invités ou des personnes provenant d'autres organisations. Les stratégies et procédures permettant l'octroi du statut équivalent d'employées et employés à des personnes comprennent le principe du besoin de savoir, la citoyenneté et le lien avec l'organisation.

AC-06(07) — Examen des privilèges d'utilisateur (---)

Énoncés :

a. Examiner les droits d'accès attribués aux [Affectation : rôles ou classes d'utilisateur définis par l'organisation] tous les [Affectation : fréquence définie par l'organisation] pour valider la nécessité de détenir ces droits d'accès;
b. Réattribuer ou retirer les droits d'accès, au besoin, pour bien refléter les besoins organisationnels liés à la mission et aux opérations.

Responsable : Aucun

Discussion :

La nécessité de détenir certains droits d'accès d'utilisatrice ou utilisateur pourrait changer au fil du temps selon les changements aux fonctions opérationnelles et aux missions organisationnelles, selon les environnements d'opération, selon les technologies ou selon les menaces. Un examen périodique des droits d'accès attribués aux utilisatrices et utilisateurs est essentiel afin de déterminer si la justification relative à l'attribution de ces droits d'accès est toujours valide. Si la nécessité ne peut être validée de nouveau, les organisations doivent prendre les mesures correctives appropriées.

AC-06(08) — Niveaux de droits d’accès pour une exécution de code (---)

Énoncés :

Empêcher les logiciels d’être exécutés à des niveaux de droits d’accès plus élevés que ceux des utilisatrices et utilisateurs qui exécutent les logiciels : [Affectation : logiciels définis par l’organisation].

Responsable : Aucun

Discussion :

Dans certains cas, les applications ou programmes logiciels doivent être exécutés avec des droits d’accès élevés pour effectuer les fonctions requises. Toutefois, selon la fonctionnalité et la configuration des logiciels, si les droits d’accès requis pour l’exécution sont à un niveau plus élevé que les droits d’accès attribués aux utilisateurs de ces applications et programmes, les utilisatrices et utilisateurs peuvent recevoir indirectement des droits d’accès plus élevés que deux qui leur ont été attribués.

AC-06(09) — Journalisation de l’utilisation des fonctions privilégiées (---)

Énoncés :

Journaliser l’exécution de fonctions privilégiées.

Responsable : Aucun

Discussion :

Une mauvaise utilisation des fonctions privilégiées, qu’elle soit intentionnelle ou non, par des utilisatrices et utilisateurs autorisés ou par des entités externes non autorisées ayant compromis des comptes système est une préoccupation constante et sérieuse qui peut avoir des répercussions négatives importantes sur les organisations. La journalisation et l’analyse des fonctions privilégiées sont une façon de détecter l’utilisation inappropriée et d’aider à atténuer les risques liés aux menaces internes et aux menaces persistantes avancées (MPA).

AC-06(10) — Interdiction aux utilisatrices et utilisateurs non privilégiés d'exécuter des fonctions privilégiées (---)

Énoncés :

Empêcher les utilisatrices et utilisateurs non privilégiés d'exécuter des fonctions privilégiées.

Responsable : Aucun

Discussion :

Les fonctions privilégiées comprennent la désactivation, le contournement ou la modification des contrôles de sécurité et de protection de la vie privée mis en oeuvre, l'établissement des comptes de système, les contrôles d'intégrité du système et l'administration des activités de gestion des clés cryptographiques. Les utilisatrices et utilisateurs non privilégiés ne détiennent pas les autorisations appropriées. Des exemples de fonctions privilégiées qui ne doivent pas être exécutées par des utilisatrices et utilisateurs non privilégiés comprennent les mécanismes de détection et de prévention d'intrusions et les mécanismes de protection contre les programmes malveillants. L'application du contrôle AC-03 empêche les utilisatrices et utilisateurs non privilégiés d'exécuter des fonctions privilégiées.

AC-07 — Tentatives d'ouverture de session infructueuses (Nc--)

Énoncés :

a. Appliquer une limite de [Affectation : nombre défini par l'organisation] tentatives d'ouverture de session non valides consécutives par l'utilisatrice ou utilisateur sur une période de [Affectation : délais définis par l'organisation];
b. [Sélection (un choix ou plus) : Verrouiller le compte ou le noeud pendant {Affectation : délais définis par l'organisation}; verrouiller le compte ou le noeud jusqu'à ce qu'une administratrice ou un administrateur le libère; retarder la prochaine invite d'ouverture de session selon {Affectation : algorithme de temporisation défini par l'organisation}; aviser l'administratrice ou administrateur de système; effectuer une autre {Affectation : opération définie par l'organisation}] automatiquement lorsque le nombre maximal de tentatives infructueuses est dépassé.

Responsable : Aucun

Discussion :

La nécessité d'une limite de tentatives d'ouverture de session infructueuses et les mesures à prendre lorsque le nombre maximal est atteint s'appliquent peu importe si la connexion a été établie localement ou par l'intermédiaire d'un réseau. En raison des risques de déni de service, les verrouillages automatiques effectués par les systèmes sont habituellement temporaires et annulés automatiquement après un délai prédéterminé établi par l'organisation. Dans le cas où elle a choisi un algorithme de temporisation, l'organisation peut utiliser différents algorithmes pour différents composants du système, selon les capacités de ces composants. Les réponses aux tentatives d'ouverture de session infructueuses peuvent être mises en oeuvre tant au niveau du système d'exploitation qu'au niveau des applications. Les opérations définies par l'organisation qui peuvent être effectuées lorsque le nombre autorisé de tentatives d'ouverture de session infructueuses est atteint comprennent notamment l'affichage d'un message invitant l'utilisatrice ou utilisateur à répondre à une question secrète en plus d'entrer son nom d'utilisateur et son mot de passe, l'utilisation d'un mode de confinement avec des capacités limitées pour les utilisatrices et utilisateurs (plutôt qu'un verrouillage complet), permettre aux utilisatrices et utilisateurs de se connecter uniquement à partir de certaines adresses de protocole Internet (IP pour Internet Protocol) précises, l'utilisation d'un test captcha pour éviter les attaques automatisées ou l'application de profils d'utilisateur qui font intervenir d'autres paramètres, comme l'emplacement, le moment de la journée, l'adresse IP, l'appareil ou l'adresse de contrôle d'accès au support (MAC pour Media Access Control). Si le verrouillage automatique du système ou l'exécution d'un algorithme de temporisation n'est pas mis en oeuvre pour soutenir l'objectif en matière de disponibilité, l'organisation considère une combinaison de mesures alternatives pour aider à prévenir les attaques par force brute. En plus de ce qui précède, l'organisation peut inviter les utilisatrices ou utilisateurs à répondre à une question secrète avant que le nombre maximal de tentatives d'ouverture de session infructueuses soit atteint. Il n'est généralement pas permis de déverrouiller automatiquement un compte après une période donnée. Des exceptions peuvent toutefois être nécessaires selon la mission ou les besoins opérationnels.

AC-07(01) — Verrouillage automatique du compte (---)

Énoncés :

Annulé : Intégré au contrôle AC-07.

Responsable : Aucun

AC-07(02) — Purge ou nettoyage d'appareils mobiles (---)

Énoncés :

Le système purge ou nettoie l'information des [Affectation : appareils mobiles définis par l'organisation] en fonction des [Affectation : techniques ou exigences en matière de purge ou de nettoyage définies par l'organisation] après [Affectation : nombre défini par l'organisation] tentatives infructueuses d'ouverture de session consécutives sur les appareils.

Responsable : Aucun

Discussion :

Un appareil mobile est un dispositif informatique de petite taille qui peut être transporté par une personne. Il est conçu pour fonctionner sans connexion physique et il dispose d'un stockage de données local, fixe ou amovible. Il comprend également une source d'alimentation autonome. La purge ou le nettoyage de l'appareil s'applique uniquement aux appareils mobiles pour lesquels un nombre défini par l'organisation de tentatives d'ouverture de session infructueuse a été établi. L'ouverture de session concerne l'appareil mobile lui-même et non les comptes qui y ont été établis, le cas échéant. Les ouvertures de session réussies dans les comptes des appareils mobiles remettent à zéro le compteur de tentatives d'ouvertures de session infructueuses. Il se peut que la purge ou le nettoyage ne soit pas nécessaire si l'information sur le dispositif est protégée à l'aide de mécanismes de chiffrement suffisamment robustes.

AC-07(03) — Limitation des tentatives par biométrie (---)

Énoncés :

Limiter le nombre de tentatives d'ouvertures de session infructueuses par biométrie à [Affectation : nombre défini par l'organisation].

Responsable : Aucun

Discussion :

La biométrie revêt un caractère probabiliste. La capacité d'authentifier de façon adéquate dépend de nombreux facteurs, notamment de la mise en correspondance du rendement et de la présentation des mécanismes de détection des attaques. Les organisations sélectionnent le nombre approprié de tentatives pour les utilisatrices et utilisateurs en fonction de facteurs qu'elles définissent.

AC-07(04) — Utilisation d’un autre facteur d’authentification (---)

Énoncés :

a. Permettre l’utilisation de [Affectation : facteurs d’authentification définis par l’organisation] qui sont différents des facteurs d’authentification principaux après que le nombre de tentatives d’ouverture de session non valides consécutives définies par l’organisation ait été dépassé
b. Appliquer une limite de [Affectation : nombre défini par l’organisation] tentatives d’ouverture de session non valides consécutives au moyen d’autres facteurs par l’utilisatrice ou utilisateur sur une période de [Affectation : délais définis par l’organisation]

Responsable : Aucun

Discussion :

Le recours à d’autres facteurs d’authentification soutient l’objectif de disponibilité et permet à une utilisatrice ou à un utilisateur qui a été verrouillé par erreur de se servir de facteurs d’authentification supplémentaires pour contourner le verrouillage.

AC-08 — Avis d'utilisation système (---)

Énoncés :

a. Afficher aux utilisatrices et utilisateurs [Affectation : message ou bannière d'avis d'utilisation du système défini par l'organisation], qui comprend des énoncés de protection de la vie privée et de sécurité conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables, et stipule ce qui suit :

1. les utilisatrices et utilisateurs qui accèdent à un système gouvernemental
2. l'utilisation du système peut être surveillée, enregistrée et faire l'objet d'une vérification
3. l'utilisation non autorisée du système est interdite et passible à des amendes administratives et à des sanctions pénales
4. les fichiers de renseignements personnels pertinents, le cas échéant
5. l'autorité légale pour la collecte de renseignements personnels
6. conséquences juridiques et administratives de tout refus de fournir des renseignements personnels
7. le droit de protection des renseignements personnels et le droit d'y accéder et de faire des demandes de correction
8. la manière dont les renseignements seront utilisés
9. le droit de déposer une plainte auprès de la Commission d'accès à l'information du Québec (CAI) concernant le traitement par les institutions des renseignements personnels des gens

b. Afficher le message ou la bannière d'avis jusqu'à ce que l'utilisatrice ou utilisateur accepte les modalités d'utilisation et opter d'ouvrir une session ou d'accéder au système

c. Dans le cas de systèmes accessibles au public :

1. afficher l'information sur l'utilisation du système selon les [Affectation : modalités définies par l'organisation] avant d'accorder l'accès
2. afficher, au besoin, des mises en garde concernant la surveillance, l'enregistrement et la vérification conformes aux dispositions sur la protection des renseignements personnels pour de tels systèmes qui interdisent généralement ces activités
3. comprendre une description des utilisations autorisées du système

Responsable : Aucun

Discussion :

Les avis concernant l'utilisation du système peuvent être mis en oeuvre au moyen de messages ou de bannières d'avertissement qui s'affichent avant qu'une utilisatrice ou un utilisateur ouvre une session sur le système. Ils sont utilisés uniquement pour l'accès au moyen des interfaces d'ouverture de session avec utilisatrices et utilisateurs humains. Ils ne sont pas requis lorsque de telles interfaces humaines n'existent pas. En tenant compte de l'évaluation des risques, les organisations doivent déterminer si un avis d'utilisation de système secondaire est nécessaire pour accéder à des applications ou à d'autres ressources système après la connexion initiale au réseau. Les organisations considèrent l'affichage des messages ou des bannières d'avis d'utilisation système en plusieurs langues selon les besoins organisationnels et la démographie des utilisatrices et utilisateurs du système. Ce contrôle autorise légalement l'ajout de contrôles de sécurité additionnels permettant notamment la surveillance, la vérification, la gestion des identifiants, l'application de l'entente d'utilisation acceptable, la détection de comportements anormaux ainsi que la détection de contamination et de tatouage numérique.

AC-09 — Avis d'ouverture de session précédente (---)

Énoncés :

Indiquer à l'utilisatrice ou utilisateur qui vient d'ouvrir une session sur le système la date et l'heure de sa dernière ouverture de session.

Responsable : Aucun

Discussion :

L'avis d'ouverture de session précédente est envoyé lorsqu'on accède au système par l'intermédiaire d'interfaces utilisateur humaines et depuis d'autres types d'architectures. L'information relative à la dernière ouverture de session fructueuse permet à une utilisatrice ou un utilisateur de déterminer si la date et l'heure fournies ne correspondent pas à son dernier accès.

AC-09(01) — Ouvertures de session infructueuses (---)

Énoncés :

Indiquer à l'utilisatrice ou utilisateur qui vient d'ouvrir une session le nombre de tentatives d'ouverture de session infructueuses depuis sa dernière tentative réussie.

Responsable : Aucun

Discussion :

L'information sur le nombre de tentatives d'ouverture de session infructueuses depuis sa dernière tentative réussie permet à l'utilisatrice ou utilisateur de savoir si le nombre de tentatives d'ouverture de session infructueuses est conforme au nombre réel de tentatives d'ouverture de session.

AC-09(02) — Tentatives fructueuses et infructueuses d'ouverture de session (---)

Énoncés :

Indiquer à l'utilisatrice ou utilisateur qui vient d'ouvrir une session le nombre de [Sélection (un choix) : tentatives d'ouverture de session fructueuses; tentatives d'ouverture de session infructueuses; tentatives d'ouverture de session fructueuses et infructueuses] pendant [Affectation : délais définis par l'organisation].

Responsable : Aucun

Discussion :

L'information sur le nombre de tentatives d'ouverture de session fructueuses et infructueuses dans un délai donné permet à l'utilisatrice ou utilisateur de savoir si le nombre et le type de tentatives d'ouverture de session sont conformes au nombre réel de tentatives d'ouverture de session.

AC-09(03) — Avis de changements au compte (Nc--)

Énoncés :

Aviser l'utilisatrice ou utilisateur qui vient d'ouvrir une session des changements apportés aux [Affectation : caractéristiques ou paramètres liés à la sécurité appliqués au compte de l'utilisatrice ou utilisateur définis par l'organisation] pendant [Affectation : délai défini par l'organisation].

Responsable : Aucun

Discussion :

L'information relative aux changements apportés aux caractéristiques liées à la sécurité appliquées au compte dans un délai donné permet à l'utilisatrice ou utilisateur de savoir si ces changements ont été faits sans son consentement.

AC-09(04) — Information supplémentaire sur l'ouverture de session (---)

Énoncés :

Aviser l'utilisatrice ou utilisateur qui vient d'ouvrir une session de l'information supplémentaire suivante : [Affectation : information supplémentaire définie par l'organisation].

Responsable : Aucun

Discussion :

Les organisations peuvent préciser de l'information supplémentaire qui sera fournie aux utilisatrices et utilisateurs lors de l'ouverture de session, comme l'emplacement de la dernière ouverture de session. L'emplacement de l'utilisatrice ou utilisateur est défini comme l'information que les systèmes peuvent établir (par exemple, les adresses IP à partir desquelles les ouvertures de session réseau ont eu lieu, les avis d'ouvertures de session locales ou les identifiants de dispositif).

AC-10 — Contrôle de sessions simultanées (---)

Énoncés :

Limiter le nombre de sessions simultanées pour chaque [Affectation : type de compte et/ou compte défini par l'organisation] à [Affectation : nombre défini par l'organisation].

Responsable : Aucun

Discussion :

Les organisations peuvent définir le nombre maximal de sessions simultanées pour les comptes du système globalement, par type de compte, par compte ou selon une combinaison. Par exemple, les organisations peuvent limiter le nombre de sessions simultanées pour les administratrices et administrateurs système ou les autres utilisatrices et utilisateurs travaillant dans des domaines particulièrement sensibles ou avec des applications essentielles à la mission. Le contrôle de sessions simultanées concerne les sessions simultanées pour les comptes du système. Il ne vise pas, toutefois, les sessions utilisateur simultanées uniques établies par l'intermédiaire de plusieurs comptes du système.

AC-11 — Verrouillage d’appareil (---)

Énoncés :

a. Empêcher d’autres accès au système [Sélection (un choix ou plus) : en procédant à un verrouillage d’appareil après {Affectation : délai défini par l’organisation} d’inactivité; en exigeant que l’utilisatrice ou utilisateur procède à un verrouillage d’appareil avant de laisser le système sans surveillance]
b. Préserver le verrouillage d’appareil jusqu’à ce que l’utilisatrice ou utilisateur rétablisse l’accès au moyen des procédures d’identification et d’authentification établies

Responsable : Aucun

Discussion :

Les verrouillages d’appareil sont des mesures temporaires servant à empêcher l’accès logique aux systèmes organisationnels lorsque les utilisatrices et utilisateurs arrêtent de travailler et ne se trouvent plus à proximité de ces systèmes et qu’ils préfèrent ne pas se déconnecter en raison de la nature temporaire de leur absence. Le verrouillage peut être mis en oeuvre au niveau du système d’exploitation ou de l’application. Un verrouillage de proximité peut être utilisé pour activer le verrouillage de l’appareil (par exemple, par le biais d’un appareil ou d’une clé électronique compatible Bluetooth). Le verrouillage d’appareil est initié par l’utilisatrice ou utilisateur. Il peut s’agir d’une opération basée sur des comportements ou des stratégies et, ainsi, il nécessite que l’utilisatrice ou utilisateur effectue une opération physique pour verrouiller son appareil. Les verrouillages d’appareil ne remplacent pas la fermeture de session sur le système, comme lorsque l’organisation exige que les utilisatrices et utilisateurs ferment leur session à la fin de leur journée de travail.

AC-11(01) — Masquage de l’affichage au moyen d’une image (---)

Énoncés :

Masquer, au moyen d’un verrouillage d’appareil, l’information auparavant visible à l’écran en utilisant une image visible.

Responsable : Aucun

Discussion :

Le masquage de l’affichage au moyen d’une image peut inclure des images statiques ou dynamiques, comme celles générées par les économiseurs d’écran, des photographies, des couleurs solides, une horloge, un indicateur de la charge de la pile ou un écran vide, ce qui assure que l’information contrôlée n’est pas affichée.

AC-12 — Fin de session (---)

Énoncés :

Mettre automatiquement fin à une session utilisateur après [Affectation : conditions ou événements déclenchant une déconnexion définis par l'organisation].

Responsable : Aucun

Discussion :

La fin de session porte sur l'interruption des sessions logiques ouvertes par les utilisatrices et utilisateurs, par opposition au contrôle SC-10 qui porte sur l'interruption des connexions réseau associées à des sessions de communication (c'est-à-dire déconnexion du réseau). Une session logique (pour l'accès local, réseau et distant) est lancée quand une utilisatrice ou un utilisateur (ou un processus exécuté en son nom) accède à un système organisationnel. De telles sessions de l'utilisatrice ou utilisateur peuvent être interrompues sans mettre fin aux sessions réseau. L'interruption de la session met fin à tous les processus liés à la session logique de l'utilisatrice ou utilisateur, à l'exception des processus créés précisément par ce dernier (c'est-à-dire la ou le propriétaire de la session) pour continuer après l'interruption de la session. Les conditions ou les événements déclenchant l'interruption automatique de la session comprennent la durée d'inactivité de l'utilisatrice ou utilisateur définie par l'organisation, des réponses ciblées à certains types d'incidents et la restriction de l'utilisation du système selon l'heure de la journée.

AC-12(01) — Fermetures de session exécutées par les utilisatrices et utilisateurs (---)

Énoncés :

Fournir une capacité de fermeture de session pour les sessions de communication lancées par les utilisatrices et utilisateurs lorsque l'authentification est utilisée pour accéder aux [Affectation : ressources d'information désignées par l'organisation].

Responsable : Aucun

Discussion :

Les ressources d'information auxquelles les utilisateurs accèdent par authentification comprennent les postes de travail locaux, les bases de données ainsi que les services Web ou sites Web protégés par mot de passe.

AC-12(02) — Message d’interruption (---)

Énoncés :

Afficher un message explicite de fermeture de session pour indiquer aux utilisatrices et utilisateurs l’interruption des sessions de communication authentifiées.

Responsable : Aucun

Discussion :

Les messages de fermeture de session pour l’accès au Web peuvent être affichés après l’interruption des sessions authentifiées. Cependant, pour certains types de sessions comme les sessions FTP, les systèmes envoient habituellement des messages de fermeture de session à titre de dernier message avant de mettre fin à la session.

AC-12(03) — Message d'avertissement de délai d'expiration (---)

Énoncés :

Afficher un message explicite aux utilisatrices et utilisateurs pour indiquer que la session prendra fin [Affectation : d'ici la fin de session définie par l'organisation].

Responsable : Aucun

Discussion :

Pour accroître l'utilisabilité, aviser les utilisatrices et utilisateurs que la fin de session est en attente et inviter ceux-ci à poursuivre la session. Le délai de fin de session en attente est basé sur les paramètres définis dans le contrôle de base AC-12.

AC-13 — Contrôle d’accès (---)

Énoncés :

Annulé : Intégré aux contrôles AC-02 et AU-06.

Responsable : Aucun

AC-14 — Opérations permises sans identification ni authentification (---)

Énoncés :

a. Identifier les [Affectation : opérations de l'utilisatrice ou utilisateur définies par l'organisation] que l'utilisatrice ou utilisateur peut exécuter dans le système sans devoir s'identifier ni s'authentifier, conformément aux fonctions opérationnelles et à la mission de l'organisation
b. Consigner et expliquer dans le plan de sécurité du système la logique sous-jacente qui permet à l'utilisatrice ou utilisateur d'effectuer des opérations qui ne nécessitent ni identification ni authentification

Responsable : Aucun

Discussion :

Les actions propres aux utilisatrices et utilisateurs peuvent être autorisées sans identification ni authentification si l'organisation détermine que l'identification et l'authentification ne sont pas requises pour de telles actions. Les organisations peuvent autoriser un nombre limité d'actions sans identification ni authentification, notamment lorsque des personnes accèdent à des sites Web publics ou à d'autres systèmesgouvernementaux accessibles au public, lorsque des personnes utilisent des téléphones mobiles pour recevoir des appels ou à la réception de télécopies. Les organisations identifient les actions nécessitant normalement une identification ou une authentification, mais permettent une dérogation à ces mécanismes dans certaines circonstances. Ces dérogations peuvent s'effectuer, par exemple, au moyen d'un commutateur physique, lisible par logiciel, qui permet de contourner la procédure d'ouverture de session et qui est protégé contre toute utilisation accidentelle ou non surveillée. Autoriser les actions sans identification ni authentification ne s'applique pas aux situations où l'identification et l'authentification ont déjà été effectuées et ne sont pas répétées. Il s'applique plutôt aux situations où les mécanismes d'identification et d'authentification n'ont pas encore eu lieu. Les organisations peuvent décider que les actions de l'utilisatrice ou utilisateur doivent être effectuées dans les systèmes organisationnels uniquement à l'aide de mécanismes d'identification et d'authentification. Par conséquent, la valeur pour les opérations d'attribution peut être « aucun ».

AC-14(01) — Usages indispensables (---)

Énoncés :

Annulé : Intégré au contrôle AC-14.

Responsable : Aucun

AC-15 — Marquage automatique (---)

Énoncés :

Annulé : Intégré au contrôle MP-03.

Responsable : Aucun

AC-16 — Attributs de sécurité et de protection de la vie privée (---)

Énoncés :

a. Fournir les moyens permettant d'associer les [Affectation : types d'attribut de sécurité et de protection de la vie privée définis par l'organisation] avec les [Affectation : valeurs des attributs de sécurité définies par l'organisation] pour l'information pendant qu'elle est stockée, traitée et/ou transmise
b. S'assurer que toutes les associations d'attribut de sécurité sont effectuées et conservées avec l'information
c. Établir les attributs de sécurité et de protection de la vie privée autorisés suivants à partir des attributs définis dans le contrôle AC-16A pour [Affectation : systèmes définis par l'organisation] : [Affectation : Attributs de sécurité et de protection de la vie privée définies par l'organisation]
d. Déterminer les valeurs ou les plages autorisées des attributs suivants pour chacun des attributs définis : [Affectation : valeurs des attributs ou des plages définies par l'organisation pour les attributs définis]
e. Vérifier les changements apportés aux attributs
f. Examiner les [Affectation : attributs de sécurité et de protection de la vie privée définis par l'organisation] aux fins d'applicabilité [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

L'information est représentée à l'interne dans les systèmes au moyen d'abstractions également appelées structures de données. Les structures de données internes peuvent représenter différents types d'entités actives et passives. Les entités actives, également appelées « sujets », sont habituellement associées à des personnes, à des dispositifs ou à des processus exécutés au nom des personnes. Les entités passives, également appelées « objets », sont habituellement associées à des structures de données comme des dossiers, des tampons, des fichiers, des canaux interprocessus et des ports de communications. Les attributs de sécurité (une forme de métadonnées) sont des abstractions des propriétés ou des caractéristiques d'entités actives et passives qui concernent la protection de l'information. Les attributs de protection de la vie privée, qui peuvent être utilisés de façon indépendante ou avec des attributs de sécurité, représentent les propriétés ou caractéristiques de base des entités actives ou passives en ce qui concerne la gestion des renseignements personnels. Les attributs peuvent être explicitement ou implicitement associés à l'information contenue dans le système de l'organisation ou ses composants. Ces attributs peuvent être associés à des entités actives (c'est-à-dire des sujets) qui ont le potentiel d'envoyer ou de recevoir de l'information, de faire circuler l'information entre des objets ou de changer l'état du système. Ils peuvent également être associés à des entités passives (c'est-à-dire des objets) qui contiennent ou reçoivent de l'information. L'association d'attributs à des sujets et objets s'appelle une liaison et fait habituellement partie de l'établissement de la valeur de l'attribut et de son type. Lorsqu'ils sont liés aux données ou à l'information, les attributs permettent de renforcer les stratégies de sécurité et de protection de la vie privée pour le contrôle de l'accès et du flux d'information, ce qui comprend les limites de conservation des données, les utilisations autorisées des renseignements personnels et l'identification des renseignements personnels dans les objets de données. Un tel renforcement s'effectue dans le cadre des processus organisationnels ou des fonctions ou mécanismes du système. Les techniques de liaison que les systèmes mettent en oeuvre nuisent à la force de la liaison entre les attributs et l'information. La force de la liaison et l'assurance associée aux techniques de liaison jouent des rôles importants dans la confiance qu'accordent les organisations au processus d'application du contrôle de flux d'information. Les techniques de liaison ont une incidence sur le nombre et le degré d'examens supplémentaires que devront exécuter les organisations. Le contenu ou les valeurs attribuées aux attributs peuvent avoir une incidence directe sur la capacité des personnes à accéder à l'information de l'organisation. Les organisations peuvent définir les types d'attributs requis pour que les systèmes appuient les fonctions liées à sa mission ou à ses activités. Plusieurs valeurs peuvent être assignées à un attribut de sécurité. En précisant les valeurs et les intervalles d'attribut permis, l'organisation s'assure que les valeurs d'attributs sont pertinentes et importantes. L'étiquetage désigne l'association d'attributs avec les sujets et objets représentés par des structures de données internes dans les systèmes. Il permet de faciliter l'application des stratégies de sécurité et de protection de la vie privée de l'information basées sur les systèmes. Les étiquettes comprennent la classification de l'information selon les exigences juridiques et de conformité (par exemple, TRÈS SECRET, SECRET, CONFIDENTIEL, PROTÉGÉ), le niveau d'incidence de l'information, l'information de bien de grande importance, les autorisations d'accès, la nationalité, la protection du cycle de vie des données (c'est-à-dire chiffrement et expiration des données), les autorisations de traitement des renseignements personnels, y compris le consentement au traitement des renseignements personnels, et l'affiliation des entrepreneures et entrepreneurs. Le marquage est un terme associé à l'étiquetage. Il désigne l'association d'attributs à des objets dans une forme lisible par un humain et qui sont affichés sur les supports d'un système. Le marquage permet d'assurer une application manuelle ou basée sur les procédures ou les processus des stratégies de sécurité et de protection de la vie privée de l'information. Les étiquettes de sécurité et de protection de la vie privée peuvent avoir la même valeur que le marquage des supports (par exemple, TRÈS SECRET, SECRET, CONFIDENTIEL). Prière de consulter le contrôle MP-03 (Marquage des supports).

AC-16(01) — Association dynamique d’attribut (---)

Énoncés :

Associer de manière dynamique les attributs de sécurité et de protection de la vie privée aux [Affectation : sujets et objets définis par l’organisation] conformément aux stratégies de sécurité et de protection de la vie privée suivantes au moment où l’information est créée et combinée : [Affectation : stratégies de sécurité et de protection de la vie privée définies par l’organisation].

Responsable : Aucun

Discussion :

L’organisation peut faire appel à l’association dynamique d’attributs lorsque les caractéristiques de sécurité de l’information changent au fil du temps. Les attributs peuvent changer en raison de problèmes relatifs au regroupement de l’information (c’est-à-dire les caractéristiques de sécurité des éléments individuels de données sont différentes des éléments combinés), ainsi qu’en raison de changements liés aux autorisations d’accès individuels (c’est-à-dire les droits d’accès), à la catégorie de sécurité de l’information, ou de changements liés à la sécurité ou aux stratégies de sécurité ou de protection de la vie privée. Les attributs peuvent également changer selon la situation.

AC-16(02) — Changements aux valeurs d’attribut par des personnes autorisées (---)

Énoncés :

Fournir à des personnes autorisées (ou à des processus exécutés au nom des personnes) la capacité de définir ou de changer la valeur des attributs de sécurité et de protection de la vie privée connexes.

Responsable : Aucun

Discussion :

Le contenu ou les valeurs attribuées aux attributs peuvent avoir une incidence directe sur la capacité des personnes à accéder à l’information de l’organisation. Par conséquent, il est important que les systèmes soient capables de fournir uniquement aux personnes autorisées la capacité de créer ou de modifier des attributs.

AC-16(03) — Maintenance des associations d'attributs par système (---)

Énoncés :

Maintenir l'intégrité des [Affectation : attributs de sécurité et de protection de la vie privée définis par l'organisation] et l'association de ceux-ci aux [Affectation : sujets et objets définis par l'organisation].

Responsable : Aucun

Discussion :

Le maintien de l'intégrité des attributs de sécurité et de protection de la vie privée et de leur association à des sujets et à des objets avec un degré d'assurance suffisant aide à garantir que les associations d'attribut peuvent servir de base aux opérations automatisées liées aux stratégies. L'intégrité d'éléments précis, comme des fichiers de configuration de sécurité, peut être maintenue au moyen d'un mécanisme de surveillance de l'intégrité qui détecte des anomalies et des changements qui dévient de bases de référence valides. Les opérations automatisées liées aux stratégies incluent les expirations de date de conservation, les décisions liées au contrôle d'accès, au contrôle de flux d'information et à la divulgation d'information.

AC-16(04) — Association d’attributs par personnes autorisées (---)

Énoncés :

Fournir les moyens d’associer des [Affectation : Attributs de sécurité et de protection de la vie privée définies par l’organisation] aux [Affectation : sujets et objets définis par l’organisation] effectuée par des personnes autorisées (ou par des processus exécutés en leur nom).

Responsable : Aucun

Discussion :

En général, les systèmes fournissent les moyens aux utilisatrices et utilisateurs privilégiés d’accorder des attributs de sécurité et de protection de la vie privée aux sujets (par exemple, utilisatrices ou utilisateurs) et aux objets (par exemple, répertoires, fichiers et ports) définis par le système. Certains systèmes offrent aux utilisatrices et utilisateurs généraux une capacité supplémentaire permettant d’accorder des attributs de sécurité et de protection de la vie privée à des objets additionnels (par exemple, fichiers, courriels). L’association d’attributs par des personnes autorisées est décrite dans la documentation sur la conception. Le soutien fourni par les systèmes peut comprendre d’inviter les utilisatrices et utilisateurs à sélectionner des attributs de sécurité et de protection de la vie privée à associer à des objets d’information, d’employer des mécanismes automatisés pour catégoriser l’information avec les attributs en fonction des politiques définies ou de veiller à ce que la combinaison d’attributs de sécurité ou de protection de la vie privée sélectionnée soit valide. Les organisations considèrent la création, la suppression ou la modification d’attributs lorsqu’elles définissent les événements vérifiables.

AC-16(05) — Affichage d'attributs des objets transmis à des dispositifs de sortie (---)

Énoncés :

Afficher sous forme lisible les attributs de sécurité et de protection de la vie privée de chaque objet que le système transmet à des dispositifs de sortie afin d'identifier les [Affectation : instructions spéciales de diffusion, de traitement ou de distribution définies par l'organisation] conformément aux [Affectation : conventions d'appellation standard, en langage lisible, définies par l'organisation].

Responsable : Aucun

Discussion :

Les sorties du système comprennent les pages d'imprimante, les saisies d'écran ou des éléments équivalents. Les dispositifs de sortie du système comprennent les imprimantes, les ordinateurs blocs-notes, les affichages vidéo, les téléphones intelligents et les tablettes. Afin d'atténuer les risques d'exposition non autorisée d'information (par exemple, espionnage par-dessus l'épaule), les sorties affichent des valeurs complètes d'attributs lorsque l'abonnée ou abonné les décèle.

AC-16(06) — Maintien des associations d'attributs (---)

Énoncés :

Permettre au personnel d'associer les [Affectation : attributs de sécurité et de protection de la vie privée définis par l'organisation] aux [Affectation : sujets et objets définis par l'organisation] et de maintenir cette association, conformément aux [Affectation : stratégies de sécurité et de sécurité définies par l'organisation].

Responsable : Aucun

Discussion :

Maintenir les associations d'attributs exige que l'utilisatrice ou utilisateur (par opposition au système) maintienne les associations d'attributs de sécurité et de protection de la vie privée aux sujets et objets.

AC-16(07) — Interprétation uniforme des attributs (---)

Énoncés :

Fournir une interprétation uniforme des attributs de sécurité et de protection de la vie privée transmis entre les composants du système distribués.

Responsable : Aucun

Discussion :

Pour appliquer des stratégies de sécurité et de sécurité dans de multiples composants de système au sein de systèmes distribués, les organisations fournissent une interprétation uniforme des attributs de sécurité qui sont utilisés dans les décisions d'application de flux et de l'accès. Les organisations peuvent établir des ententes et des processus pour aider à s'assurer que tous les composants de systèmes distribués mettent en oeuvre des attributs avec des interprétations uniformes dans les opérations automatisées d'application de flux et de l'accès.

AC-16(08) — Techniques et technologies d’association (---)

Énoncés :

Mettre en oeuvre des [Affectation : techniques et technologies définies par l’organisation] en associant des attributs de sécurité et de protection de la vie privée à l’information.

Responsable : Aucun

Discussion :

L’association d’attributs de sécurité et de protection de la vie privée à de l’information dans les systèmes est très importante en ce qui a trait à l’exécution des opérations automatisées d’application de flux et d’accès. L’association de tels attributs à l’information (par exemple, liaison) peut être accomplie au moyen de technologies ou de techniques offrant différents niveaux d’assurance. Par exemple, les systèmes peuvent établir des liaisons cryptographiques entre des attributs et de l’information au moyen de signatures numériques et des clés cryptographiques connexes protégées par des dispositifs matériels (également appelés base matérielle sécurisée).

AC-16(09) — Réaffectation d'attribut – Mécanismes remaniés (---)

Énoncés :

Changer les attributs de sécurité et de protection de la vie privée associés à l'information uniquement par des mécanismes remaniés validés au moyen de [Affectation : techniques ou procédures définies par l'organisation].

Responsable : Aucun

Discussion :

Un mécanisme remanié est un processus de confiance autorisé à reclassifier et réétiqueter des données conformément à une exception définie sur le plan de la stratégie. Les organisations emploient des mécanismes remaniés validés afin de fournir les niveaux d'assurance requis pour les activités de réattribution d'attribut. La validation est facilitée si les mécanismes remaniés sont monofonctions et ont des fonctions limitées. Étant donné que les changements d'attributs de sécurité et de protection de la vie privée peuvent avoir une incidence directe sur les opérations d'application des stratégies de sécurité, l'utilisation de mécanismes remaniés fiables est nécessaire afin de s'assurer que ces mécanismes fonctionnent correctement et uniformément.

AC-16(10) — Configuration d’attribut par des personnes autorisées (---)

Énoncés :

Fournir aux personnes autorisées la capacité de définir ou de changer le type et la valeur des attributs de sécurité et de protection de la vie privée disponibles pouvant être associés à des sujets et à des objets.

Responsable : Aucun

Discussion :

Le contenu ou les valeurs attribuées aux attributs de sécurité et de protection de la vie privée peuvent avoir une incidence directe sur la capacité des personnes d’accéder à l’information de l’organisation. Par conséquent, il est important que les systèmes soient capables de fournir uniquement aux personnes autorisées la capacité de créer ou de modifier le type et la valeur des attributs pouvant être associés à des sujets et à des objets.

AC-17 — Accès à distance (Nc--)

Énoncés :

a. Définir et consigner les restrictions d'utilisation, les exigences en matière de configuration et de connexion, ainsi que les directives de mise en oeuvre de chaque type d'accès à distance autorisé;
b. Autoriser chaque type d'accès à distance au système avant d'autoriser de telles connexions.

Responsable : Aucun

Discussion :

Par accès à distance (ou accès distant), on entend l'accès des utilisatrices et utilisateurs (ou des processus exécutés en leur nom) aux systèmes organisationnels au moyen de réseaux externes, comme Internet. Les types d'accès à distance comprennent l'accès par ligne commutée, à large bande et sans fil. Les organisations utilisent des réseaux privés virtuels (RPV) chiffrés pour augmenter la confidentialité et l'intégrité des connexions à distance. L'utilisation de RPV chiffrés permet à l'organisation de s'assurer qu'elle peut traiter efficacement ce type de connexion comme des réseaux internes si les mécanismes de chiffrement utilisés sont mis en oeuvre conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Cela dit, les connexions RPV traversent des réseaux externes et les RPV chiffrés n'augmentent pas la disponibilité des connexions distantes. Les RPV dotés de tunnels chiffrés peuvent également avoir une incidence sur la capacité de l'organisation à surveiller adéquatement le trafic de communication réseau à des fins de détection de programmes malveillants. Les contrôles d'accès à distance s'appliquent aux systèmes autres que les serveurs Web publics ou les systèmes conçus pour l'accès public. Chaque type d'accès à distance exige une autorisation avant de permettre l'accès distant, sans préciser les formats de cette autorisation. Bien que les organisations puissent avoir recours à des ententes sur la sécurité des échanges d'information et des connexions aux systèmes pour gérer l'accès à distance aux autres systèmes, ces ententes relèvent du contrôle CA-03. Le contrôle AC-03 porte sur l'application des restrictions d'accès à distance.

AC-17(01) — Surveillance et contrôle (---)

Énoncés :

Utiliser des mécanismes automatisés pour faciliter la surveillance et le contrôle des méthodes d'accès à distance.

Responsable : Aucun

Discussion :

La surveillance et le contrôle des méthodes d'accès à distance permettent aux organisations de détecter les attaques et de s'assurer du respect constant des stratégies d'accès à distance grâce à la vérification des activités de connexion des utilisatrices et utilisateurs distants sur une variété de composants du système, y compris des serveurs, des ordinateurs blocs-notes, des postes de travail, des téléphones intelligents et des tablettes. La journalisation des données de vérification pour l'accès à distance est appliquée par le contrôle AU-
02. Les événements vérifiables sont définis dans le contrôle AU-02A.

AC-17(02) — Protection de la confidentialité et de l'intégrité au moyen du chiffrement (---)

Énoncés :

Mettre en oeuvre des mécanismes cryptographiques pour protéger la confidentialité et l'intégrité des sessions d'accès à distance.

Responsable : Aucun

Discussion :

Les RPV peuvent servir à protéger la confidentialité et l'intégrité des sessions d'accès à distance. Le protocole TLS est un exemple de protocole cryptographique qui assure la sécurité des communications de bout à bout sur des réseaux et il est utilisé pour les communications Internet et les transactions en ligne.

AC-17(03) — Points de contrôle d’accès gérés (---)

Énoncés :

Acheminer l’accès distant au moyen de points de contrôle d’accès réseau autorisés et gérés.

Responsable : Aucun

Discussion :

Les organisations tiennent compte d’une solution de points de contrôle d’accès gérés pour les connexions réseau externes puisque la limitation du nombre de points de contrôle d’accès pour les accès à distance réduit la superficie d’attaque des organisations.

AC-17(04) — Commandes et accès privilégiés (---)

Énoncés :

a. Autorise l'exécution de commandes privilégiées et de l'accès à l'information liée à la sécurité au moyen de l'accès à distance seulement dans un format qui fournit des preuves justificatives de confiance, et ce, pour les besoins suivants : [Affectation : besoins définis par l'organisation]
b. Consigner la justification pour cet accès dans le plan de sécurité du système

Responsable : Aucun

Discussion :

L'accès distant à des systèmes représente une vulnérabilité potentielle importante pouvant être exploitée par des adversaires. Ainsi, la restriction des commandes et des accès privilégiés à l'information liée à la sécurité au moyen d'un accès à distance réduit l'exposition des organisations et la vulnérabilité aux menaces provenant des adversaires.

AC-17(05) — Surveillance pour connexions non autorisées (---)

Énoncés :

Annulé : Intégré au contrôle SI-04.

Responsable : Aucun

AC-17(06) — Protection de l’information sur les mécanismes (---)

Énoncés :

Protéger l’information sur les mécanismes d’accès à distance contre toute utilisation et divulgation non autorisée.

Responsable : Aucun

Discussion :

L’accès à distance à l’information organisationnelle par des entités non organisationnelles peut accroître les risques d’utilisation et de divulgation non autorisées sur les mécanismes d’accès à distance. L’organisation considère d’inclure des exigences en matière d’accès à distance dans les ententes d’échange d’information avec d’autres organisations, le cas échéant. Ces exigences peuvent aussi être intégrées aux règles de comportement (voir le contrôle PL-04) et aux ententes d’accès (voir le contrôle PS-06).

AC-17(07) — Protection supplémentaire pour l'accès aux fonctions de sécurité (---)

Énoncés :

Annulé : Intégré au contrôle AC-03(10).

Responsable : Aucun

AC-17(08) — Désactiver les protocoles réseau non sécurisés (---)

Énoncés :

Annulé : Intégré au contrôle CM-07.

Responsable : Aucun

AC-17(09) — Déconnecter ou désactiver l'accès (---)

Énoncés :

Fournir la capacité de déconnecter ou de désactiver l'accès à distance au système dans un délai de [Affectation : délai défini par l'organisation].

Responsable : Aucun

Discussion :

La vitesse de la déconnexion ou de la désactivation du système dépend de la criticité des fonctions liées à la mission ou aux activités, ainsi que de la nécessité d'éliminer l'accès distant immédiat ou futur aux systèmes.

AC-17(10) — Authentification des commandes à distance (---)

Énoncés :

Mettre en place les [Affectation : mécanismes définis par l'organisation] pour authentifier [Affectation : commandes à distance définies par l'organisation].

Responsable : Aucun

Discussion :

L'authentification de commandes à distance assure une protection contre les commandes non autorisées et la réexécution des commandes autorisées. La capacité d'authentification est importante pour les systèmes à distance dont la perte, le mauvais fonctionnement, la mauvaise conduite ou l'exploitation pourraient avoir des conséquences immédiates ou sérieuses, par exemple, blessures, mort, dommages à la propriété, perte de biens de grande valeur, échec de missions ou de fonctions opérationnelles, ou compromission d'information classifiée ou protégée. Les mécanismes d'authentification des commandes à distance font en sorte que le système accepte et exécute les commandes dans l'ordre prévu. De plus, le système ne traite que les commandes autorisées et rejette les commandes non autorisées. Des mécanismes cryptographiques peuvent être employés, par exemple, pour authentifier les commandes à distance.

AC-17(400) — Accès à distance à des comptes privilégiés (---)

Énoncés :

L'accès à distance à des comptes privilégiés s'effectue à partir de consoles de gestion spécialisées utilisées exclusivement à cette fin.

Responsable : Aucun

Discussion :

L'accès à distance à des comptes privilégiés s'effectue à partir de consoles de gestion spécialisées régies entièrement par les stratégies de sécurité du système et utilisées exclusivement à cette fin (par exemple, l'accès à Internet n'est pas autorisé). Dans le contexte de ce contrôle, accès à distance signifie tout ce qui n'est pas local par rapport à l'hôte.

AC-18 — Accès sans fil (---)

Énoncés :

a. Établir les restrictions d'utilisation, les exigences en matière de configuration et de connexion, ainsi que les directives de mise en oeuvre pour chaque type d'accès sans fil
b. Autoriser chaque type d'accès sans fil au système avant d'autoriser de telles connexions

Responsable : Aucun

Discussion :

Les technologies sans fil comprennent les hyperfréquences, la radiocommunication à commutation de paquets (bande d'ondes décimétriques ou bande d'ondes métriques), 802.11x et Bluetooth. Les réseaux sans fil utilisent des protocoles d'authentification afin de fournir une protection au moyen d'un authentifiant et d'une authentification mutuelle.

AC-18(01) — Authentification et chiffrement (---)

Énoncés :

Protéger l'accès sans fil au système au moyen de l'authentification des [Sélection (un choix ou plus) : utilisatrices et utilisateurs; dispositifs] et du chiffrement.

Responsable : Aucun

Discussion :

Les capacités de réseau sans fil représentent une vulnérabilité potentielle importante pouvant être exploitée par des adversaires. Afin de protéger les systèmes avec des points d'accès sans fil, un mécanisme rigoureux d'authentification des utilisatrices et utilisateurs et des appareils, avec un chiffrement robuste peuvent réduire sensiblement les menaces que font peser les adversaires exploitant des technologies sans fil.

AC-18(02) — Surveillance des connexions non autorisées (---)

Énoncés :

Annulé : Intégré au contrôle SI-04.

Responsable : Aucun

AC-18(03) — Désactivation du réseautage sans fil (---)

Énoncés :

Désactiver, lorsqu'on ne prévoit pas les utiliser, les capacités de réseautage sans fil intégrées aux composants du système avant leur remise et leur déploiement.

Responsable : Aucun

Discussion :

Les capacités de réseau sans fil intégrées aux composants de systèmes représentent une vulnérabilité potentielle importante pouvant être exploitée par des adversaires. La désactivation des capacités sans fil non nécessaires à la mission ou aux activités peut réduire sensiblement les menaces que font peser les adversaires exploitant des technologies sans fil.

AC-18(04) — Restriction des configurations par les utilisatrices et utilisateurs (---)

Énoncés :

Identifier les utilisatrices et utilisateurs et les autoriser explicitement à configurer eux-mêmes les capacités de réseautage sans fil.

Responsable : Aucun

Discussion :

Les autorisations organisationnelles permettant aux utilisateurs sélectionnés de configurer les capacités de réseautage sans fil sont appliquées en partie par les mécanismes d'application de l'accès employés dans les systèmes organisationnels.

AC-18(05) — Antennes et puissance de transmission (---)

Énoncés :

Sélectionner des antennes radio et calibrer la puissance de transmission afin de réduire la probabilité que les signaux puissent être reçus en dehors des frontières que contrôle l'organisation.

Responsable : Aucun

Discussion :

Les mesures pouvant être prises pour limiter l'utilisation non autorisée de communications sans fil en dehors des frontières contrôlées par l'organisation comprennent la réduction de la puissance des transmissions sans fil pour qu'elles risquent moins d'émettre un signal qui pourrait être utilisé à l'extérieur du périmètre physique de l'organisation, l'utilisation de mesures telles que la sécurité des émissions pour contrôler les émissions sans fil, et l'utilisation d'antennes directionnelles ou de mise en forme de faisceaux qui réduisent la probabilité que des personnes non prévues réussissent à intercepter les signaux. Avant de prendre de telles mesures d'atténuation, l'organisation peut mener des enquêtes sans fil périodiques pour comprendre le profil de radiofréquence des systèmes organisationnels ainsi que d'autres systèmes qui pourraient être en fonction dans le secteur.

AC-19 — Contrôle d'accès pour les appareils mobiles (Nc--)

Énoncés :

a. Établir les exigences en matière de configuration et de connexion, ainsi que les directives de mise en oeuvre des appareils mobiles contrôlés par l'organisation à inclure lorsque ces appareils se trouvent à l'extérieur des zones contrôlées
b. Autoriser les connexions d'appareils mobiles aux systèmes organisationnels

Responsable : Aucun

Discussion :

Un appareil mobile est un dispositif informatique de petite taille qui peut facilement être transporté par une personne. Il est conçu pour fonctionner sans connexion physique et il dispose d'un stockage de données local, fixe ou amovible. Il comprend également une source d'alimentation autonome. Les fonctionnalités des appareils mobiles peuvent également comprendre des capacités de communication vocale, des capteurs embarqués permettant aux appareils de recueillir des données et/ou des fonctions intégrées de synchronisation de données locales avec des emplacements distants. Les téléphones intelligents et les tablettes sont des exemples d'appareils mobiles. Les appareils mobiles sont typiquement associés à une seule personne et certains renseignements sont définis comme étant personnels. Par exemple, les appareils mobiles peuvent localiser l'accès en activant l'identification de la géolocalisation de l'utilisatrice ou utilisateur. De plus, comme certains appareils mobiles fournis à des fins professionnelles activent les profils personnels, les ministères gouvernementaux devraient mettre en place des stratégies et des procédures pour documenter la garde et le contrôle des transactions personnelles effectuées dans le profil personnel à partir de tels appareils. Les capacités de traitement, de stockage et de transmission de l'appareil mobile sont comparables à un sous-ensemble de postes de travail, selon la nature et l'utilisation prévue de l'appareil. La protection et le contrôle des appareils mobiles sont basés sur les comportements et les stratégies, et nécessitent que les utilisatrices et utilisateurs effectuent des opérations physiques afin de protéger et de contrôler leurs appareils lorsqu'ils se trouvent à l'extérieur des zones contrôlées. Les zones contrôlées sont des espaces dans lesquels les organisations appliquent des contrôles physiques ou procéduraux afin de respecter les exigences établies pour la protection de l'information et des systèmes. En raison de la grande variété d'appareils mobiles, y compris leur vaste gamme de caractéristiques et de capacités, les restrictions organisationnelles peuvent varier en fonction des classes ou des types d'appareils. Les restrictions d'utilisation et les conseils de mises en oeuvre propres aux appareils mobiles comprennent notamment la gestion des configurations, l'identification et l'authentification des appareils, la mise en oeuvre obligatoire de logiciels de protection, l'analyse des appareils afin de détecter les programmes malveillants, la mise à jour des logiciels antivirus, la recherche des mises à jour et des correctifs critiques, la vérification de l'intégrité du système d'exploitation de base et possiblement d'autres logiciels résidents, et la désactivation du matériel qui n'est pas nécessaire. Les restrictions concernant l'utilisation et l'autorisation d'accès peuvent varier selon les systèmes organisationnels. Par exemple, l'organisation peut autoriser la connexion des appareils mobiles à ses réseaux et imposer un ensemble de restrictions concernant l'utilisation, tandis qu'une ou un propriétaire de système peut refuser la connexion d'appareils mobiles à des applications en particulier ou imposer des restrictions additionnelles avant d'autoriser la connexion d'appareils mobiles à un système. Pour protéger adéquatement les appareils mobiles, il faut faire plus que se conformer aux exigences précisées dans le contrôle AC-

19. Plusieurs mesures de protection des appareils mobiles sont comprises dans d'autres contrôles. Le contrôle AC-20 porte sur les appareils mobiles qui ne sont pas contrôlés par les organisations. Le contrôle AC-08 dresse la liste des exigences relatives aux avis à envoyer par rapport à la collecte des renseignements personnels associés à l'utilisation de téléphones cellulaires professionnels fournis par le gouvernement.

AC-19(01) — Utilisation de dispositifs de stockage portatifs et accessibles en écriture (---)

Énoncés :

Annulé : Intégré au contrôle MP-07.

Responsable : Aucun

AC-19(02) — Utilisation de dispositifs de stockage portatifs appartenant à des particuliers (---)

Énoncés :

Annulé : Intégré au contrôle MP-07.

Responsable : Aucun

AC-19(03) — Utilisation de dispositifs de stockage portatifs sans propriétaire identifiable (---)

Énoncés :

Annulé : Intégré au contrôle MP-07.

Responsable : Aucun

AC-19(04) — Restrictions liées à l'information classifiée (---)

Énoncés :

a. Interdire l'utilisation d'appareils mobiles non classifiés dans les installations qui hébergent des systèmes qui traitent, stockent ou transmettent de l'information classifiée, sauf si l'autorité responsable le permet
b. Appliquer par le biais de l'autorité responsable les restrictions ci-après aux personnes autorisées à utiliser des appareils mobiles non classifiés dans les installations hébergeant des systèmes qui traitent, stockent ou transmettent de l'information classifiée :

1. il est interdit de connecter des appareils mobiles non classifiés à des systèmes classifiés
2. la connexion d'appareils mobiles non classifiés à des systèmes non classifiés requiert l'approbation de l'autorité responsable
3. il est interdit d'utiliser des modems internes ou externes, ou des interfaces sans fil, avec les appareils mobiles non classifiés
4. les appareils mobiles non classifiés et l'information qui y est stockée peuvent faire l'objet d'examens ou d'inspections aléatoires par [Affectation : agentes et agents de sécurité définis par l'organisation]; si l'inspection confirme la présence d'information classifiée, la stratégie de traitement des incidents est appliquée

c. Limiter la connexion d'appareils mobiles classifiés à des systèmes classifiés conformément aux [Affectation : stratégies de sécurité définies par l'organisation]

Responsable : Aucun

AC-19(05) — Chiffrement complet des appareils ou chiffrement des contenants (Nc--)

Énoncés :

Employer le [Sélection (un choix ou plus) : chiffrement complet des appareils ; chiffrement des contenants] pour protéger la confidentialité et l'intégrité de l'information sur les [Affectation : appareils mobiles définis par l'organisation].

Responsable : Aucun

Discussion :

Le chiffrement des contenants fournit une approche à granularité fine au chiffrement des données et de l'information sur les appareils mobiles, y compris le chiffrement des structures de données sélectionnées, telles que les fichiers, les dossiers et les champs.

AC-19(400) — Appareils sans fil (---)

Énoncés :

Annulé : Transféré sous le contrôle SC-42(400).

Responsable : Aucun

AC-20 — Utilisation de systèmes externes (---)

Énoncés :

a. [Sélection (un choix ou plus) : Établir les {Affectation : conditions générales d'utilisation définies par l'organisation}; identifier les {Affectation : contrôles définis par l'organisation dont la mise en place est présumée sur les systèmes externes}], conformément aux relations d'approbation établies avec les autres organisations qui possèdent, exploitent et/ou maintiennent les systèmes externes, de manière à ce que les personnes autorisées puissent faire ce qui suit :

1. accéder au système à partir des systèmes externes

2. traiter, stocker ou transmettre de l'information contrôlée par l'organisation au moyen de systèmes externes

b. Interdire l'utilisation de [Affectation : types de systèmes externes définis par l'organisation]

Responsable : Aucun

Discussion :

Par systèmes externes, on entend les systèmes qui sont utilisés par des systèmes organisationnels, sans en faire partie, et sur lesquels l'organisation n'exerce aucun contrôle direct sur le plan de la mise en oeuvre des contrôles requis ou de l'évaluation de l'efficacité des contrôles. Les systèmes externes comprennent les systèmes, les composants ou les appareils appartenant à des particuliers; les dispositifs de calcul et de communication appartenant à des intérêts privés dans des installations commerciales ou publiques; les systèmes appartenant à des organismes non gouvernementaux ou sous le contrôle de tels organismes; les systèmes gérés par des entrepreneures et entrepreneurs; et les systèmes d'information gouvernementaux qui ne sont ni la propriété des organisations, ni exploités ou contrôlés sous leur supervision directe et leur autorité. Les systèmes externes comprennent également les systèmes qui sont la propriété d'autres éléments de la même organisation (ou exploités par ces derniers) et les systèmes au sein de l'organisation dont les limites d'autorisation sont différentes. Les organisations ont l'option d'interdire l'utilisation de tous les types de systèmes externes ou de certains types de systèmes externes (par exemple, interdire l'utilisation de systèmes externes qui n'appartiennent pas à l'organisation ou interdire l'utilisation de systèmes appartenant à des particuliers). Dans le cas de certains systèmes externes (c'est-à-dire ceux exploités par d'autres organisations), les relations d'approbation établies entre ces organisations et l'organisation concernée peuvent être telles qu'aucune condition générale d'utilisation explicite n'est requise. Les systèmes dans ces organisations ne peuvent pas être considérés comme des systèmes externes. Ces situations se produisent, par exemple, lorsque des ententes d'échange d'information (implicites ou explicites) existaient déjà et avaient été établies entre les organisations ou composants, ou lorsque de telles ententes sont stipulées dans les lois, les décrets, les directives, la réglementation, les politiques ou les normes applicables. Les personnes autorisées comprennent notamment le personnel de l'organisation, les entrepreneures et entrepreneurs ou toute autre personne autorisée à accéder aux systèmes organisationnels et à qui les organisations sont en droit d'imposer des règles de conduite précises quant à l'accès au système. Les restrictions que les organisations imposent aux personnes autorisées n'ont pas besoin d'être uniformes puisqu'elles peuvent varier selon les relations de confiance entre les organisations. Par conséquent, les organisations peuvent choisir d'imposer aux entrepreneures et entrepreneurs des restrictions de sécurité différentes de celles imposées à un gouvernement fédéral, provincial ou municipal. Les systèmes externes utilisés pour accéder aux interfaces publiques qui mènent aux systèmes de l'organisation ne sont pas visés par le contrôle AC-

20. Les organisations établissent les conditions générales d'utilisation des systèmes externes conformément à leurs stratégies et procédures de sécurité. Au minimum, les conditions générales d'utilisation portent sur les types d'applications accessibles sur les systèmes organisationnels à partir des systèmes externes, et la catégorie de sécurité la plus élevée de l'information qui peut être traitée, stockée ou transmise dans des systèmes externes. Si les organisations ne peuvent pas établir des conditions générales d'utilisation avec les propriétaires des systèmes externes, elles peuvent imposer des restrictions au personnel utilisant ces systèmes externes.

AC-20(01) — Limites relatives à l'utilisation autorisée (---)

Énoncés :

Permettre aux personnes autorisées d'utiliser un système externe afin d'accéder au système ou afin de traiter, de stocker ou de transmettre de l'information contrôlée par l'organisation seulement après les opérations suivantes :
a. vérifier que les contrôles ont été mis en oeuvre dans le système externe tel qu'il est stipulé dans les stratégies de sécurité et de protection de la vie privée et les plans de sécurité et de protection de la vie privée
b. conserver les ententes approuvées de connexion au système ou de traitement avec l'entité organisationnelle qui héberge le système externe

Responsable : Aucun

Discussion :

Limiter l'usage autorisé permet de reconnaître que dans certaines circonstances, des utilisatrices et utilisateurs de systèmes externes ont besoin d'accéder aux systèmes organisationnels. Les organisations doivent avoir l'assurance que les systèmes externes comportent les contrôles nécessaires afin qu'ils ne compromettent pas ou n'endommagent pas les systèmes de l'organisation, ou encore qu'ils ne nuisent pas à ceux-ci. La vérification visant à s'assurer que les contrôles requis ont été mis en oeuvre peut être réalisée par des évaluations externes et indépendantes, des attestations ou d'autres moyens, selon le degré de certitude dont ont besoin les organisations.

AC-20(02) — Dispositifs de stockage portatifs – Utilisation restreinte (---)

Énoncés :

Restreindre l'utilisation de dispositifs de stockage portatifs contrôlés par l'organisation aux personnes autorisées pour les systèmes externes conformément aux [Affectation : restrictions définies par l'organisation].

Responsable : Aucun

Discussion :

Les limites ayant trait à l'utilisation des dispositifs de stockage portatifs contrôlés par l'organisation dans les systèmes externes incluent les restrictions sur la façon dont les dispositifs peuvent être utilisés et les conditions qui s'y rattachent.

AC-20(03) — Systèmes ne faisant pas partie de l'organisation – Utilisation restreinte (Nc--)

Énoncés :

Limiter l'utilisation de systèmes ne faisant pas partie de l'organisation ou de composants de systèmes qui traitent, stockent ou transmettent de l'information de l'organisation au moyen de [Affectation : restrictions définies par l'organisation].

Responsable : Aucun

Discussion :

Les composants de systèmes ou les systèmes ne faisant pas partie de l'organisation comprennent les systèmes ou les composants de systèmes appartenant à d'autres organisations ainsi que des dispositifs personnels. L'utilisation de tels systèmes ou composants comporte des risques. Dans certains cas, le risque est suffisamment élevé pour en interdire l'utilisation (voir le code AC-20B). Dans d'autres cas, l'utilisation de tels systèmes ou composants de systèmes peut être autorisée, mais avec certaines limitations. Les restrictions comprennent l'exigence de mettre en oeuvre des contrôles approuvés avant d'autoriser de telles connexions de composants et de systèmes ne faisant pas partie de l'organisation; la limitation de l'accès à certains types d'information, de services ou d'applications; l'utilisation de techniques de virtualisation pour limiter le traitement et le stockage d'activités sur des serveurs ou des composants de systèmes fournis par l'organisation; l'acceptation des modalités d'utilisation. Les organisations consultent la Commission d'accès à l'information du Québec (CAI) au sujet des enjeux juridiques associés à l'utilisation d'appareils personnels, y compris les exigences relatives à l'analyse judiciaire dans le cadre d'enquêtes à la suite d'un incident.

AC-20(04) — Dispositifs de stockage accessibles par réseau – Utilisation interdite (---)

Énoncés :

Interdire l'utilisation de [Affectation : dispositifs de stockage accessibles par réseau, définis par l'organisation] dans des systèmes externes.

Responsable : Aucun

Discussion :

Les dispositifs de stockage accessibles par réseau dans des systèmes externes comprennent les dispositifs de stockage en ligne dans des systèmes infonuagiques publics, hybrides ou communautaires.

AC-20(05) — Dispositifs de stockage portatifs – Utilisation interdite (---)

Énoncés :

Interdire l'utilisation de dispositifs de stockage portatifs contrôlés par l'organisation aux personnes autorisées pour les systèmes externes.

Responsable : Aucun

Discussion :

Les limites ayant trait à l'utilisation des dispositifs de stockage portatifs contrôlés par l'organisation dans les systèmes externes incluent l'interdiction absolue d'utiliser ces dispositifs. L'interdiction d'une telle utilisation s'applique au moyen de méthodes techniques ou non techniques (c'est-à-dire des méthodes basées sur les procédures).

AC-21 — Échange d'information (---)

Énoncés :

a. Permettre aux utilisatrices et utilisateurs autorisés de déterminer si les autorisations d'accès accordées aux partenaires d'échange respectent les restrictions d'accès à l'information et d'utilisation en tenant compte de [Affectation : circonstances d'échange d'information définies par l'organisation où l'utilisateur doit faire preuve de discrétion]
b. Employer des [Affectation : mécanismes automatisés ou des processus manuels définis par l'organisation] pour aider les utilisatrices et utilisateurs à prendre des décisions concernant l'échange d'information et la collaboration

Responsable : Aucun

Discussion :

L'échange d'information s'applique à l'information susceptible de faire l'objet de restrictions en fonction d'un mode quelconque de détermination officielle ou administrative. Des exemples d'une telle information incluent l'information relative à un contrat, l'information protégée, l'information classifiée relative à des programmes ou à des compartiments à accès spéciaux, l'information privilégiée, l'information exclusive et l'information personnelle. Les évaluations des risques liés à la sécurité et à la protection de la vie privée ainsi que les lois, les règlements et les politiques applicables peuvent fournir des éléments utiles pour prendre des décisions. Selon les circonstances, les partenaires d'échange peuvent être définis comme des personnes, des groupes ou des organisations. L'information peut être définie par contenu, type, catégorie de sécurité, ou programme ou compartiment à accès spécial. Les restrictions d'accès peuvent nécessiter des ententes de non-divulgation, et des droits d'accès devraient être définis chez l'organisation destinataire en fonction de l'utilisation autorisée de l'information et conformément au principe démontré du besoin de savoir. L'information échangée devrait se limiter à la quantité minimale d'information nécessaire à l'organisation destinataire. Les techniques de flux d'information et les attributs de sécurité peuvent être utilisés pour offrir une assistance automatisée aux utilisatrices et utilisateurs pour aider les utilisatrices et utilisateurs à prendre des décisions concernant l'échange d'information et la collaboration.

AC-21(01) — Application des décisions automatisées (---)

Énoncés :

Utiliser des [Affectation : mécanismes automatisés définis par l'organisation] pour appliquer des décisions sur l'échange d'information par une utilisatrice ou un utilisateur autorisé en fonction des autorisations d'accès des partenaires d'échange et des restrictions d'accès à l'information à échanger.

Responsable : Aucun

Discussion :

Les mécanismes automatisés sont utilisés pour appliquer les décisions relatives à l'échange d'information.

AC-21(02) — Recherche et récupération d'information (---)

Énoncés :

Le système d'information met en oeuvre des services de recherche et de récupération de l'information qui appliquent des [Affectation : restrictions liées à l'échange d'information définies par l'organisation].

Responsable : Aucun

Discussion :

Les services de recherche et de récupération d'information déterminent les ressources des systèmes d'information qui sont pertinentes pour l'information requise.

AC-21(400) — Accord d’échange de renseignements (---)

Énoncés :

Veiller, à la suite des accords écrits, à prendre les mesures de protection appropriées de l’information sensible échangée avec des entités du secteur public externes et des organisations.

Responsable : Aucun

Discussion :

Un accord décrit les conditions générales d’utilisation en vertu desquelles les renseignements personnels sont divulgués entre les parties et il peut, ou non, être juridiquement contraignant. S’assurer que l’accord documente les dispositions législatives, les utilisations autorisées et les normes relatives à la conservation de l’organisation destinataire.

AC-21(401) — Entente d’échange de renseignements (---)

Énoncés :

Veiller, à la suite des ententes écrites, à prendre les mesures de protection appropriées de l’information sensible échangée entre et au sein des institutions gouvernementales.

Responsable : Aucun

AC-22 — Contenu accessible au public (---)

Énoncés :

a. Désigner les personnes qui sont autorisées à rendre l'information accessible au public
b. Former les personnes autorisées afin de s'assurer que l'information accessible au public ne contient pas d'information non publique
c. Examiner le contenu d'information proposé avant de l'afficher sur le système accessible au public pour s'assurer qu'il ne contient aucune information non publique
d. Examiner le contenu du système accessible au public tous les [Affectation : fréquence définie par l'organisation] pour vérifier s'il contient de l'information non publique et pour la supprimer, le cas échéant

Responsable : Aucun

Discussion :

Conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables, le grand public n'est pas autorisé à accéder à de l'information non publique, y compris aux renseignements personnels, à l'information protégée en vertu de la Loi sur la protection des renseignements personnels dans le secteur privé et à l'information exclusive. Le contenu accessible au public concerne les systèmes contrôlés par l'organisation et accessibles au public, généralement sans l'application de mesures d'identification ou d'authentification. L'affichage d'information sur les systèmes non organisationnels (par exemple, sites Web publics non organisationnels, forums et médias sociaux) n'est pas couvert par une stratégie organisationnelle. Alors que les organisations peuvent compter sur des personnes qui sont responsables du développement et de la mise en oeuvre de stratégies sur l'information pouvant être rendue publique, le contenu accessible au public concerne la gestion des personnes qui rendent l'information accessible au public.

AC-23 — Protection contre l'exploration de données (---)

Énoncés :

Employer des [Affectation : techniques de détection et de prévention de l'exploration de données définies par l'organisation] pour les [Affectation : objets de stockage de données définis par l'organisation] pour détecter l'exploration de données et protéger les systèmes contre celle-ci.

Responsable : Aucun

Discussion :

L'exploration de données est un processus analytique qui tente de trouver des corrélations ou des tendances dans de grands ensembles de données aux fins de découverte de données ou de connaissances, et à l'occasion qui fait correspondre l'information concernant une personne entre les jeux de données (correspondance de données). Les objets de stockage de données comprennent les enregistrements de base de données et les champs de base de données. L'information sensible peut être extraite des opérations d'exploration de données. Lorsque l'information consiste en des renseignements personnels, elle peut conduire à des révélations inattendues sur les personnes et engendrer des risques d'atteinte à la vie privée. Avant toute activité d'exploration de données, ces risques doivent être identifiés, gérés et, le cas échéant, atténués. Avant de mener les activités d'exploration de données, les organisations déterminent si de telles activités sont autorisées par la loi. Les techniques de détection et de prévention d'exploration de données incluent de limiter le nombre et la fréquence des requêtes de base de données afin d'augmenter le facteur de travail requis pour déterminer le contenu de telles bases de données, de limiter les types de réponses fournis aux requêtes de base de données, d'appliquer des techniques de protection de la vie privée différentielle ou de chiffrement homomorphique, et d'aviser le personnel lorsque des requêtes de base de données ou des accès irréguliers ont lieu. Aviser le personnel approprié lorsque des requêtes de base de données ou des accès irréguliers ont lieu est essentiel, car ils sont susceptibles de constituer une atteinte à la vie privée ou une violation de la sécurité. La protection contre l'exploration de données met l'accent sur la protection de l'information de l'organisation lorsque l'information est conservée dans des magasins de données. À l'inverse, le contrôle AU-13 porte sur la surveillance de diffusions inappropriées de l'information organisationnelle qui pourrait avoir été explorée ou obtenue de magasins de données et qui est maintenant offerte comme de l'information de sources ouvertes.

AC-24 — Décisions de contrôle d’accès (---)

Énoncés :

[Sélection (un choix ou plus) : Établir les procédures; mettre en oeuvre des mécanismes] pour s’assurer que les [Affectation : décisions de contrôle d’accès définies par l’organisation] sont appliquées à chacune des demandes d’accès avant l’application de l’accès.

Responsable : Aucun

Discussion :

Les décisions de contrôle d’accès (également appelées décisions d’autorisation) ont lieu lorsque l’information d’autorisation est appliquée à des accès précis. Par contre, l’application de l’accès se produit lorsque les systèmes appliquent les décisions de contrôle d’accès. Bien qu’il arrive couramment qu’une même entité mette en oeuvre les décisions de contrôle d’accès et l’application de l’accès, il n’est pas nécessaire ni toujours optimal qu’une seule entité soit responsable de ces deux mises en oeuvre. Pour certains systèmes distribués et certaines architectures, des entités différentes peuvent prendre les décisions de contrôle d’accès et appliquer e l’accès.

AC-24(01) — Transmission de l'information sur l'autorisation d'accès (---)

Énoncés :

Transmettre [Affectation : information d'autorisation d'accès définie par l'organisation] au moyen de [Affectation : contrôles définis par l'organisation] aux [Affectation : systèmes désignés par l'organisation] qui appliquent les décisions de contrôle d'accès.

Responsable : Aucun

Discussion :

Les processus d'autorisation et les décisions de contrôle d'accès peuvent avoir lieu dans des parties distinctes des systèmes. Dans ce cas, l'information sur l'autorisation est transmise de façon sécurisée (par exemple, au moyen de mécanismes cryptographiques) afin que les décisions de contrôle d'accès puissent être appliquées aux emplacements appropriés. Afin d'appuyer les décisions de contrôle d'accès, il pourrait s'avérer nécessaire de transmettre les attributs de sécurité et de protection de la vie privée connexes avec l'information sur l'autorisation d'accès. En effet, dans les systèmes distribués, diverses décisions de contrôle d'accès doivent être prises en série par différentes entités qui ont toutes besoin de certains attributs de sécurité pour prendre les décisions. La protection de l'information sur l'autorisation d'accès permet d'empêcher que cette information soit modifiée, mystifiée ou compromise au cours de la transmission.

AC-24(02) — Aucune identité d’utilisatrices, utilisateurs ou processus (---)

Énoncés :

Le système applique les décisions de contrôle d’accès en fonction des [Affectation : attributs de sécurité ou de protection de la vie privée définis par l’organisation] qui ne contiennent pas l’identité d’utilisatrices ou utilisateurs ni le processus exécuté en leur nom.

Responsable : Aucun

Discussion :

Dans certaines situations, il est important que les décisions de contrôle d’accès soient prises sans information concernant l’identité des utilisatrices et utilisateurs présentant les demandes. La protection de la vie privée des personnes est alors de la plus haute importance. Dans d’autres situations, l’information d’identification des utilisatrices et utilisateurs n’est pas nécessaire pour les décisions de contrôle d’accès et, surtout dans le cas des systèmes distribués, la transmission de cette information avec le degré d’assurance requis pourrait être très coûteuse ou difficile à accomplir. Le contrôle d’accès au support (MAC), le contrôle d’accès basé sur les rôles (RBAC), le contrôle d’accès basé sur les attributs (ABAC) ainsi que les stratégies de contrôle basé sur les étiquettes, par exemple, pourraient ne pas inclure l’identité de l’utilisatrice ou utilisateur comme attribut.

AC-25 — Moniteur de référence (---)

Énoncés :

Mettre en oeuvre un moniteur de référence pour les [Affectation : stratégies de contrôle d'accès définies par l'organisation] qui est résistant aux intrusions, systématiquement appelé et suffisamment simple pour faire l'objet d'une analyse et de tests dont l'exhaustivité peut être assurée.

Responsable : Aucun

Discussion :

Un moniteur de référence est un ensemble d'exigences de conception sur un mécanisme de validation de référence qui, en tant qu'élément clé d'un système d'exploitation, applique une stratégie de contrôle d'accès à tous les sujets et objets. Un mécanisme de validation de référence est systématiquement appelé, résistant aux intrusions et suffisamment petit pour faire l'objet d'une analyse et de tests dont l'exhaustivité peut être assurée (c'est-à-dire vérifiable). L'information est représentée à l'interne dans les systèmes au moyen d'abstractions également appelées structures de données. Les structures de données internes peuvent représenter différents types d'entités actives et passives. Les entités actives, également appelées « sujets », sont associées à des personnes, à des dispositifs ou à des processus exécutés au nom des personnes. Les entités passives, également appelées « objets », sont associées à des structures de données comme des dossiers, des tampons, des ports de communications, des tableaux, des fichiers et des canaux interprocessus. Les moniteurs de référence appliquent les stratégies de contrôle d'accès limitant l'accès aux objets en fonction de l'identité des sujets ou des groupes auxquels les sujets appartiennent. Le système applique la stratégie de contrôle d'accès en fonction des règles établies par la stratégie. La propriété de résistance aux intrusions du moniteur de référence empêche les adversaires de compromettre le fonctionnement du mécanisme de validation de référence. La propriété systématiquement appelée empêche les adversaires de contourner le mécanisme et d'enfreindre la politique de sécurité. La propriété de petite taille aide à assurer l'exhaustivité de l'analyse et des tests des mécanismes pour détecter les faiblesses ou les lacunes (c'est-à-dire les lacunes latentes) qui empêcheraient l'application de la stratégie de sécurité.

AT

Formation du personnel à la cybersécurité

Awareness and Training

AT-01 — Politique et procédures de sensibilisation et de formation (---)

Énoncés :

a. Développer, consigner et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :

1. une politique de sensibilisation et de formation [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, à la jurisprudence, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables

2. Procédures pour faciliter la mise en oeuvre de la politique de sensibilisation et de formation ainsi que des contrôles de sensibilisation et de formation connexes

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures de sensibilisation et de formation

c. Passer en revue et mettre à jour, par rapport à la sensibilisation et à la formation :

1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La politique et les procédures de sensibilisation et de formation abordent les contrôles de la famille AT qui ont été mis en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement des telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à l'élaboration de la politique et des procédures de sensibilisation et de formation. En règle générale, les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin de politiques et de procédures propres à la mission ou au système. L'approche à l'égard de la sensibilisation et de la formation peut être intégrée à la stratégie générale sur la sécurité et la protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission et aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures de sensibilisation et de formation comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.

AT-02 — Formation et sensibilisation en matière de sécurité (Nc--)

Énoncés :

a. Fournir une formation sur la sécurité et la protection de la vie privée aux utilisatrices et utilisateurs du système (y compris les gestionnaires, les cadres supérieures et supérieurs et les entrepreneures et entrepreneurs) :

1. dans le cadre d'une formation de base pour les nouvelles utilisatrices et nouveaux utilisateurs, et tous les [Affectation : fréquence définie par l'organisation] par la suite

2. lors de changements apportés au système ou à la suite de [Affectation : événements définis par l'organisation]

b. Utiliser les techniques suivantes pour accroître la sensibilisation à la sécurité et à la protection de la vie privée des utilisatrices et utilisateurs du système [Affectation : techniques de sensibilisation définies par l'organisation]

c. Mettre à jour le contenu de la formation et sensibilisation en matière de sécurité tous les [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

d. Incorporer les leçons apprises des incidents ou des violations de sécurité internes ou externes dans les techniques de formation et sensibilisation en matière de sécurité

Responsable : Aucun

Discussion :

Les organisations peuvent fournir des niveaux de base et avancés de formation sur la sécurité aux utilisatrices et utilisateurs, y compris des mesures visant à tester leur niveau de connaissance. Selon les besoins, les organisations peuvent apporter un complément au contenu de la formation et de la sensibilisation à la sécurité en fonction de leurs exigences organisationnelles particulières, des systèmes auxquels le personnel a accès et des environnements de travail (par exemple, le télétravail). Le contenu devrait comprendre une présentation des besoins de sécurité et de protection de la vie privée ainsi que les mesures que doivent prendre les utilisatrices et utilisateurs afin de maintenir la sécurité et de protéger les renseignements personnels et d'intervenir en cas d'incident soupçonné. Le contenu devrait inclure les mesures nécessaires en matière de sécurité opérationnelle et de traitement des renseignements personnels. Les techniques de sensibilisation comprennent des affiches, des objets affichant des rappels de sécurité et de protection de la vie privée, des messages au moment de la connexion, des avis envoyés par courriel ou de la part des responsables de l'organisation et des événements de sensibilisation. La formation sur la sécurité suivant la formation initiale décrite dans l'AT-02A.1, est menée à une fréquence conforme aux lois, aux directives, à la réglementation et aux politiques applicables. Une formation ultérieure sur la sécurité peut prendre la forme de courtes séances occasionnelles et comprendre de l'information ponctuelle sur de récents plans d'attaque, des changements apportés aux stratégies en matière de sécurité et de protection de la vie privée de l'organisation, des attentes révisées concernant la sécurité et la protection de la vie privée ou un sous-ensemble de sujets tirés de la formation initiale. La mise à jour périodique du contenu de formation et de sensibilisation aide à s'assurer que le contenu reste pertinent. Les événements qui peuvent précipiter une mise à jour du contenu de la formation comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables.

AT-02(01) — Exercices pratiques (Nc--)

Énoncés :

Fournir des exercices pratiques en formation en matière de sécurité qui simulent des événements et des incidents.

Responsable : Aucun

Discussion :

Les exercices pratiques peuvent comprendre des tentatives sans préavis de collecte d'information par des mécanismes de piratage psychologique, des accès non autorisés ou des simulations de conséquences négatives associées à l'ouverture de pièces jointes malveillantes ou à l'utilisation de liens vers des sites Web malveillants découlant d'attaques de harponnage.

AT-02(02) — Menace interne (---)

Énoncés :

Fournir une formation en matière de sécurité pour que le personnel sache reconnaître les indicateurs potentiels de menace interne et pour qu'il les signale.

Responsable : Aucun

Discussion :

Les indicateurs potentiels et les possibles signes précurseurs d'une menace interne peuvent comprendre des comportements comme les suivants : des comportements excessifs, de l'insatisfaction de longue durée en ce qui a trait à son travail, des tentatives d'accès à de l'information inutile dans le cadre de ses tâches, des accès inexpliqués à des ressources financières, de l'intimidation ou du harcèlement envers des collègues, de la violence en milieu de travail et d'autres manquements graves aux politiques, aux procédures, aux directives, aux règlements, aux règles ou aux pratiques. La formation en matière de sécurité et de protection de la vie privée porte notamment sur la façon dont les membres du personnel et de la direction peuvent communiquer leurs préoccupations concernant des indicateurs potentiels de menace interne conformément aux stratégies et aux procédures organisationnelles établies. Les organisations peuvent adapter le sujet de la sensibilisation aux menaces internes en fonction du rôle. Par exemple, la formation des gestionnaires peut se concentrer sur les changements dans les comportements des membres de l'équipe, alors que la formation des employées et employés peut porter sur des observations plus générales.

AT-02(03) — Piratage psychologique et exploration de données (---)

Énoncés :

Fournir une formation en matière de sécurité pour que le personnel sache reconnaître les indicateurs potentiels et réels de piratage psychologique et de l'exploration de données dans les médias sociaux.

Responsable : Aucun

Discussion :

Le piratage psychologique vise à tromper une personne pour l'inciter à révéler de l'information ou à faire une opération pouvant servir à s'introduire dans un système, à le compromettre ou à nuire à un système. Le piratage psychologique comprend l'hameçonnage, le faux-semblant, l'usurpation d'identité, l'appâtage, l'arnaque de la contrepartie, le détournement de chaînes de courriels, l'exploitation des médias sociaux et le talonnage. L'exploration de données dans les médias sociaux vise à recueillir de l'information à propos de l'organisation qui pourrait servir à appuyer des attaques à venir. La formation en matière de sécurité et de protection de la vie privée porte notamment sur la façon dont les membres du personnel et de la direction peuvent communiquer leurs préoccupations concernant des instances réelles et potentielles de piratage psychologique et d'exploration de données, au moyen des voies de communication de l'organisation, conformément aux stratégies et aux procédures établies.

AT-02(04) — Communications suspectes et comportements anormaux de systèmes (---)

Énoncés :

Fournir une formation en matière de sécurité sur la façon de reconnaître les communications suspectes et les comportements anormaux dans les systèmes organisationnels au moyen [Affectation : indicateurs de programmes malveillants définis par l'organisation].

Responsable : Aucun

Discussion :

Un effectif bien formé représente une autre mesure de protection pour les organisations, car il joue un rôle dans le cadre d'une stratégie de défense en profondeur en se protégeant contre des programmes malveillants qui tentent d'infiltrer les systèmes organisationnels par des courriels ou des applications Web. Le personnel est formé pour détecter les courriels potentiellement suspects (par exemple, réception de courriels inattendus, drôlement rédigés ou contenant des fautes de grammaire, ou provenant d'une expéditrice ou un expéditeur inconnu, qui semble être associé à une ou un partenaire ou à une entrepreneuse ou un entrepreneur connu). Le personnel reçoit également la formation nécessaire pour savoir quoi faire lorsqu'il reçoit ce type de courriels ou de communications Web suspects. Pour veiller au bon fonctionnement du processus, le personnel est bien formé et est mis au courant des caractéristiques des communications suspectes. Grâce à la formation qu'il reçoit pour détecter les comportements anormaux dans les systèmes, le personnel peut avertir rapidement l'organisation de la présence de programmes malveillants. En reconnaissant des comportements anormaux, le personnel de l'organisation peut servir de complément aux outils et aux systèmes que les organisations utilisent pour détecter les programmes malveillants et s'en protéger.

AT-02(05) — Menaces persistantes avancées (---)

Énoncés :

Fournir une formation en matière de sécurité sur les menaces persistantes avancées.

Responsable : Aucun

Discussion :

Un moyen efficace de détecter des menaces persistantes avancées (MPA) et de prévenir la réussite des attaques est d'offrir au personnel une formation spécifique en matière de sécurité. La formation en matière de sécurité implique de faire connaître au personnel différents moyens qui permettent aux MPA d'infiltrer l'organisation (par exemple : par le biais de sites Web, de courriels, de fenêtres contextuelles de publicité, d'articles et de piratage psychologique). Une formation efficace comporte des techniques permettant de reconnaître des courriels suspects, l'utilisation de systèmes amovibles dans un milieu non sécurisé et la possibilité que des gens soient ciblés à la maison.

AT-02(06) — Environnement de cybermenaces (---)

Énoncés :

a. Fournir une formation en matière de sécurité sur l'environnement de cybermenaces
b. Refléter l'information actuelle sur les cybermenaces dans les opérations du système

Responsable : Aucun

Discussion :

Étant donné que les menaces continuent d'évoluer, la formation en matière de sécurité de l'organisation est dynamique. De plus, la formation en matière de sécurité ne se fait pas en vase clos par rapport aux opérations du système qui soutiennent des fonctions liées à la mission et aux activités de l'organisation.

AT-03 — Formation selon le rôle (---)

Énoncés :

a. Fournir une formation en sécurité et en protection de la vie privée basée sur les rôles au personnel détenant les rôles et responsabilités suivants : [Affectation : rôles et responsabilités définis par l'organisation]

1. avant d'autoriser l'accès au système ou à de l'information, ou avant la réalisation des tâches attribuées et tous les [Affectation : fréquence définie par l'organisation] par la suite

2. lorsque des changements apportés au système l'exigent

b. Mettre à jour le contenu de la formation offerte selon le rôle tous les [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

c. Incorporer les leçons apprises des incidents ou des violations de sécurité internes ou externes dans la formation axée sur les rôles

Responsable : Aucun

Discussion :

Les organisations déterminent le contenu de la formation en tenant compte des rôles et des responsabilités des personnes, ainsi que des exigences de sécurité et de protection de la vie privée de l'organisation et des systèmes auxquels le personnel est autorisé à accéder, ce qui comprend la formation technique spécialement adaptée pour les tâches attribuées. Parmi les rôles pouvant nécessiter une formation selon le rôle, notons les cadres supérieurs ou les dirigeantes principales et dirigeants principaux (par exemple, une ou un chef d'organisme/une ou un chef de la direction, une dirigeante principale ou un dirigeant principal de l'information, une ou un cadre supérieur responsable de la gestion des risques, une ou un cadre supérieur de la gouvernance, une haute ou un haut fonctionnaire ou cadre supérieure ou supérieur approprié en matière de protection de la vie privée), les propriétaires des systèmes, les autorités responsables; les responsables de la sécurité des systèmes; les agentes et agents de la protection des systèmes et de la vie privée; les responsables chargés de l'acquisition et de l'approvisionnement; les architectes d'entreprise; les ingénieures et ingénieurs de système; les développeuses et développeurs de logiciels; les ingénieures et ingénieurs en sécurité des systèmes; les praticiennes et praticiens de la protection de la vie privée; les administratrices et administrateurs de système, de réseau et de bases de données; les vérificatrices et vérificateurs; le personnel responsable des activités de gestion des configurations; le personnel responsable des activités de vérification et de validation; le personnel doté d'un accès logiciel de niveau système; les évaluatrices et évaluateurs des contrôles; le personnel ayant des tâches liées à la planification d'urgence et à l'intervention en cas d'incident; le personnel assumant des responsabilités liées à la gestion de la protection de la vie privée; et le personnel ayant accès aux renseignements personnels. La formation complète axée sur les rôles concerne les rôles et les responsabilités techniques, opérationnels et de gestion qui sont associés aux contrôles physiques, techniques et du personnel. Une formation axée sur les rôles comporte également des stratégies, des procédures, des outils, des méthodes et des artéfacts qui sont adaptés aux rôles de sécurité et de protection de la vie privée définis. Dans le cadre de leur programme de sécurité et de protection de la vie privée, les organisations doivent également fournir la formation nécessaire afin que les personnes puissent s'acquitter de leurs responsabilités en matière de gestion des opérations et de la chaîne d'approvisionnement. La formation selon le rôle s'applique également aux entrepreneures et entrepreneurs qui fournissent des services aux organismes fédéraux. Les types de formation comprennent la formation Web et assistée par ordinateur, la formation en classe ainsi que la formation pratique (incluant une microformation). Mettre à jour la formation selon le rôle sur une base régulière aide à s'assurer que le contenu demeure pertinent et efficace. Les événements qui peuvent précipiter une mise à jour du contenu de la formation comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables.

AT-03(01) — Contrôles environnementaux (---)

Énoncés :

Offrir à [Affectation : personnel ou rôles définis par l'organisation] la formation initiale sur l'utilisation et le fonctionnement des contrôles environnementaux [Affectation : fréquence définie par l'organisation].

Responsable : Aucun

Discussion :

Les contrôles environnementaux comprennent notamment les dispositifs ou les systèmes de suppression et de détection des incendies, les systèmes de gicleurs, les extincteurs manuels, les boyaux d'arrosage fixes, les détecteurs de fumée, les dispositifs de contrôle de la température et de l'humidité, le chauffage, la ventilation et la climatisation de même que l'alimentation dans les installations de l'organisation.

AT-03(02) — Contrôles de sécurité physiques (---)

Énoncés :

Offrir à [Affectation : personnel ou rôles définis par l'organisation] la formation initiale sur l'utilisation et le fonctionnement des contrôles environnementaux [Affectation : fréquence définie par l'organisation].

Responsable : Aucun

Discussion :

Les contrôles de sécurité physique comprennent les dispositifs de contrôle d'accès physique, les avertisseurs d'intrusion physique et de détection, les procédures d'exploitation pour les gardiennes et gardiens de sécurité, et l'équipement de contrôle et de surveillance.

AT-03(03) — Exercices pratiques (---)

Énoncés :

Inclure dans la formation à la sécurité et protection de la vie privée des exercices pratiques qui renforcent les objectifs de formation.

Responsable : Aucun

Discussion :

Les exercices pratiques comprennent une formation à la sécurité pour les développeuses et développeurs de logiciels, comportant des simulations d'attaques qui exploitent les vulnérabilités les plus courantes des logiciels ou d'attaques par harponnage visant des cadres supérieures et supérieurs. Les exercices pratiques d'une formation sur la protection de la vie privée comprennent des modules avec des jeux-questionnaires pour identifier des renseignements personnels, évaluer l'utilisation autorisée de l'information et des processus acceptables dans le traitement des renseignements personnels dans différents scénarios ou scénarios sur l'exécution d'une EFVP.

AT-03(04) — Communications suspectes et comportements anormaux de systèmes (---)

Énoncés :

Annulé : Transféré sous le contrôle AT-02(4).

Responsable : Aucun

AT-03(05) — Traitement des renseignements personnels (---)

Énoncés :

Offrir à [Affectation : personnel ou rôles définis par l'organisation] la formation initiale sur l'utilisation et le fonctionnement des contrôles de traitement des renseignements personnels et de transparence [Affectation : fréquence définie par l'organisation].

Responsable : Aucun

Discussion :

Les contrôles de traitement des renseignements personnels et de transparence impliquent de déterminer l'autorité donnant droit à recueillir, à utiliser ou à communiquer des renseignements personnels ainsi qu'à communiquer aux personnes les pratiques de traitement de ceux-ci.

AT-04 — Dossiers de formation (---)

Énoncés :

a. Consigner et surveiller les activités de formation en matière de sécurité et de protection de la vie privée de l'information, y compris la formation sur la sensibilisation à la sécurité et à la protection de la vie privée, et la formation en sécurité et en protection de la vie privée basée sur des rôles spécifiques
b. Conserver les dossiers de formation individuels pendant [Affectation : délai défini par l'organisation]

Responsable : Aucun

Discussion :

À la discrétion de l'organisation, chaque superviseur peut consigner les cours spécialisés que suit son personnel.

AT-05 — Contacts avec les groupes et associations de sécurité (---)

Énoncés :

Annulé : Intégré au contrôle PM-15.

Responsable : Aucun

AT-06 — Rétroaction sur les formations suivies (---)

Énoncés :

Fournir une rétroaction sur les résultats de la formation organisationnelle au personnel suivant [Affectation : fréquence définie par l'organisation] : [Affectation : personnel désigné par l'organisation].

Responsable : Aucun

Discussion :

La rétroaction sur les formations suivies inclut les résultats de la formation sur la sensibilisation et les résultats de la formation selon le rôle. Les résultats de la formation, plus particulièrement en ce qui a trait aux manquements du personnel occupant des rôles essentiels, peuvent révéler un problème potentiellement grave. Par conséquent, il est important que les cadres supérieures et supérieurs soient informés de ces situations pour qu'ils puissent intervenir de manière appropriée. La rétroaction sur les formations suivies soutient l'évaluation et la mise à jour de la formation organisationnelle décrite dans le contrôle AT-02B et le contrôle AT-03B.

AU

Journaux d’audit, traçabilité des actions

Audit and Accountability

AU-01 — Politique et procédures de vérification et de responsabilisation (---)

Énoncés :

a. Développer, consigner et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :

1. une politique de vérification et de responsabilisation [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables

2. des procédures pour faciliter la mise en oeuvre de la politique de vérification et de responsabilisation ainsi que des contrôles connexes

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures de vérification et de responsabilisation

c. Passer en revue et mettre à jour, par rapport à la vérification et la responsabilisation :

1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La politique et les procédures de vérification et de responsabilisation abordent les contrôles de la famille AU qui ont été mis en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à l'élaboration de la politique et des procédures de vérification et de responsabilisation. En règle générale, les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin de politiques et de procédures propres à la mission ou au système. La politique peut être intégrée à la politique générale de sécurité et de protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures de vérification et de responsabilisation comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle. Les utilisatrices et utilisateurs dont les activités consistent à surveiller les journaux de vérification devraient être mis au courant de l'activité.

AU-02 — Journalisation d'événements (Nc--)

Énoncés :

a. Déterminer les types d'événements que le système est en mesure de journaliser pour soutenir la fonction de vérification [Affectation : types d'événements définis par l'organisation que le système est en mesure de journaliser]
b. Coordonner la fonction de journalisation avec d'autres entités organisationnelles qui nécessitent de l'information en matière de vérification afin d'orienter et d'éclairer la sélection des critères pour les événements à journaliser
c. Préciser les types d'événements suivants pour la journalisation dans le système [Affectation : types d'événements définis par l'organisation (sous-ensemble de types d'événements défini dans le contrôle AU-02A) et fréquence de journalisation (ou la situation qui la justifie) de chaque type d'événement]
d. Expliquer pourquoi les types d'événements sélectionnés pour la journalisation sont jugés adéquats pour soutenir les enquêtes après coup des incidents
e. Vérifier et mettre à jour les types d'événements sélectionnés pour la journalisation tous les [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

On entend par événement tout fait observable dans un système. Les types d'événements pour lesquels une journalisation est requise sont liés à la sécurité des systèmes et à la protection de la vie privée. La journalisation d'événements appuie également des besoins particuliers en matière de surveillance et de vérification. Les types d'événements comprennent les changements de mots de passe, les ouvertures de session infructueuses, les accès infructueux aux systèmes, les changements apportés aux attributs de sécurité et de protection de la vie privée, l'accès ou la consultation de renseignements personnels, l'utilisation de privilèges d'administrateur, l'utilisation de justificatifs d'identité numériques, les changements liés aux actions de données, les paramètres de requêtes ou l'utilisation de justificatifs d'identité externes. En définissant l'ensemble des types d'événements pour lesquels une journalisation est requise, les organisations étudient la mise en place d'une vérification adaptée à chacun des contrôles. Par souci d'exhaustivité, la journalisation d'événements inclut tous les protocoles qui sont utilisés et pris en charge par le système. Dans le but d'établir un équilibre entre les besoins en matière de surveillance et de vérification et les autres besoins du système, la journalisation d'événements exige que soit déterminé le sous-ensemble des types d'événements qui seront journalisés à un moment précis. Par exemple, les organisations peuvent déterminer que les systèmes doivent pouvoir journaliser tous les accès aux fichiers, réussis ou non, mais ne pas activer cette capacité – sauf dans certaines circonstances – en raison de la charge potentielle qu'elle représente envers les performances du système. Les types d'événements que les organisations veulent journaliser peuvent changer. L'examen et la mise à jour de l'ensemble des événements journalisés sont nécessaires pour s'assurer que les événements sont toujours pertinents et continuent de soutenir les besoins de l'organisation. Les organisations devraient réfléchir à la façon dont les types d'événements de journalisation peuvent révéler de l'information au sujet des personnes, ce qui donnerait lieu à des risques d'atteinte à la vie privée, et comment atténuer de tels risques. Par exemple, il est possible que des renseignements personnels soient divulgués dans la piste de vérification, en particulier si l'événement de journalisation est basé sur des modèles ou le moment d'utilisation. D'autres contrôles et améliorations de contrôle peuvent faire référence aux besoins en matière de journalisation d'événements, dont le besoin de journaliser des types d'événements particuliers. Cela comprend les contrôles AC-02(04), AC-03(10), AC-06(09), AC-17(01), CM-03F, CM-05(01), IA-03(03)b, MA-04(01), MP-04(02), PE-03, PM-21, PT-07, RA-08, SC-07(09), SC-07(15), SI-03(08), SI-04(22), SI-07(08) et SI-10(01). Les organisations tiennent compte des types d'événements exigés en vertu des lois, des décrets, des directives, des politiques, de la réglementation, des normes et des lignes directrices applicables. Les dossiers de vérification peuvent être créés à différents niveaux, y compris au niveau des paquets lorsque l'information traverse le réseau. La sélection du niveau approprié de journalisation des événements est un élément important de la capacité de surveillance et de vérification dans la mesure où elle peut aider à relever les causes profondes d'un problème. Pour définir les types d'événements, les organisations doivent considérer la journalisation nécessaire pour couvrir les types d'événements connexes, comme les étapes dans les processus distribués basés sur une transaction et les actions qui surviennent dans les architectures orientées service.

AU-02(01) — Compilation d'enregistrements de vérification provenant de sources multiples (---)

Énoncés :

Annulé : Intégré au contrôle AU-12.

Responsable : Aucun

AU-02(02) — Sélection d'événements de vérification par composant (---)

Énoncés :

Annulé : Intégré au contrôle AU-12.

Responsable : Aucun

AU-02(03) — Examens et mises à jour (---)

Énoncés :

Annulé : Intégré au contrôle AU-02.

Responsable : Aucun

AU-02(04) — Fonctions privilégiées (---)

Énoncés :

Annulé : Intégré au contrôle AC-06(09).

Responsable : Aucun

AU-03 — Contenu des enregistrements de vérification (Nc--)

Énoncés :

S'assurer que les enregistrements de vérification contiennent l'information nécessaire pour établir :
a. le type d'événement qui s'est produit
b. le moment auquel l'événement s'est produit
c. l'endroit où l'événement s'est produit
d. la source de l'événement
e. le résultat de l'événement
f. l'identité des personnes, des sujets, des objets ou des entités associés à l'événement

Responsable : Aucun

Discussion :

Le contenu des dossiers de vérification qui peut être nécessaire pour soutenir la fonction de vérification comprend les descriptions d'événements (élément A), les horodatages (élément B), les adresses source et de destination (élément C), les identifiants d'utilisateur ou de processus (éléments D et F), les indicateurs de réussite ou d'échec (élément E) et les noms de fichiers touchés (éléments A, C, E et F). Les résultats des événements peuvent comprendre des indicateurs de réussite ou d'échec et des résultats propres à l'événement, comme la posture de sécurité et de protection de la vie privée du système après l'événement. Les organisations réfléchissent à la façon dont les enregistrements de vérification peuvent révéler de l'information au sujet des personnes, ce qui donnerait lieu à des risques d'atteinte à la vie privée; et elles cherchent à savoir comment atténuer de tels risques. Par exemple, il est possible que des renseignements personnels soient divulgués dans la piste de vérification, en particulier si les enregistrements de vérification sont basés sur des modèles ou le moment d'utilisation.

AU-03(01) — Information de vérification supplémentaire (---)

Énoncés :

Générer des enregistrements de vérification comportant l'information supplémentaire suivante : [Affectation : information supplémentaire définie par l'organisation].

Responsable : Aucun

Discussion :

La capacité d'ajouter l'information générée dans les enregistrements de vérification dépend des fonctionnalités du système permettant de configurer le contenu des enregistrements de vérification. Les organisations peuvent considérer ajouter de l'information supplémentaire dans les enregistrements de vérification, y compris les règles de contrôle d'accès et de contrôle de flux invoquées et les identités individuelles des utilisatrices et utilisateurs appartenant à un compte de groupe. Les organisations peuvent également envisager de limiter l'information supplémentaire à ajouter aux enregistrements de vérification en incluant seulement celle qui est nécessaire aux exigences de vérification. Ainsi, l'utilisation des pistes de vérification et des journaux de vérification serait simplifiée, car on ne tiendrait pas compte de l'information qui pourrait être trompeuse, rendre difficile la localisation de l'information pertinente ou accroître les risques liés à la vie privée.

AU-03(02) — Gestion centralisée du contenu des enregistrements de vérification (---)

Énoncés :

Annulé : Intégré au contrôle PL-09.

Responsable : Aucun

AU-03(03) — Limitation des éléments liés aux renseignements personnels (---)

Énoncés :

Limiter les renseignements personnels contenus dans les enregistrements de vérification aux éléments suivants identifiés dans l'évaluation des facteurs relatifs à la vie privée : [Affectation : éléments définis par l'organisation].

Responsable : Aucun

Discussion :

Limiter les renseignements personnels contenus dans les enregistrements de vérification lorsque cette information n'est pas nécessaire à des fins opérationnelles aide à réduire le niveau de risque d'atteinte à la vie privée engendré par un système.

AU-04 — Capacité de stockage des journaux de vérification (Nc--)

Énoncés :

Attribuer une capacité de stockage de journaux de vérification en fonction des [Affectation : exigences de conservation des journaux de vérification].

Responsable : Aucun

Discussion :

Les organisations tiennent compte des types de journalisation de vérification à effectuer et des exigences de traitement pour attribuer la capacité de stockage des journaux de vérification. En attribuant une capacité de stockage des journaux suffisante, on réduit les risques de dépassement de cette capacité, qui engendrait possiblement l'interruption ou la réduction de cette capacité de stockage de vérification.

AU-04(01) — Transfert vers une capacité de stockage secondaire (---)

Énoncés :

Transférer les journaux de vérification [Affectation : fréquence définie par l'organisation] à un système, composant du système ou un support différent du système ou du composant du système faisant l'objet de la journalisation.

Responsable : Aucun

Discussion :

Le transfert de journaux de vérification, aussi appelé déchargement, est un processus courant attribuable aux systèmes ayant des capacités de stockage de journaux de vérification limitées; et ce processus soutient la disponibilité des journaux de vérification. Le stockage des journaux de vérification n'est alors qu'une solution temporaire jusqu'à ce que le système puisse communiquer avec le système secondaire ou de substitution mis en place pour stocker les journaux de vérification. Transférer les journaux de vérification au stockage secondaire est similaire au contrôle AU-09(02) dans le sens où les journaux de vérification sont transférés à une différente entité. Toutefois, la sélection du contrôle AU-09(02) vise à protéger la confidentialité et l'intégrité des enregistrements de vérification. Les organisations peuvent opter pour l'amélioration du contrôle afin de profiter des avantages d'une capacité accrue de stockage des journaux de vérification et assurer la confidentialité, l'intégrité et la disponibilité des journaux et des enregistrements de vérification.

AU-05 — Intervention en cas d'échec du processus de journalisation des données de vérification (---)

Énoncés :

a. Alerter [Affectation : personnel ou rôles désignés de l'organisation] dans [Affectation : délais définis par l'organisation] en cas d'échec d'un processus de journalisation des données de vérification
b. Prendre les mesures supplémentaires suivantes : [Affectation : mesures supplémentaires définies par l'organisation]

Responsable : Aucun

Discussion :

Les échecs du processus de journalisation des données de vérification incluent les erreurs logicielles et matérielles, l'échec des mécanismes de saisie des journaux de vérification et l'atteinte ou le dépassement de la capacité de stockage du journal de vérification. Les mesures définies par l'organisation comprennent l'écrasement des journaux de vérification plus anciens, la fermeture du système et l'arrêt de la génération des enregistrements de vérification. Les organisations peuvent choisir de définir des mesures supplémentaires associées aux échecs du processus de journalisation des données de vérification en fonction du type d'échec, de l'emplacement de l'échec, de la gravité de l'échec, ou encore une combinaison de ces facteurs. Lorsque l'échec du processus de journalisation est associé au stockage, l'intervention doit s'appliquer au référentiel de stockage des journaux de vérification (c'est-à-dire le composant d'un système particulier où les journaux de vérification sont stockés), au système sur lequel les journaux de vérification se trouvent, à la capacité de stockage totale de l'organisation pour les journaux de vérification (c'est-à-dire tous les référentiels de stockage de journaux de vérification) ou à ces trois éléments. Les organisations peuvent décider de ne pas prendre de mesures supplémentaires après avoir avisé les rôles ou le personnel désignés.

AU-05(01) — Avertissement de capacité de stockage (---)

Énoncés :

Avertir [Affectation : personnel, rôles et/ou emplacements définis par l'organisation] dans un délai de [Affectation : délai défini par l'organisation] lorsque le volume de stockage des journaux de vérification attribué aux enregistrements de journaux vérification atteint [Affectation : pourcentage défini par l'organisation] de sa capacité maximale.

Responsable : Aucun

Discussion :

Les organisations peuvent se voir attribuer plusieurs référentiels de stockage de journaux de vérification se trouvant dans de multiples composants de système; chacun des référentiels a une capacité de volume de stockage différente.

AU-05(02) — Alertes en temps réel (---)

Énoncés :

Fournir une alerte [Affectation : personnel, rôles et/ou emplacements définis par l'organisation] en [Affectation : délais en temps réel définis par l'organisation] lorsque les événements d'échec de vérification suivants se produisent : [Affectation : événements d'échec de journalisation des données de vérification définis par l'organisation qui nécessitent une alerte en temps réel].

Responsable : Aucun

Discussion :

Les alertes génèrent des messages d'urgence pour les organisations. La vitesse à laquelle ces messages sont générés à la suite des alertes en temps réel dépend de la technologie de l'information utilisée (le temps qui s'écoule entre la détection de l'événement et de l'alerte est inférieur à quelques secondes).

AU-05(03) — Seuils de volume de trafic configurables (---)

Énoncés :

Appliquer des seuils de volume de trafic configurables aux communications réseau, qui représentent les limites de la capacité de vérification et [Sélection (un choix) : rejette; retarde] tout trafic réseau supérieur à ces seuils.

Responsable : Aucun

Discussion :

Les organisations peuvent rejeter ou retarder le traitement du trafic des communications réseau si l'on juge que l'information de journalisation des données de vérification concernant ce trafic dépasse la capacité de stockage de la fonction de journalisation des données de vérification. Le choix de rejeter ou de retarder le trafic dépend des seuils de volume de trafic établis par l'organisation, qui peuvent être adaptés en fonction des changements apportés à la capacité de stockage des journaux de vérification.

AU-05(04) — Interruption en cas d'échec (---)

Énoncés :

Évoquer une [Sélection (un choix) : interruption complète du système; interruption partielle du système; détérioration des opérations en limitant les fonctions associées à la mission ou aux activités] en cas de [Affectation : échecs de la journalisation des données de vérification définis par l'organisation], sauf s'il existe une capacité de journalisation des données de vérification de substitution.

Responsable : Aucun

Discussion :

Les organisations déterminent les types d'échecs de journalisation des données de vérification qui peuvent engendrer automatiquement l'interruption ou la détérioration des opérations du système. Étant donné l'importance de veiller à la continuité de leur mission et de leurs activités, les organisations peuvent déterminer que la nature de l'échec de journalisation des données de vérification n'est pas assez grave pour justifier l'interruption complète du système qui permet de mener les fonctions principales liées à la mission et aux activités de l'organisation. Le cas échéant, l'interruption partielle du système ou la dégradation des opérations réduisant les capacités peuvent constituer des solutions viables.

AU-05(05) — Capacité de journalisation des données de vérification secondaire (---)

Énoncés :

Prévoir une capacité de journalisation des données de vérification secondaire en vue de parer à l'impossibilité d'avoir recours à la capacité de journalisation des données de vérification principale, et de mettre en oeuvre [Affectation : autres fonctions de journalisation des données de vérification définies par l'organisation].

Responsable : Aucun

Discussion :

Une capacité de journalisation des données de vérification secondaire n'est, par définition, qu'une solution de protection à court terme à laquelle l'organisation fait appel jusqu'au rétablissement de la capacité de journalisation des données de vérification principale. À ce titre, l'organisation peut décider de n'offrir qu'un sous-ensemble de la fonction de journalisation des données de vérification principale touchée par cette inexécution.

AU-06 — Examen, analyse et production de rapports liés aux enregistrements de vérification (---)

Énoncés :

a. Examiner et analyser les enregistrements de vérification du système tous les [Affectation : fréquence définie par l'organisation] pour déceler toute indication de [Affectation : activités inappropriées ou inhabituelles définies par l'organisation] et les répercussions potentielles d'activités inappropriées ou inhabituelles
b. Faire rapport des résultats à [Affectation : personnel ou rôles définis par l'organisation]
c. Ajuster le niveau d'examen, d'analyse et de rapports d'enregistrements de vérification dans le système lorsqu'un changement fondé sur des renseignements relatifs au maintien de l'ordre, du renseignement brut ou d'autres sources crédibles d'information est apporté au risque

Responsable : Aucun

Discussion :

L'examen, l'analyse et les rapports des dossiers vérification portent sur la journalisation en matière de sécurité et de protection de la vie privée de l'information qu'effectuent les organisations, ce qui comprend la journalisation qui découle de la surveillance de l'utilisation d'un compte, de l'accès à distance, de la connectivité sans fil, de la connexion d'appareils mobiles, de paramètres de configuration, de l'inventaire des composants de système, de l'utilisation d'outils de maintenance et de télémaintenance, de l'accès physique, de la température et de l'humidité, de la livraison et du retrait d'équipement, de communications aux frontières du système et de l'utilisation de code mobile et de voix sur protocole Internet (VoIP pour Voice over Internet Protocol). Les résultats peuvent être communiqués aux entités organisationnelles, comme l'équipe d'intervention en cas d'incident, le service de dépannage et le bureau de la sécurité ou de la protection de la vie privée. Dans la mesure du possible, les renseignements personnels devraient être supprimés des journaux de vérification s'ils ne sont pas nécessaires aux processus de production de rapports. Si les organisations ne sont pas autorisées à examiner et à analyser les enregistrements de vérification ou si elles sont incapables de mener de telles activités, les activités d'examen et d'analyse peuvent être menées par les organisations disposant d'une telle autorité. Il est possible d'ajuster la fréquence, la portée ou la profondeur de l'examen, de l'analyse ou des rapports de vérification des dossiers pour répondre aux besoins organisationnels lorsqu'une nouvelle information est reçue.

AU-06(01) — Intégration de processus automatisés (---)

Énoncés :

Intégrer des processus d'examen, d'analyse et de production de rapports liés aux enregistrements de vérification au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Les processus organisationnels qui tirent avantage d'examen, d'analyse et de production de rapports intégrés liés aux enregistrements de vérification incluent l'intervention en cas d'incident, la surveillance continue, la planification d'urgence, l'enquête et l'intervention en cas d'activités suspectes, et les vérifications du Vérificateur général du Québec (VGQ)

AU-06(02) — Alertes de sécurité automatisées (---)

Énoncés :

Annulé : Intégré au contrôle SI-04.

Responsable : Aucun

AU-06(03) — Correspondance des référentiels pour les enregistrements de vérification (---)

Énoncés :

Analyser et mettre en correspondance les enregistrements de vérification provenant de différents référentiels afin d'établir une connaissance de la situation à l'échelle de l'organisation.

Responsable : Aucun

Discussion :

La connaissance globale de la situation de l'organisation comprend la connaissance des trois niveaux de gestion des risques (niveau de l'organisation, niveau de la mission et processus opérationnel ainsi que le niveau du système d'information) et aide avoir une connaissance interorganisationnelle.

AU-06(04) — Analyses et examens centralisés (---)

Énoncés :

Fournir et mettre en oeuvre la capacité de centraliser les examens et les analyses des enregistrements de vérification provenant de plusieurs composants du système.

Responsable : Aucun

Discussion :

On compte parmi les mécanismes automatisés liés aux examens et aux analyses centralisés les produits de gestion des informations et des événements de sécurité (GIES).

AU-06(05) — Analyse intégrée des enregistrements de vérification (---)

Énoncés :

Intégrer l'analyse des enregistrements de vérification et l'analyse de [Sélection (un choix ou plus) : l'information liée au balayage des vulnérabilités; les données de rendement; l'information sur la surveillance du système d'information; {Affectation : données ou information recueillies par d'autres sources définies par l'organisation}] pour accroître sa capacité de détecter les activités inappropriées ou inhabituelles.

Responsable : Aucun

Discussion :

L'analyse intégrée des enregistrements de vérification n'est pas nécessaire pour le balayage des vulnérabilités, la génération de données de rendement et la surveillance du système. L'analyse intégrée nécessite plutôt que l'analyse d'information générée par balayage, surveillance ou autres activités de collecte de données soit intégrée à l'analyse de l'information d'enregistrement de vérification. Les outils de GIES peuvent faciliter le regroupement et la consolidation des enregistrements de vérification produits par les nombreux composants du système, de même que leur analyse et leur mise en corrélation. L'utilisation de scripts normalisés d'analyse des enregistrements de vérification développés par les organisations (complétés par des scripts localisés, au besoin) offre une approche plus rentable de l'analyse de l'information liée aux enregistrements de vérification recueillie. La corrélation entre l'information contenue dans les enregistrements de vérification et celle produite par le balayage des vulnérabilités est importante, car elle permet d'établir la justesse des balayages de vulnérabilités du système et d'établir des liens entre les événements de détection d'attaques et les résultats des balayages. Les liens avec les données de rendement peuvent permettre de détecter des attaques par déni de service ou d'autres types d'attaques qui entraînent l'utilisation non autorisée de ressources. Les associations avec l'information sur la surveillance du système peuvent contribuer à détecter des attaques et à établir un lien accru entre l'information de vérification et les situations opérationnelles.

AU-06(06) — Corrélation avec la surveillance physique (---)

Énoncés :

Mettre en corrélation l'information des enregistrements de vérification avec celle obtenue lors de la surveillance de l'accès physique pour accroître la capacité d'identification des activités suspectes, inappropriées, inhabituelles ou malveillantes.

Responsable : Aucun

Discussion :

En mettant en corrélation l'information des enregistrements de vérification liée à la surveillance physique et les enregistrements de vérification des systèmes, les organisations peuvent détecter des comportements suspects ou des signes associés à ce type de comportement. Par exemple, la corrélation entre l'identité d'un individu qui permet l'accès logique à certains systèmes et l'information liée à la sécurité physique supplémentaire qui révèle la présence de l'individu sur place lorsque l'accès logique a eu lieu peut s'avérer utile dans le cadre d'enquêtes.

AU-06(07) — Opérations autorisées (---)

Énoncés :

Préciser les opérations qui sont autorisées concernant chaque [Sélection (un choix ou plus) : processus de système; rôle; utilisateur] associé à l'examen, à l'analyse et aux rapports de l'information de vérification.

Responsable : Aucun

Discussion :

Les organisations précisent les opérations autorisées concernant les processus, les rôles et les utilisateurs du système en ce qui a trait à l'examen, à l'analyse et aux rapports des enregistrements de vérification en recourant à des activités de gestion des comptes du système. Il s'agit d'une façon d'appliquer le principe des droits d'accès minimaux. Le système veille au respect des opérations autorisées, dont la lecture, l'écriture, l'exécution, l'annexion et la suppression.

AU-06(08) — Analyse plein texte des commandes privilégiées (---)

Énoncés :

Mener une analyse plein texte des commandes privilégiées enregistrées dans un composant de système ou un sous-système physiquement distinct du système ou dans un autre système conçu pour mener cette analyse.

Responsable : Aucun

Discussion :

Une analyse plein texte de commandes privilégiées exige l'utilisation d'un environnement distinct pour analyser l'information enregistrée de vérification concernant les utilisateurs qui détiennent des droits d'accès privilégiés afin de ne pas compromettre l'information dans le système dans lequel les utilisatrices et utilisateurs ont des privilèges élevés, dont la capacité d'exécuter des commandes privilégiées. On entend par analyse plein texte l'analyse qui prend en compte le texte intégral associé aux commandes privilégiées (c'est-à-dire, les commandes et les paramètres) contrairement aux analyses qui ne tiennent compte que du nom de la commande. L'analyse plein texte comprend le recours au filtrage et à l'heuristique.

AU-06(09) — Corrélation avec l'information provenant de sources non techniques (---)

Énoncés :

Mettre en corrélation l'information provenant de sources non techniques et l'information d'enregistrement de vérification afin d'acquérir une connaissance globale de sa situation.

Responsable : Aucun

Discussion :

On compte parmi les sources non techniques les enregistrements qui répertorient les manquements aux politiques organisationnelles liés au harcèlement sexuel et à l'utilisation inappropriée de biens d'information. Grâce à ce type d'information, les efforts d'analyse sont ciblés et permettent de détecter les possibles activités malveillantes provenant de l'interne. Les organisations limitent l'accès disponible de sources non techniques en raison de sa nature délicate. Un accès limité permet de minimiser les risques de divulgation par inadvertance de renseignements personnels à des personnes qui ne répondent pas au besoin de connaître. On établit généralement des liens entre l'information provenant de sources non techniques et l'information d'enregistrement de vérification uniquement lorsque l'on soupçonne l'implication d'un individu dans un incident. Les organisations sollicitent des conseils juridiques avant de prendre des mesures.

AU-06(10) — Ajustement du niveau d’examen (---)

Énoncés :

Annulé : Intégré au contrôle AU-06.

Responsable : Aucun

AU-07 — Réduction des enregistrements de vérification et génération de rapports (---)

Énoncés :

Fournir et mettre en oeuvre une capacité de réduction des enregistrements de vérification et de génération de rapports qui :
a. prend en charge les exigences en matière d'examen, d'analyse et de production de rapports liés aux enregistrements de vérification sur demande et les enquêtes après coup sur les incidents
b. ne change pas le contenu original ni le classement chronologique des enregistrements de vérification

Responsable : Aucun

Discussion :

La réduction des enregistrements de vérification est un processus qui transforme l'information des journaux de vérification recueillie et les condense afin d'en accroître la valeur pour les analystes. Les capacités de réduction des enregistrements de vérification et de génération de rapports ne proviennent pas toujours du même système ou des mêmes entités organisationnelles qui mènent les activités de journalisation des données de vérification. Les capacités de réduction des enregistrements de vérification peuvent inclure des techniques d'exploration de données modernes comportant des filtres de données évolués afin de détecter les comportements anormaux dans les enregistrements de vérification. Les capacités de génération de rapports fournies par le système peuvent générer des rapports personnalisables. Le classement chronologique des dossiers de vérification peut représenter un enjeu si la granularité de l'estampille temporelle de l'enregistrement est insuffisante.

AU-07(01) — Traitement automatique (---)

Énoncés :

Permettre et mettre en oeuvre le tri et la recherche des enregistrements de vérification liés à des événements d'intérêt selon le contenu suivant : [Affectation : champs d'enregistrements de vérification définis par l'organisation].

Responsable : Aucun

Discussion :

Il est possible de déterminer les événements d'intérêt selon le contenu des enregistrements de vérification, notamment les ressources système impliquées, les objets d'information auxquels on a accédé, l'identité des individus, les types d'événements, les emplacements, les heures et les dates des événements ou les adresses IP concernées. Les organisations peuvent définir les critères d'événements de vérification selon le degré de granularité requis, comme les emplacements choisis par l'emplacement du réseau général ou par un composant du système précis. Si des renseignements personnels sont saisis dans un rapport de journaux de vérification et que ceux-ci ne sont pas nécessaires à la résolution de l'incident, ces renseignements personnels devraient être supprimés du rapport ou masqués de manière appropriée avant que l'enregistrement de vérification soit mis en circulation.

AU-07(02) — Triage et recherche automatisés (---)

Énoncés :

Annulé : Intégré au contrôle AU-07(01).

Responsable : Aucun

AU-08 — Horodatage du contrôle (Nc--)

Énoncés :

a. Utiliser les horloges internes du système pour horodater les enregistrements de vérification
b. Consigner l'horodatage des enregistrements de vérification correspondant à [Affectation : granularité de mesure du temps définie par l'organisation] et utilisant le temps universel coordonné (UTC), un décalage fixe par rapport à l'UTC correspondant à l'heure locale, ou encore en incluant le décalage local dans les données d'horodatage

Responsable : Aucun

Discussion :

L'horodatage généré par le système comprend la date et l'heure. L'heure est souvent exprimée selon l'UTC ou selon l'heure locale qui est un décalage par rapport à l'UTC. La granularité des mesures temporelle fait référence au degré de synchronisation entre les horloges du système et des horloges de référence (par exemple, la synchronisation des horloges avec une précision à des centaines ou à des dizaines de millisecondes). Les organisations peuvent définir des granularités de temps différentes pour les divers composants de système. Le service lié au temps peut s'avérer essentiel dans le cas d'autres capacités de sécurité comme le contrôle d'accès ainsi que l'identification et l'authentification, selon la nature des mécanismes employés pour soutenir ces capacités.

AU-08(01) — Synchronisé avec source de temps qui fait autorité (---)

Énoncés :

Annulé : Transféré sous le contrôle SC-45(01).

Responsable : Aucun

AU-08(02) — Deuxième source de temps qui fait autorité (---)

Énoncés :

Annulé : Transféré sous le contrôle SC-45(02).

Responsable : Aucun

AU-09 — Protection de l'information de vérification (---)

Énoncés :

a. Protéger l'information de vérification et les outils de journalisation des données de vérification contre les accès non autorisés, les modifications et les suppressions
b. Alerter [Affectation : personnel ou rôles définis par l'organisation] advenant la détection d'une modification ou d'une suppression non autorisée de l'information de vérification, ou d'un accès non autorisé à celle-ci

Responsable : Aucun

Discussion :

L'information de vérification comprend tous les renseignements nécessaires pour mener à bien la vérification des activités du système, notamment les dossiers de vérification, les paramètres de journalisation des données de vérification, les rapports de vérification et les renseignements personnels. Les outils de journalisation des données de vérification sont des programmes et des dispositifs servant à mener les activités de vérification et de journalisation du système. La protection de l'information de vérification se concentre sur la protection physique et empêche des personnes non autorisées d'accéder à des outils de journalisation des données de vérification et de les exécuter. Les contrôles de protection des supports ainsi que les contrôles de protection physiques et environnementaux protègent physiquement l'information de vérification.

AU-09(01) — Supports matériels non réinscriptibles (---)

Énoncés :

Consigner les enregistrements de vérification sur des supports matériels non réinscriptibles.

Responsable : Aucun

Discussion :

La consignation des enregistrements de vérification sur des supports matériels non réinscriptibles s'applique aux pistes de vérification de première génération (c'est-à-dire les enregistrements de vérification qui constituent l'information qu'il faut utiliser à des fins de détection, d'analyse et d'élaboration de rapports) ainsi qu'aux pistes de vérification sauvegardées. La consignation des enregistrements de vérification sur des supports matériels non réinscriptibles ne s'applique pas aux enregistrements de vérification de première génération avant leur consignation dans une piste de vérification. Les supports matériels non réinscriptibles comprennent les lecteurs de disques compacts inscriptibles (CD-R pour Compact Disc-Recordable), de disques Blu-Ray (BD-R) et de disques numériques universels enregistrables (DVD-R pour Digital Versatile Disc-Recordable). À l'inverse, le recours à des supports de protection d'écriture commutables, comme des cartouches de bande magnétique ou des bus série universel (USB pour Universal Serial Bus), des disques compacts réinscriptibles (CD-RW pour Compact Disc Re-Writeable) et des supports DVD-RW (Digital Versatile Disc-Read Write) entraîne l'utilisation de supports de protection d'écriture, pas l'utilisation de supports non réinscriptibles.

AU-09(02) — Stockage sur des systèmes ou des composants physiques séparés (---)

Énoncés :

Stocker les enregistrements de vérification [Affectation : fréquence définie par l'organisation] dans un référentiel faisant partie d'un système ou d'un composant de système qui est physiquement différent du système ou du composant faisant l'objet de la vérification.

Responsable : Aucun

Discussion :

Stocker des enregistrements de vérification dans un référentiel distinct du système vérifié ou du composant de système permet de faire en sorte qu'une compromission du système faisant l'objet de la vérification ne se solde pas également par une compromission des enregistrements de vérification. Stocker des enregistrements de vérification sur des systèmes physiques ou des composants différents permet également d'assurer la confidentialité et l'intégrité des enregistrements de vérification et facilite la gestion de ces enregistrements dans le cadre d'une activité à l'échelle de l'organisation. Le stockage des enregistrements de vérification sur des systèmes ou des composants différents s'applique à la génération initiale ainsi qu'au stockage de secours ou à long terme des enregistrements de vérification.

AU-09(03) — Protection cryptographique (---)

Énoncés :

Utiliser des mécanismes cryptographiques pour protéger l'intégrité de l'information de vérification et des outils de vérification.

Responsable : Aucun

Discussion :

Les mécanismes cryptographiques de protection de l'intégrité de l'information de vérification comprennent des fonctions de hachage signées faisant appel à la cryptographie asymétrique. Cela permet de diffuser la clé publique pour vérifier l'information de hachage tout en préservant la confidentialité de la clé secrète ayant servi à générer l'algorithme de hachage.

AU-09(04) — Accès par un sous-ensemble d'utilisateurs privilégiés (---)

Énoncés :

Autoriser l'accès pour la gestion de la fonctionnalité de journalisation des données de vérification uniquement à [Affectation : sous-ensemble d'utilisatrices et utilisateurs ou de rôles privilégiés définis par l'organisation].

Responsable : Aucun

Discussion :

Les personnes ou les rôles dotés d'un accès privilégié à un système et qui sont également l'objet d'une vérification par ce système peuvent affecter la fiabilité de l'information de vérification en bloquant les activités de vérification ou en modifiant les enregistrements de vérification. Le fait d'exiger un accès privilégié mieux défini en ce qui concerne les privilèges associés aux vérifications et les autres privilèges limite le nombre d'utilisatrices et utilisateurs ou de rôles qui détiennent les privilèges associés aux vérifications.

AU-09(05) — Double autorisation (---)

Énoncés :

Appliquer le principe de double autorisation pour [Sélection (un choix ou plus) : déplacement; suppression] de [Affectation : information de vérification définie par l'organisation].

Responsable : Aucun

Discussion :

Les organisations peuvent choisir différentes options pour les divers types d'information de vérification. Les mécanismes de double autorisation, également appelée contrôle par deux personnes, exigent l'approbation de deux personnes autorisées pour exécuter les fonctions de vérification. Pour réduire le risque de collusion, les organisations considèrent la rotation des tâches à double autorisation avec d'autres particuliers. Les organisations n'ont pas besoin de mécanismes de double autorisation lorsqu'il faut agir immédiatement pour assurer la sécurité publique et environnementale.

AU-09(06) — Accès en lecture seule (---)

Énoncés :

Autoriser l'accès en lecture seule pour l'information de vérification à [Affectation : sous-ensemble d'utilisatrices et utilisateurs ou de rôles privilégiés définis par l'organisation].

Responsable : Aucun

Discussion :

En restreignant les droits d'accès aux utilisatrices et utilisateurs privilégiés pour qu'ils n'aient qu'un accès « lecture seule », on limite les possibles dommages qui pourraient être causés par ces utilisatrices et utilisateurs ou rôles, comme supprimer les enregistrements de vérification pour dissimuler des activités malveillantes.

AU-09(07) — Stockage sur composant avec un système d'exploitation différent (---)

Énoncés :

Stocker de l'information de vérification sur un composant exécutant un système d'exploitation différent du système ou du composant faisant l'objet de la vérification.

Responsable : Aucun

Discussion :

Stocker de l'information de vérification sur un composant de système exécutant un système d'exploitation différent réduit le risque qu'une vulnérabilité propre au système puisse entraîner une compromission des enregistrements de vérification.

AU-10 — Non-répudiation (---)

Énoncés :

Fournir une preuve irréfutable qu'une personne (ou un processus exécuté en son nom) a effectué [Affectation : opérations de non-répudiation définies par l'organisation].

Responsable : Aucun

Discussion :

La création d'information, l'envoi et la réception de messages et l'approbation d'information sont des exemples d'opérations de non-répudiation effectuées par des personnes. La non-répudiation protège contre toute déclaration d'une auteure ou un auteur qui nie être le créateur de certains documents, d'une émettrice ou un émetteur qui nie avoir transmis un message, d'une ou un destinataire qui nie avoir reçu un message et d'une ou un signataire qui nie avoir signé un document. Les services de non-répudiation peuvent servir à déterminer si l'information provient d'une personne en particulier, si une personne a pris des mesures particulières (par exemple, envoi d'un courriel, signature d'un contrat, approbation d'une demande d'approvisionnement) ou si elle reçoit certains renseignements. Les organisations obtiennent des services de non-répudiation grâce à plusieurs techniques ou mécanismes, notamment les signatures numériques, reçus numériques de message.

AU-10(01) — Association avec les identités (---)

Énoncés :

a. Associer l'identité de l'auteure ou auteur d'une information avec l'information de [Affectation : robustesse du lien définie par l'organisation]
b. Permettre aux personnes autorisées de déterminer l'identité de l'auteure ou auteur de l'information

Responsable : Aucun

Discussion :

Associer les identités à l'information permet de satisfaire aux exigences de vérification selon lesquelles le personnel de l'organisation doit pouvoir identifier l'auteure ou auteur d'une information particulière dans l'éventualité d'un transfert d'information. Les organisations déterminent et approuvent la robustesse du lien entre l'auteure ou auteur de l'information et l'information en fonction de la catégorie de sécurité de l'information et des facteurs de risque pertinents.

AU-10(02) — Validité du lien avec l'identité de l'auteure ou auteur de l'information (---)

Énoncés :

a. Valider le lien entre l'identité de l'auteure ou auteur de l'information et l'information [Affectation : fréquence définie par l'organisation]
b. Effectuer [Affectation : opérations définies par l'organisation] en cas d'erreur de validation

Responsable : Aucun

Discussion :

Valider le lien entre l'identité de l'auteure ou auteur de l'information et l'information permet de prévenir toute modification de l'information entre sa production et son examen. La validation des liens peut être effectuée, par exemple, au moyen des totaux de contrôle cryptographiques. Les organisations déterminent si les validations découlent des demandes d'utilisatrices et utilisateurs ou si elles sont générées automatiquement.

AU-10(03) — Chaîne de possession (---)

Énoncés :

Conserver, dans la chaîne de possession établie, l'identité et les justificatifs d'identité de l'examinatrice ou examinateur ou de l'émettrice ou émetteur pour l'information examinée ou diffusée.

Responsable : Aucun

Discussion :

La chaîne de possession est un processus qui permet de faire le suivi des transferts de l'information lors de sa collecte, de sa protection et de son cycle de vie en consignant le nom de chaque personne l'ayant traité, la date et l'heure de la collecte et du transfert de la preuve ainsi que l'objectif de son transfert. Si l'examen est effectué par une personne ou si la fonction d'examen est automatisée, mais distincte de la fonction de diffusion ou de transfert, le système associe à l'information et à l'étiquette de l'information l'identité de l'examinatrice ou examinateur de l'information à diffuser. Dans le cas d'un examen effectué par une personne, conserver les justificatifs d'identité des examinatrices et examinateurs ou des émettrices et émetteurs permet à l'organisation d'identifier la personne qui a examiné et diffusé l'information. Dans le cas d'un examen automatisé, cela permet d'assurer que seules des fonctions d'examen approuvées ont été utilisées.

AU-10(04) — Validité du lien avec l'identité de l'examinatrice ou examinateur de l'information (---)

Énoncés :

a. Valider le lien entre l'identité de l'examinatrice ou examinateur et l'information au point de transfert ou de diffusion, avant que l'information ne soit transférée ou diffusée [Affectation : d'un domaine de sécurité à un autre définis par l'organisation]
b. Effectuer [Affectation : opérations définies par l'organisation] en cas d'erreur de validation

Responsable : Aucun

Discussion :

Valider le lien entre l'identité de l'examinatrice ou examinateur de l'information et l'information aux points de transfert ou de diffusion permet de prévenir toute modification non autorisée de l'information entre son examen et son transfert ou sa diffusion. La validation des liens peut être effectuée au moyen de totaux de contrôle cryptographiques. Les organisations déterminent si les validations découlent des demandes d'utilisatrices et utilisateurs ou si elles sont générées automatiquement.

AU-10(05) — Signatures numériques (---)

Énoncés :

Annulé : Intégré au contrôle SI-07.

Responsable : Aucun

AU-11 — Conservation des enregistrements de vérification (Nc--)

Énoncés :

Conserver les enregistrements de vérification pendant [Affectation : délais définis par l'organisation et conformément à la stratégie de conservation des dossiers] pour appuyer les enquêtes après coup sur les incidents et satisfaire aux exigences réglementaires et organisationnelles de conservation de l'information.

Responsable : Aucun

Discussion :

Les organisations conservent les enregistrements de vérification jusqu'à ce qu'il soit établi qu'ils ne sont plus requis aux fins administratives, juridiques, de vérification, opérationnelles ou autres. Les organisations créent des catégories pour les enregistrements de vérification en fonction de ces types de mesures de même que des processus d'intervention pour chacun des types de mesure.

AU-11(01) — Capacité de récupération à long terme (---)

Énoncés :

Recourir à [Affectation : mesures définies par l'organisation] pour s'assurer que les enregistrements de vérification à long terme que génère le système sont récupérables.

Responsable : Aucun

Discussion :

Les organisations doivent consulter les enregistrements de vérification nécessitant un stockage à long terme (en fonction des années). On compte parmi les mesures pour faciliter la récupération des enregistrements de vérification : la conversion des enregistrements dans de nouveaux formats, la conservation de l'équipement pouvant lire les enregistrements ainsi que la conservation de documents nécessaires pour aider le personnel à comprendre comment interpréter les enregistrements.

AU-12 — Génération d’enregistrements de vérification (Nc--)

Énoncés :

a. Fournir une capacité de génération d’enregistrements de vérification pour les types d’événements que le système est en mesure de vérifier conformément au contrôle AU-02A sur [Affectation : composants du système définis par l’organisation]
b. Permettre à [Affectation : personnel ou rôles définis par l’organisation] de sélectionner les types d’événements qui doivent être journalisés par des composants de système particuliers
c. Générer des enregistrements de vérification pour les types d’événements définis au contrôle AU-02C dont le contenu des enregistrements de vérification est défini au contrôle AU-03

Responsable : Aucun

Discussion :

Les enregistrements de vérification peuvent provenir de nombreux différents composants de système. Les types d’événements indiqués au contrôle AU-02D portent sur les journaux de vérification qui doivent être générés et contiennent un sous-ensemble de tous les types d’événements pour lesquels le système peut générer des enregistrements de vérification. Si les enregistrements générés pour le processus de vérification contiennent des renseignements personnels qui ne sont pas requis pour le processus de vérification, les renseignements personnels doivent être retirés ou caviardés.

AU-12(01) — Piste de vérification à l'échelle du système et corrélée dans le temps (---)

Énoncés :

Compiler les enregistrements de vérification provenant de [Affectation : composants du système définis par l'organisation] en une piste de vérification (logique ou physique) globale qui est corrélée dans le temps, en-dedans de [Affectation : niveau de tolérance défini par l'organisation pour les relations entre les estampilles temporelles des enregistrements individuels de la piste de vérification].

Responsable : Aucun

Discussion :

Les pistes de vérification sont corrélées dans le temps lorsque les estampilles temporelles des enregistrements de vérification individuels peuvent être associées de manière fiable aux estampilles temporelles d'autres enregistrements pour permettre un classement chronologique des enregistrements à l'intérieur des limites de tolérance définies par l'organisation.

AU-12(02) — Formats normalisés (---)

Énoncés :

Produire une piste de vérification (logique ou physique) globale composée d'enregistrements de vérification dans un format normalisé.

Responsable : Aucun

Discussion :

Les enregistrements de vérification qui suivent un format commun facilitent l'interopérabilité et l'échange de l'information entre des dispositifs et des systèmes. Favoriser l'interopérabilité et l'échange d'information permet la production d'information sur les événements plus faciles à analyser et à mettre en corrélation. Dans le cas des mécanismes de journalisation qui ne sont pas conformes aux formats normalisés, les systèmes peuvent convertir chacun des enregistrements de vérification en un format normalisé au moment de compiler les pistes de vérification globales.

AU-12(03) — Modifications par des personnes autorisées (---)

Énoncés :

Permettre et mettre en oeuvre à [Affectation : liste des personnes ou des rôles définie par l'organisation] de modifier la journalisation à effectuer sur [Affectation : composants de système définis par l'organisation] en fonction de [Affectation : critères d'événement sélectionnables définis par l'organisation] dans un délai de [Affectation : délai défini par l'organisation].

Responsable : Aucun

Discussion :

Autoriser des personnes autorisées à apporter des modifications à la journalisation du système permet aux organisations d'accroître ou de limiter la journalisation au besoin pour répondre aux exigences organisationnelles. Il est possible d'accroître (de manière temporaire ou permanente) les activités de journalisation qui sont limitées pour préserver les ressources du système afin de répondre à certaines situations de menace. Les activités de journalisation peuvent aussi au contraire être limitées à un ensemble précis de types d'événements afin de faciliter la réduction des vérifications ainsi que l'analyse et les rapports de vérification. Les organisations peuvent déterminer la durée pendant laquelle les opérations de journalisation sont modifiées (par exemple, en temps quasi réel, en quelques minutes ou en quelques heures).

AU-12(04) — Vérifications des paramètres d'interrogation des renseignements personnels (---)

Énoncés :

Fournir et mettre en oeuvre la capacité de vérifier les paramètres des événements d'interrogation d'utilisatrices et utilisateurs pour des jeux de données comportant des renseignements personnels.

Responsable : Aucun

Discussion :

Les paramètres d'interrogation sont des critères explicites qu'une personne ou un système automatisé soumet à un système pour récupérer des données. La vérification des paramètres d'interrogation de jeux de données qui comportent des renseignements personnels permet à une organisation d'effectuer un meilleur suivi et de mieux comprendre l'accès, l'usage ou le partage de renseignements personnels par le personnel autorisé.

AU-13 — Surveillance de la divulgation d'information (---)

Énoncés :

a. Surveiller [Affectation : sites d'information ou sites d'information de source ouverte définis par l'organisation] [Affectation : fréquence définie par l'organisation] pour veiller à ce qu'il n'y ait aucune divulgation non autorisée d'information liée à l'organisation
b. Si une divulgation d'information est découverte :
1. Informer [Affectation : personnel ou rôles définis par l'organisation]
2. Prendre les mesures supplémentaires suivantes : [Affectation : mesures supplémentaires définies par l'organisation]

Responsable : Aucun

Discussion :

La divulgation non autorisée d'information est une forme de fuite de données.

AU-13(01) — Utilisation d’outils automatisés (---)

Énoncés :

Surveiller des sites d’information de source ouverte ou des sites d’information au moyen de [Affectation : mécanismes automatisés définis par l’organisation].

Responsable : Aucun

Discussion :

Des scripts automatisés visant à surveiller les nouveaux messages affichés sur des sites Web ainsi que des services commerciaux qui envoient des avis et des alertes aux organisations représentent des exemples de mécanismes automatisés.

AU-13(02) — Examen des sites surveillés (---)

Énoncés :

Examiner la liste des sites d'information de source ouverte faisant l'objet d'une surveillance [Affectation : fréquence définie par l'organisation].

Responsable : Aucun

Discussion :

Passer en revue sur une base régulière la liste à jour de sites d'information de source ouverte faisant l'objet d'une surveillance aide à s'assurer que les sites sélectionnés restent pertinents. Cet examen permet également d'ajouter de nouveaux sites d'information de source ouverte qui pourraient fournir une preuve de divulgation non autorisée d'information liée à l'organisation. La liste de sites surveillés peut être guidée et informée par du renseignement sur les menaces d'autres sources crédibles d'information.

AU-13(03) — Duplication non autorisée d'information (---)

Énoncés :

Employer des techniques, des processus et des outils de découverte pour déterminer si des entités externes reproduisent l'information de l'organisation de façon non autorisée.

Responsable : Aucun

Discussion :

L'utilisation ou la duplication non autorisée de l'information de l'organisation par des entités externes peut avoir des effets néfastes sur les opérations et les biens de l'organisation, en causant notamment une atteinte à la réputation. Une telle activité peut comprendre la duplication d'un site Web organisationnel par une ou un adversaire ou un auteur de menace cherchant à usurper l'identité de l'organisation d'hébergement Web. Les outils, techniques et processus de découverte utilisés pour déterminer si des entités externes reproduisent l'information de l'organisation de façon non autorisée comprennent le balayage des sites Web externes, la surveillance des médias sociaux et la formation du personnel pour repérer l'utilisation non autorisée de l'information de l'organisation.

AU-14 — Vérification des sessions (---)

Énoncés :

a. Permettre et mettre en oeuvre la capacité pour les [Affectation : utilisatrices et utilisateurs ou rôles définis par l'organisation] de [Sélection (un choix ou plus) : enregistrer; afficher; écouter; journaliser] le contenu d'une session d'utilisatrice ou utilisateur pour des [Affectation : circonstances définies par l'organisation]
b. Les activités de vérification des sessions sont mises au point, intégrées et utilisées après consultation avec des conseillères et conseillers juridiques, conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables

Responsable : Aucun

Discussion :

Les vérifications de session peuvent comprendre la surveillance des frappes et des sites Web consultés de même que l'enregistrement de l'information ou des transferts de dossiers. La capacité de vérification des sessions est mise en oeuvre avec la journalisation d'événements et peut impliquer l'application d'une technologie spécialisée de saisie des sessions. Les organisations réfléchissent à la façon dont la vérification peut révéler de l'information au sujet des personnes, ce qui donnerait lieu à des risques d'atteinte à la vie privée, et comment atténuer de tels risques. Étant donné que la vérification des sessions peut avoir une incidence sur le rendement du système et du réseau, les organisations activent la capacité en fonction de situations bien définies (par exemple, l'organisation se méfie d'une personne en particulier). Les organisations consultent une conseillère ou un conseiller juridique et des responsables de la protection de la vie privée pour s'assurer que les obligations juridiques, de protection des renseignements personnels, ou les droits reconnus par la Charte, y compris l'utilisation de renseignements personnels, sont traités de manière adéquate.

AU-14(01) — Démarrage du système (---)

Énoncés :

Lancer la vérification des sessions automatiquement au démarrage du système.

Responsable : Aucun

Discussion :

Le lancement automatique des vérifications de sessions au démarrage aide à s'assurer que l'information saisie sur des personnes données est complète et ne fait pas l'objet d'une compromission par le biais de trafiquage émanant d'auteurs de menace.

AU-14(02) — Contenu de la saisie et de l'enregistrement (---)

Énoncés :

Annulé : Intégré au contrôle AU-14.

Responsable : Aucun

AU-14(03) — Visualisation et écoute à distance (---)

Énoncés :

Fournir et mettre en oeuvre la capacité qui permet aux utilisatrices et utilisateurs autorisés de visualiser ou d'écouter à distance et en temps réel tout le contenu d'une session utilisateur établie.

Responsable : Aucun

AU-15 — Capacité de journalisation des données de vérification secondaire (---)

Énoncés :

Annulé : Transféré sous le contrôle AU-05(05).

Responsable : Aucun

AU-16 — Journalisation des données de vérification transorganisationnelle (---)

Énoncés :

Utiliser [Affectation : méthodes définies par l'organisation] pour coordonner [Affectation : information de contrôle définie par l'organisation] avec d'autres organisations lorsque l'information de contrôle est transmise au-delà des frontières organisationnelles.

Responsable : Aucun

Discussion :

La capacité de journalisation des données de vérification nécessite une approche transorganisationnelle coordonnée dans la mesure où l'organisation utilise les systèmes ou les services d'organisations externes. Par exemple, le maintien de l'identité des utilisatrices et utilisateurs qui font appel à des services offerts au-delà des frontières de l'organisation peut s'avérer difficile et toute tentative en ce sens risque de donner lieu à des ramifications importantes sur le plan des performances et du respect de la vie privée. C'est pourquoi la journalisation des données de vérification transorganisationnelle ne capture souvent que l'identité des utilisatrices et utilisateurs à l'origine des demandes d'accès au système initial, tandis que les systèmes subséquents enregistrent si ces demandes proviennent de personnes autorisées. Les organisations devraient envisager d'inclure des processus pour la coordination des exigences liées à l'information de vérification et la protection de l'information de vérification dans les ententes d'échange d'information.

AU-16(01) — Préservation de l’identité (---)

Énoncés :

Préserver l’identité des personnes dans des pistes de vérification transorganisationnelles

Responsable : Aucun

Discussion :

La préservation de l’identité s’applique dans les cas où il est nécessaire de faire le suivi des actions menées par une utilisatrice ou un utilisateur en particulier au-delà des frontières de l’organisation.

AU-16(02) — Échange d'information de vérification (---)

Énoncés :

Fournir de l'information de vérification trans-organisationnelle aux [Affectation : organisations définies par l'organisation] en vertu des [Affectation : accords liés à l'échange transorganisationnel définis par l'organisation].

Responsable : Aucun

Discussion :

L'échange d'information de vérification transorganisationnel peut s'avérer essentiel à l'analyse de la vérification effectuée en raison de l'étalement de l'information de vérification. Par exemple, les enregistrements de vérification appartenant à l'une des organisations peuvent ne pas fournir suffisamment d'information pour déterminer si les utilisatrices et utilisateurs d'autres organisations ont employé des ressources informationnelles de façon appropriée ou inappropriée. Dans certains cas, seule l'organisation où travaillent les employées et employés possèdent les connaissances nécessaires pour établir de tels faits, d'où l'importance d'échanger l'information de vérification entre organisations.

AU-16(03) — Dissociabilité (---)

Énoncés :

Mettre en oeuvre des [Affectation : mesures définies par l'organisation] pour dissocier des individus de l'information de vérification transmise au-delà des frontières organisationnelles.

Responsable : Aucun

Discussion :

Préserver les identités dans les pistes de vérification pourrait donner lieu à des ramifications sur le plan du respect de la vie privée, en permettant d'effectuer le suivi et le profilage de personnes, mais cela peut ne pas être nécessaire d'un point de vue opérationnel. Ces risques pourraient être développés davantage en transmettant de l'information au-delà des frontières organisationnelles. L'application de techniques cryptographiques renforçant la protection de la vie privée peut dissocier des individus de l'information de vérification et réduire les risques d'atteinte à la vie privée tout en préservant la responsabilisation.

CA

Évaluation des systèmes et autorisation

Security Assessment and Authorization

CA-01 — Politique et procédures d'évaluation, d'autorisation et de surveillance (---)

Énoncés :

a. Développer, consigner et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :

1. une politique d'évaluation, d'autorisation et de surveillance [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, aux directives, à la réglementation, à la jurisprudence, aux politiques, aux normes et aux lignes directrices applicables

2. des procédures pour faciliter la mise en oeuvre de la politique d'évaluation, d'autorisation et de surveillance ainsi que des contrôles de surveillance connexes

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures d'évaluation d'autorisation et de surveillance

c. Passer en revue et mettre à jour, par rapport à l'évaluation, l'autorisation et la surveillance :

1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La politique et les procédures d'évaluation, d'autorisation et de surveillance abordent les contrôles de la famille CA qui ont été mis en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les praticiennes et praticiens de la protection de la vie privée collaborent à l'élaboration de la politique et des procédures d'évaluation, d'autorisation et de surveillance. En règle générale, les politiques et les cadres liés au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin pour des politiques et des procédures propres à la mission ou au système. La politique peut être intégrée au cadre général de la sécurité et de la protection de la vie privée ou elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures d'évaluation d'autorisation et de surveillance comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets applicables, aux directives, à la réglementation, à la jurisprudence, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.

CA-02 — Évaluations de contrôle (---)

Énoncés :

a. Sélectionner l'évaluatrice ou évaluateur ou l'équipe d'évaluation qui convient pour le type d'évaluation à effectuer
b. Élaborer un plan d'évaluations de contrôle qui décrit la portée de l'évaluation, y compris :
  1. les contrôles et les améliorations de contrôle faisant l'objet d'une évaluation
  2. les procédures d'évaluation à utiliser pour déterminer l'efficacité des contrôles
  3. l'environnement d'évaluation, l'équipe d'évaluation et les rôles et responsabilités liés à l'évaluation
c. S'assurer que le plan d'évaluation des contrôles est examiné et approuvé par l'autorité responsable ou une représentante ou un représentant désigné avant d'effectuer l'évaluation
d. Évaluer les contrôles du système et l'environnement dans lequel il est exploité [Affectation : fréquence définie par l'organisation] pour déterminer dans quelle mesure les contrôles ont été mis en oeuvre correctement, s'ils fonctionnent comme prévu et s'ils produisent les résultats escomptés tout en respectant les exigences relatives à la sécurité et à la protection de la vie privée
e. Produire un rapport d'évaluation de contrôle qui documente les résultats de l'évaluation
f. Remettre les résultats de l'évaluation des contrôles à [Affectation : personnel et rôles définis par l'organisation]

Responsable : Aucun

Discussion :

Les organisations s'assurent que les évaluatrices et évaluateurs des contrôles possèdent les compétences et l'expertise nécessaires pour élaborer des plans d'évaluation efficaces et pour mener des évaluations de contrôles propres au système, hybrides et communes, et diriger des programmes et des activités de développement de système, au besoin. À cet égard, les praticiennes et praticiens de la protection de la vie privée doivent posséder les compétences et l'expertise technique pour évaluer la conformité de l'activité liée à un programme en ce qui a trait aux exigences de protection de la vie privée. Les compétences nécessaires peuvent comprendre une connaissance générale des concepts et des approches en matière de gestion des risques ainsi qu'une connaissance exhaustive et une expérience des composants de systèmes matériels, logiciels et micrologiciels installés. La connaissance des obligations en matière de protection des renseignements personnels, comme il est documenté dans la loi, la réglementation, la jurisprudence et l'ensemble des politiques, est nécessaire pour effectuer les EFVP. Les organisations évaluent les contrôles dans les systèmes et les environnements dans lesquels ces systèmes fonctionnent dans le cadre des autorisations initiales ou continues du système, de la surveillance continue, de la conception et du développement des systèmes, de l'ingénierie de la sécurité et de la protection de la vie privée des systèmes, et du cycle de développement des systèmes comme il est recommandé dans les documents Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée (ITSP.10.036) et Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes (ITSP.10.037). Les évaluations aident à assurer que les organisations respectent les exigences de sécurité et de protection de la vie privée, à identifier les faiblesses et les lacunes dans le processus de conception et de développement du système, et à fournir les renseignements essentiels nécessaires pour prendre des décisions en fonction des risques dans le cadre des processus d'autorisation, et assurer le respect des procédures d'atténuation des vulnérabilités. Les organisations effectuent des évaluations des contrôles mis en oeuvre comme il est documenté dans les plans de sécurité et de protection de la vie privée. Bien qu'il soit possible d'effectuer les évaluations tout au long du cycle de développement des systèmes dans le cadre des processus d'ingénierie des systèmes et d'ingénierie de la sécurité des systèmes, il est recommandé de réaliser les évaluations tôt pendant la phase de conception pour s'assurer que la protection de la protection de la vie privée et de la sécurité soit prise en compte dans le programme ou la conception du système. La conception pour les contrôles peut être évaluée alors que les demandes de proposition sont élaborées, les interventions évaluées et les revues de conception effectuées. Si une conception pour mettre en oeuvre des contrôles et une mise en oeuvre subséquente conformément à la conception sont évaluées durant la phase de développement, l'essai final des contrôles peut s'avérer une simple confirmation faisant appel à une évaluation de contrôle précédemment effectuée et à des résultats combinés. Les organisations peuvent élaborer un seul plan consolidé d'évaluation de la sécurité et de la protection de la vie privée pour le système ou tenir à jour plusieurs plans distincts. Un plan d'évaluation consolidé délimite clairement les rôles et les responsabilités lors de l'évaluation de contrôle. Si plusieurs organisations participent à l'évaluation d'un système, une approche coordonnée peut permettre de réduire les redondances et les coûts connexes. Les organisations peuvent mener d'autres types d'activités d'évaluation, comme l'analyse des vulnérabilités et la surveillance du système, pour maintenir la posture de sécurité et de protection de la vie privée des systèmes durant tout leur cycle de vie. Les rapports d'évaluation consignent les résultats à un niveau que les organisations jugent suffisamment détaillé pour leur permettre d'en déterminer l'exactitude et l'exhaustivité et d'établir dans quelle mesure les contrôles sont mis en oeuvre correctement, fonctionnent comme prévu et produisent les résultats escomptés tout en respectant les exigences relatives aux contrôles. Les résultats des évaluations sont présentés aux personnes ou aux rôles appropriés pour les types d'évaluations menées. Par exemple, les évaluations effectuées pour soutenir les décisions d'autorisation sont fournies aux autorités responsables, aux cadres supérieures et supérieurs appropriés en matière de protection de la vie privée, aux cadres supérieures et supérieurs de la gouvernance en matière de sécurité du ministère, et aux représentantes et représentants désignés par l'autorité responsable. Pour répondre aux exigences liées aux évaluations périodiques, les organisations peuvent avoir recours aux résultats d'évaluation provenant des sources suivantes : autorisations initiales ou continues du système d'information, surveillance continue, processus

d'ingénierie des systèmes ou activités du cycle de développement du système. Les organisations s'assurent que les résultats d'évaluation sont actuels et pertinents afin de déterminer l'efficacité des contrôles et qu'ils sont obtenus conformément au niveau requis d'indépendance de l'évaluatrice ou évaluateur. On peut réutiliser les résultats d'évaluation d'un contrôle dans la mesure où ils demeurent valables et qu'ils peuvent être complétés par d'autres évaluations, au besoin. Après les autorisations initiales, les organisations évaluent les contrôles pendant une surveillance continue. Elles établissent également la fréquence des évaluations de contrôle de sécurité permanentes conformément aux stratégies de surveillance continue des organisations. Les vérifications externes, y compris celles effectuées par des entités externes, comme les organismes réglementaires sont hors de la portée du contrôle CA-02.

CA-02(01) — Évaluatrices et évaluateurs indépendants (---)

Énoncés :

Utiliser des évaluatrices et évaluateurs ou des équipes d'évaluatrices et évaluateurs indépendants pour mener des évaluations de contrôle.

Responsable : Aucun

Discussion :

Les évaluatrices et évaluateurs ou les équipes d'évaluatrices et évaluateurs indépendants sont des personnes ou des groupes chargés de mener des évaluations impartiales des systèmes. L'impartialité signifie que les évaluatrices et évaluateurs ne doivent en aucun cas se trouver en conflit d'intérêts, subjectif ou réel, en ce qui a trait au développement, aux opérations, au maintien ou à la gestion des systèmes qui font l'objet d'évaluations ou en ce qui a trait à l'établissement de l'efficacité du contrôle. Pour assurer l'impartialité, les évaluatrices et évaluateurs n'ont pas un intérêt commun ou concurrentiel avec les organisations pour lesquelles ils mènent des évaluations, ils évaluent leur propre travail, agissent en tant que gestionnaires ou employées et employés des organisations pour lesquelles ils mènent les évaluations ou agissent à titre de conseillères et de conseillers pour les organisations qui ont recours à leurs services. Les évaluations indépendantes peuvent être menées par des éléments des organisations ou par des sous-traitants provenant d'entités publiques ou privées extérieures aux organisations concernées. Les autorités responsables déterminent le niveau d'indépendance requis en fonction des catégories de sécurité liées aux systèmes ou au risque associé aux opérations, à la sensibilité des renseignements personnels connexes, aux biens et aux personnes de l'organisation. Les autorités responsables déterminent également si ce niveau d'indépendance est suffisant pour que l'organisation puisse avoir confiance que les résultats sont fiables et peuvent servir à prendre des décisions crédibles concernant les risques. L'établissement de l'indépendance des évaluatrices et évaluateurs comprend de déterminer si les sous-traitants qui offrent les services d'évaluation sont assez indépendants, par exemple lorsque les propriétaires de systèmes ne participent pas directement aux processus contractuels ou qu'ils ne peuvent pas influencer indûment l'objectivité des évaluatrices et évaluateurs. Durant la conception du système et la phase de développement, le fait d'avoir des évaluatrices et évaluateurs indépendants est similaire au fait d'avoir des spécialistes en la matière impliquées ou impliqués dans les revues de conception. Lorsque les organisations qui détiennent les systèmes sont de petite taille ou lorsque les structures organisationnelles exigent que les évaluations soient menées par des personnes qui font partie de la chaîne de développement, d'opérations ou de gestion des propriétaires des systèmes, on peut s'assurer de l'indépendance des processus d'évaluation en examinant minutieusement les résultats des évaluations et en veillant à ce que des équipes de spécialistes indépendants mènent des analyses pour valider le caractère exhaustif, l'exactitude, l'intégrité et la fiabilité des résultats. Les évaluations menées autrement que pour appuyer directement les décisions liées aux autorisations – si elles sont menées par des évaluatrices et évaluateurs suffisamment indépendants – risquent d'être davantage utiles pour prendre ce genre de décisions, ce qui permet de réduire le besoin de répéter les évaluations.

CA-02(02) — Évaluations spécialisées (---)

Énoncés :

Elles comprennent dans le cadre des évaluations de contrôle, [Affectation : fréquence définie par l'organisation], [Sélection (un choix) : annoncé; non annoncé], [Sélection (un choix ou plus) : une surveillance approfondie; une instrumentation de sécurité; des cas de tests de sécurité automatisés; une analyse des vulnérabilités; des tests liés aux utilisatrices et utilisateurs malveillants; une évaluation des menaces internes; des tests de charge et de performance; une évaluation des fuites de données ou des pertes de données; {Affectation : autres formes d'évaluation de sécurité définies par l'organisation}].

Responsable : Aucun

Discussion :

Les organisations peuvent mener des évaluations spécialisées, y compris des vérifications et des validations, la surveillance des systèmes, l'évaluation de menaces internes, des tests concernant les utilisatrices et utilisateurs malveillants ou tout autre test. Ces évaluations peuvent permettre de mieux se préparer en mettant en oeuvre des capacités organisationnelles et en indiquant les niveaux de performance actuels afin d'orienter les efforts et d'accroître ainsi la sécurité et la protection de la vie privée. Les organisations mènent des évaluations spécialisées conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Les autorités responsables approuvent les méthodes d'évaluation parallèlement à la fonction de gestion des risques organisationnels. Les organisations peuvent inclure les vulnérabilités découvertes durant les évaluations aux processus d'atténuation des vulnérabilités. Les évaluations spécialisées peuvent également être menées tôt pendant le cycle de développement de systèmes (par exemple, pendant la conception initiale, le développement et les tests unitaires).

CA-02(03) — Tirer parti des résultats d'évaluation provenant d'organisations externes (---)

Énoncés :

Tirer parti des résultats des évaluations de contrôle menées par [Affectation : organisation externe désignée par l'organisation] sur le [Affectation : système désigné par l'organisation] lorsque l'évaluation respecte [Affectation : exigences définies par l'organisation].

Responsable : Aucun

Discussion :

Les organisations peuvent compter sur des évaluations de contrôle des systèmes organisationnels menées par des organisations externes. En recourant à ces évaluations et en réutilisant l'information provenant d'évaluations déjà menées, les organisations diminuent le temps et les ressources nécessaires aux activités d'évaluation en limitant le nombre d'activités d'évaluation indépendante qu'elles doivent mener. Les facteurs dont elles peuvent tenir compte pour déterminer si les résultats d'évaluation provenant d'organisations externes sont acceptables peuvent varier. Parmi ces facteurs, on compte les expériences antérieures de l'organisation avec l'organisation qui a mené l'évaluation, la réputation de l'organisation d'évaluation, le niveau de détails appuyant les données d'évaluation fournies et les mandats imposés en vertu des lois, des décrets, des directives, des politiques, de la réglementation, des normes et des lignes directrices applicables.

CA-03 — Échange d'information (---)

Énoncés :

a. Approuver et gérer l'échange d'information entre le système et d'autres systèmes au moyen de [Sélection (un choix ou plus) : ententes sur la sécurité des interconnexions; ententes sur la sécurité de l'échange d'information; ententes ou protocoles d'entente; accords d'échange de renseignements; ententes d'échange de renseignements; accords sur les niveaux de service; ententes avec les utilisatrices et utilisateurs; accords de non-divulgation; {Affectation : type d'entente défini par l'organisation}]
b. Consigner, dans le cadre des ententes d'échange, les caractéristiques d'interface, les exigences de sécurité et de protection de la vie privée ainsi que les responsabilités liées à chacun des systèmes, et le niveau d'incidence de l'information communiquée
c. Examiner et tenir à jour les ententes [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

Les exigences en matière d'échange d'information du système s'appliquent aux échanges d'information entre au moins deux systèmes. Les échanges d'information du système comprennent les connexions par des liaisons louées ou des RPV, des connexions aux fournisseurs d'accès Internet, le partage ou l'échange de renseignements sur les transactions de bases de données, des connexions et des échanges avec des services infonuagiques, des échanges par des services sur le Web, ou des échanges de fichiers par des protocoles de transfert de fichiers, des protocoles réseau (par exemple, IPv4, IPv6), courriel ou d'autres communications entre organisations. L'information échangée devrait se limiter à la quantité minimale de renseignements personnels nécessaires. Les organisations doivent considérer les risques associés aux menaces nouvelles ou grandissantes qui peuvent être introduites lorsque les systèmes échangent de l'information avec d'autres systèmes qui peuvent avoir des contrôles et des exigences de sécurité et de protection de la vie privée différents. Cela comprend les systèmes au sein de la même organisation et les systèmes qui sont à l'extérieur de l'organisation. Une autorisation conjointe des systèmes qui échangent de l'information, comme il est décrit dans le contrôle CA-06(01) ou CA-06(02), peut faciliter la communication et réduire le risque. Les autorités responsables déterminent le risque associé à l'échange d'information du système et les contrôles requis pour appliquer des mesures d'atténuation des risques adéquates. Les types d'ententes doivent être sélectionnés en fonction de facteurs comme le niveau d'incidence de l'information échangée, la relation entre les organisations qui échangent de l'information (par exemple, d'un organisme gouvernemental à un autre, d'un organisme gouvernemental à une entreprise, d'une entreprise à une autre, d'un organisme gouvernemental ou d'une entreprise à un fournisseur de services, d'un organisme gouvernemental ou d'une entreprise à personne) ou le niveau d'accès au système organisationnel par les utilisatrices et utilisateurs de l'autre système. Si les systèmes qui échangent de l'information sont associés à la même autorité responsable, les organisations peuvent ne pas avoir besoin d'élaborer des ententes. En effet, les caractéristiques d'interface entre les systèmes (par exemple, la façon dont l'information est échangée, comment l'information est protégée et l'utilisation autorisée de l'information) sont décrites dans les plans de sécurité et de protection de la vie privée. Si les systèmes qui échangent de l'information sont associés aux mêmes autorités responsables au sein de la même organisation, les organisations peuvent élaborer des ententes ou fournir la même information qui serait fourni dans le type d'entente approprié à partir du contrôle CA-03A dans les plans respectifs de sécurité et de protection de la vie privée pour les systèmes. Les organisations peuvent intégrer l'information des ententes dans des contrats officiels, en particulier pour les échanges d'information entre des ministères et organismes gouvernementaux et des organisations non gouvernementales (comme des prestataires de services, des entrepreneures et entrepreneurs, des développeuses et développeurs de systèmes et des intégratrices et intégrateurs de systèmes). Les risques concernent les systèmes qui partagent les mêmes réseaux.

CA-03(01) — Connexions à des systèmes de sécurité nationaux non classifiés (---)

Énoncés :

Annulé : Transféré sous le contrôle SC-07(25).

Responsable : Aucun

CA-03(02) — Connexions à des systèmes de sécurité nationaux classifiés (---)

Énoncés :

Annulé : Transféré sous le contrôle SC-07(26).

Responsable : Aucun

CA-03(03) — Connexions à des systèmes de sécurité non nationaux non classifiés (---)

Énoncés :

Annulé : Transféré sous le contrôle SC-07(27).

Responsable : Aucun

CA-03(04) — Connexions aux réseaux publics (---)

Énoncés :

Annulé : Transféré sous le contrôle SC-07(28).

Responsable : Aucun

CA-03(05) — Connexions restreintes à des systèmes externes (---)

Énoncés :

Annulé : Transféré sous le contrôle SC-07(05).

Responsable : Aucun

CA-03(06) — Autorisations de transfert (---)

Énoncés :

Vérifier que les personnes ou les systèmes qui transfèrent des données entre des systèmes interconnectés ont les autorisations nécessaires (c'est-à-dire des autorisations écrites ou privilégiées) avant d'accepter de telles données.

Responsable : Aucun

Discussion :

Pour éviter que des personnes ou des systèmes non autorisés puissent effectuer des transferts d'information vers des systèmes protégés, le système protégé, par des moyens indépendants, si la personne ou le système qui tente le transfert d'information est autorisé à le faire. La vérification de l'autorisation à transférer l'information vise également le trafic du plan de contrôle (par exemple, le routage et le DNS) et les services (par exemple, les relais SMTP authentifiés).

CA-03(07) — Échanges d’information éphémère (---)

Énoncés :

a. Identifier les échanges d’information éphémères (en aval) avec d’autres systèmes par le biais des systèmes identifiés au contrôle CA-03A
b. Prendre les mesures nécessaires pour assurer que les échanges d’information éphémères (en aval) cessent lorsqu’il devient impossible de vérifier ou de valider les contrôles sur des systèmes (en aval) éphémères

Responsable : Aucun

Discussion :

Les échanges d’information éphémère ou en aval sont des échanges d’information entre le système ou les systèmes avec lesquels le système de l’organisation échange de l’information et d’autres systèmes. Pour les applications, les systèmes et les services essentiels à la mission, notamment les biens de grande importance, il est nécessaire d’identifier de tels échanges d’information. La transparence des contrôles ou les mesures de protection en place dans de tels systèmes en aval connectés directement ou indirectement aux systèmes organisationnels sont essentielles pour bien comprendre les risques liés à la sécurité et à la protection de la vie privée résultant de ces échanges d’information. Les systèmes organisationnels peuvent hériter de risques provenant de systèmes en aval par le biais de connexion éphémères ou d’échanges d’information qui peuvent rendre les systèmes organisationnels plus susceptibles aux menaces, aux risques et aux incidences négatives.

CA-04 — Certification de sécurité (---)

Énoncés :

Annulé : Intégré au contrôle CA-02.

Responsable : Aucun

CA-05 — Plan d’action et des jalons (---)

Énoncés :

a. Développer un plan d’action et des jalons pour le système afin de consigner les mesures correctives de l’organisation pour corriger les faiblesses ou les lacunes relevées durant l’évaluation des contrôles et pour réduire et éliminer les vulnérabilités connues du système
b. Mettre à jour le plan d’action et les jalons existants [Affectation : fréquence définie par l’organisation] en tenant compte des constatations des évaluations de contrôles, des vérifications ou des examens indépendants et des activités de surveillance continue

Responsable : Aucun

Discussion :

Les plans d’action et des jalons sont utiles pour tout type d’organisation pour faire le suivi des mesures correctives planifiées. Par respect de la protection de la vie privée, le plan d’action et des jalons est souvent consigné dans l’EFVP. La réponse de la direction au risque associé et à l’engagement de la gardienne ou du gardien à l’égard de l’atténuation des risques d’atteinte à la vie privée devrait être documentée dans l’artéfact du plan d’action et des jalons. Le plan de sécurité et de protection de la vie privée et le plan d’action et des jalons documentent différents aspects de conformité nécessaire. Bien qu’il puisse y avoir un certain chevauchement, il est à noter qu’en général, les documents n’indiquent pas les mêmes risques.

CA-05(01) — Automatisation du soutien aux fins d'exactitude et d'actualité (---)

Énoncés :

Assurer l'exactitude, l'actualité et la disponibilité du plan d'action et des jalons pour le système se servant de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Utiliser des outils automatisés contribue à assurer l'exactitude, l'actualité et la disponibilité du plan d'action et des jalons, et facilite la coordination et l'échange d'évaluations de la conformité en matière de sécurité et de protection de la vie privée dans l'ensemble de l'organisation. Cette coordination et cet échange d'information permettent de mieux identifier les faiblesses ou lacunes systémiques des systèmes organisationnels et ils veillent à ce que les ressources appropriées soient appliquées aux vulnérabilités des systèmes les plus critiques, et ce, en temps opportun.

CA-06 — Autorisation (---)

Énoncés :

a. Attribuer à une cadre supérieure ou un cadre supérieur le rôle d'autorité responsable ou de gardienne ou gardien du système
b. Attribuer à une cadre supérieure ou un cadre supérieur le rôle d'autorité responsable ou de gardienne ou gardien des contrôles courants pouvant être hérités par les systèmes organisationnels
c. S'assurer que l'autorité responsable ou la gardienne ou le gardien du système, avant de débuter les opérations :
    1. accepte l'utilisation de contrôles communs hérités par le système
    2. autorise l'exploitation du système
d. S'assurer que l'autorité responsable ou la gardienne ou le gardien des contrôles communs autorise l'utilisation de ces contrôles pour que les systèmes organisationnels en héritent
e. Mettre à jour les autorisations [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

Les autorisations de sécurité sont des décisions de gestion officielles qu'une ou un cadre supérieur communique pour autoriser l'exploitation de systèmes, autoriser l'utilisation de contrôles communs pouvant être hérités par les systèmes organisationnels et accepter explicitement les risques concernant les activités, les biens et les personnes liés à l'organisation ainsi que les autres organisations et le gouvernement, tant qu'un ensemble convenu de contrôles est mis en oeuvre. Les autorités responsables supervisent le budget lié aux systèmes organisationnels et contrôles communs ou s'occupent des fonctions liées à la mission et aux activités qui sont prises en charge par ces systèmes ou contrôles communs. Les autorités responsables ou les gardiennes et gardiens sont responsables et imputables quant aux risques en matière de sécurité et de protection de la vie privée associés à l'exploitation et à l'utilisation des systèmes organisationnels. Les organismes non gouvernementaux peuvent faire appel à des processus similaires pour accorder des droits d'accès aux systèmes et aux cadres supérieures et supérieurs qui assument le rôle d'autorisation et des responsabilités connexes. Les autorités responsables ou les gardiennes et gardiens émettent des autorisations permanentes pour des systèmes en se basant sur des éléments de preuve tirés de programmes de surveillance continue mis en oeuvre. Les programmes de surveillance continue robustes réduisent la nécessité de recourir à des processus de réautorisation distincts. En recourant à des processus de surveillance continue et exhaustive, l'information contenue dans les trousses d'autorisation (c'est-à-dire les plans de sécurité et de protection de la vie privée, les rapports d'évaluation, ainsi que les plans d'action et les jalons) peut continuellement être mise à jour. Cela fournit aux autorités responsables et aux gardiennes et gardiens de systèmes un aperçu de l'état de la posture de sécurité et de protection de la vie privée de leurs systèmes et de leurs environnements d'exploitation. Pour réduire les coûts associés aux réautorisations, les autorités responsables ou les gardiennes et gardiens utilisent autant que possible les résultats du processus de surveillance continue pour prendre les décisions concernant ces réautorisations.

CA-06(01) — Autorisation conjointe (au sein de l'organisation) (---)

Énoncés :

Faire appel à un processus d'autorisation conjointe pour le système qui comprend plusieurs autorités responsables de la même organisation menant le processus d'autorisation.

Responsable : Aucun

Discussion :

Affecter plusieurs autorités responsables ou gardiennes et gardiens d'une même organisation aux rôles d'autorités coresponsables pour le système augmente le niveau d'indépendance dans le cadre du processus de prise de décisions fondée sur le risque. Cela implique également la mise en oeuvre de concepts de séparation des tâches et de double autorisation tel qu'il est appliqué au processus d'autorisation du système. Le processus d'autorisation conjointe au sein de l'organisation est plus pertinent pour les systèmes connectés, les systèmes partagés et les systèmes ayant plusieurs propriétaires de l'information.

CA-06(02) — Autorisation conjointe (interorganisation) (---)

Énoncés :

Faire appel à un processus d'autorisation conjointe pour le système qui comprend plusieurs autorités responsables avec au moins une ou un responsable de l'autorisation provenant d'une organisation à l'extérieur de l'organisation menant le processus d'autorisation.

Responsable : Aucun

Discussion :

Affecter plusieurs autorités responsables, alors qu'au moins une provient d'une organisation externe, pour occuper les rôles d'autorités coresponsables pour le système augmente le niveau d'indépendance dans le cadre du processus de prise de décisions fondée sur le risque. Cela implique la mise en oeuvre de concepts de séparation des tâches et de double autorisation tel qu'il est appliqué au processus d'autorisation du système. Se servir d'autorités responsables d'organisations externes pour compléter l'équipe d'autorités responsables de l'organisation à qui appartient le système ou qui héberge celui-ci peut s'avérer nécessaire lorsque les organisations externes ont un intérêt manifeste dans les résultats de la décision d'autorisation. Le processus d'autorisation conjointe interorganisation est pertinent et convient aux systèmes connectés, aux services ou systèmes partagés et aux systèmes ayant plusieurs propriétaires de l'information. Les autorités responsables des organisations externes sont des principales et principaux intervenants du système faisant l'objet de l'autorisation.

CA-07 — Surveillance continue (---)

Énoncés :

Élaborer et mettre en oeuvre une stratégie de surveillance continue des systèmes conformément à la stratégie de surveillance continue de l'organisation qui comprend :
a. Établir les mesures au niveau du système à surveiller pour : [Affectation : mesures au niveau du système définies par l'organisation]
b. la mise en place d'activités de surveillance [Affectation : fréquences définies par l'organisation] et [Affectation : fréquences définies par l'organisation] pour l'évaluation de l'efficacité des contrôles
c. les évaluations de contrôle de sécurité permanentes conformément aux stratégies de surveillance continue
d. la surveillance en permanence des mesures, conformément à la stratégie de surveillance continue définie par l'organisation
e. la corrélation et l'analyse de l'information générée par les évaluations de contrôle et la surveillance
f. les mesures d'intervention concernant les résultats qui découlent de l'analyse de l'information
g. le signalement de l'état de la sécurité et de la protection de la vie privée du système à la ou au [Affectation : personnel ou rôles définis par l'organisation] [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

La surveillance continue du système facilite une sensibilisation permanente de la sécurité du système et de la posture liée à la protection de la vie privée afin d'appuyer les décisions relatives à la gestion des risques organisationnels. Les termes « continu » et « permanent » signifient que les organisations évaluent et surveillent leurs contrôles et leurs risques à une fréquence suffisante pour appuyer les décisions en fonction des risques. Différents types de contrôles peuvent nécessiter différentes fréquences de surveillance. Les résultats associés à une surveillance continue sont à l'origine des mesures d'intervention liées aux risques que mettent en oeuvre les organisations. Lorsque vient le temps de surveiller l'efficacité de multiples contrôles qui ont été groupés selon des capacités, une analyse des causes fondamentales peut s'avérer nécessaire pour déterminer le contrôle qui a échoué. Grâce aux programmes de surveillance continue, les organisations peuvent maintenir en permanence les autorisations des systèmes de même que les contrôles communs dans un environnement d'exploitation très dynamique où les menaces, les vulnérabilités, les technologies et les besoins liés à la mission et aux activités sont en constante évolution. En pouvant accéder en tout temps à de l'information sur la sécurité et la protection de la vie privée dans les rapports ou les tableaux de bord, les responsables des organisations peuvent prendre des décisions sur la gestion des risques de façon efficace et opportune, comme des décisions sur les autorisations permanentes. Parfois, la surveillance peut impliquer la collecte ou la création de renseignements personnels et un niveau de protection convenable doit être appliqué. L'automatisation permet d'appuyer des mises à jour plus fréquentes des inventaires de matériel, de logiciels et de micrologiciels, ainsi que d'autres systèmes. Il est possible d'accroître l'efficacité lorsque les résultats de la surveillance continue sont modifiés de sorte à fournir de l'information précise, mesurable, concrète, pertinente et opportune. Les activités de surveillance continue sont adaptées aux catégories de sécurité des systèmes. Les exigences en matière de surveillance du système, y compris une surveillance spécifique, peuvent se trouver dans d'autres exigences, comme AC-2G, AC-02(07), AC-02(12)a, AC-02(07)b, AC-02(07)c, AC-17(01), AT-04A, AU-13, AU-13(01), AU-13(02), CM-03F, CM-06D, CM-11C, IR-05, MA-02B, MA-03A, MA-04A, PE-03D, PE-06, PE-14B, PE-16, PE-20, PM-06, PM-23, PM-31, PS-07E, SA-09C, SR-04, SC-05(03)b, SC-07A, SC-07(24)b, SC-18B, SC-43B et SI-04.

CA-07(01) — Évaluation indépendante (---)

Énoncés :

Faire appel à des évaluatrices et évaluateurs indépendants ou à des équipes d'évaluation pour surveiller en permanence les contrôles du système.

Responsable : Aucun

Discussion :

Les organisations peuvent optimiser la valeur de leurs évaluations de contrôles en demandant que les évaluations soient effectuées par des évaluatrices et évaluateurs détenant un niveau d'indépendance suffisant. Le niveau d'indépendance requis est basé sur les stratégies de surveillance continue des organisations. L'indépendance des évaluatrices et évaluateurs offre un degré d'impartialité au processus de surveillance. Pour assurer cette impartialité, les évaluatrices et évaluateurs n'ont pas un intérêt commun ou concurrentiel avec les organisations pour lesquelles ils mènent des évaluations, ils évaluent leur propre travail, agissent en tant que gestionnaires ou employées et employés des organisations pour lesquelles ils mènent les évaluations ou agissent à titre de conseillères et conseillers pour les organisations qui ont recours à leurs services.

CA-07(02) — Types d’évaluations (---)

Énoncés :

Annulé : Intégré au contrôle CA-02.

Responsable : Aucun

CA-07(03) — Analyses des tendances (---)

Énoncés :

Utiliser des analyses de tendances pour déterminer s'il faut modifier les mises en oeuvre de contrôles, la fréquence des activités de surveillance continue ou tout autre type d'activités utilisées dans le cadre du processus de surveillance continue, en se basant sur des données empiriques.

Responsable : Aucun

Discussion :

On compte parmi les analyses de tendances l'examen de l'information récente sur les menaces associées aux types d'événements menaçants qui ont eu lieu au sein de l'organisation, des taux de réussite de certains types d'attaques, des vulnérabilités émergentes dans les technologies, des techniques d'ingénierie sociale qui ne cessent d'évoluer, de l'efficacité des paramètres de configuration, des résultats provenant de différentes évaluations de contrôle et les constatations des vérificatrices et vérificateurs.

CA-07(04) — Surveillance des risques (---)

Énoncés :

S'assurer que la surveillance des risques fait partie intégrante de la stratégie de surveillance continue qui comprend ce qui suit :
a. la surveillance de l'efficacité
b. la surveillance de la conformité
c. la surveillance des changements

Responsable : Aucun

Discussion :

La surveillance des risques s'appuie sur la tolérance au risque établie de l'organisation. La surveillance de l'efficacité détermine l'efficacité continue des mesures d'intervention mises en oeuvre et qui sont liées aux risques. La surveillance de la conformité permet de s'assurer que les mesures d'intervention liées aux risques sont mises en oeuvre. Elle vérifie également que les exigences de sécurité et de protection de la vie privée sont respectées. La surveillance des changements détermine les changements apportés aux systèmes de l'organisation et aux environnements d'exploitation pouvant toucher le risque lié à la sécurité et à la protection de la vie privée.

CA-07(05) — Analyse de la cohérence (---)

Énoncés :

Utiliser les mesures suivantes pour valider que les stratégies sont établies et que les contrôles mis en oeuvre sont fonctionnels de façon uniforme : [Affectation : actions définies par l'organisation].

Responsable : Aucun

Discussion :

Les contrôles de sécurité et de protection de la vie privée sont souvent ajoutés graduellement à un système. Par conséquent, il peut arriver que les stratégies pour la sélection et la mise en oeuvre de contrôles puissent ne pas convenir, et les contrôles pourraient ne pas fonctionner ensemble de manière cohérente ou coordonnée. Au minimum, le manque de cohérence et de coordination pourrait indiquer des lacunes inacceptables sur le plan de la conformité en matière de sécurité et de protection de la vie privée dans le système. Au pire, cela pourrait indiquer que certains des contrôles mis en oeuvre dans un emplacement ou par un composant, compromettent la fonctionnalité d'autres contrôles (par exemple, chiffrer le trafic des réseaux internes peut nuire à la surveillance). Dans d'autres situations, ne pas surveiller de manière cohérente tous les protocoles réseau mis en oeuvre (par exemple, une double pile du protocole IPv4 et du protocole IPv6) peut créer des vulnérabilités non désirées dans le système, lesquelles pourraient être exploitées par des adversaires. Il est important de vérifier – par des tests, une surveillance et une analyse – que les contrôles mis en oeuvre fonctionnent de manière cohérente, coordonnée et sans interférence.

CA-07(06) — Soutien automatisé pour la surveillance (---)

Énoncés :

Assurer l'exactitude, l'actualité et la disponibilité des résultats de surveillance pour le système en se servant de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Utiliser des outils automatisés contribue à assurer l'exactitude, l'actualité et la disponibilité de l'information de surveillance, ce qui aide ensuite à accroître le niveau de sensibilisation permanente de la posture de sécurité et de protection de la vie privée du système afin d'appuyer les décisions relatives à la gestion des risques organisationnels. Si un tiers fournit un soutien automatisé,des mesures de protection liées à la collecte et à l'utilisation par le fournisseur de tout renseignement personnel connexe doivent être en place dans le mécanisme de passation de marchés.

CA-08 — Tests d’intrusion (---)

Énoncés :

Effectuer des tests d’intrusion [Affectation : fréquence définie par l’organisation] sur [Affectation : systèmes ou composants de systèmes définis par l’organisation].

Responsable : Aucun

Discussion :

Les tests d’intrusion sont des évaluations spécialisées menées sur des systèmes ou sur des composants des systèmes individuels qui visent à détecter des vulnérabilités que pourraient exploiter des adversaires. Les tests d’intrusion vont au-delà de l’analyse des vulnérabilités automatiques et ils sont exécutés par des agentes et agents ainsi que des équipes ayant des compétences et une expérience manifestes comprenant une expertise technique des réseaux, des systèmes d’exploitation ou de la sécurité au niveau des applications. Il est possible d’avoir recours à ces tests pour valider les vulnérabilités ou déterminer le niveau de résistance à l’intrusion des systèmes face à des adversaires en tenant compte de certaines contraintes. Parmi ces contraintes, notons le temps, les ressources et les compétences. Les tests d’intrusion tentent de reproduire les actions des adversaires et ils fournissent une analyse plus en profondeur des faiblesses ou des lacunes en lien à la sécurité et à la protection de la vie privée. Ces tests sont particulièrement importants lorsque les organisations passent des anciennes technologies aux nouvelles technologies (par exemple, le passage des protocoles réseau IPv4 à IPv6). Les organisations peuvent se servir des résultats des analyses des vulnérabilités pour soutenir les activités liées aux tests d’intrusion. Ces tests peuvent être effectués à l’interne ou à l’externe sur des composants matériels, logiciels et micrologiciels d’un système et peuvent exercer des contrôles à la fois physiques et techniques. Une méthode utilisée dans le cadre de ces tests consiste à mener une analyse prétest basée sur une connaissance détaillée du système, à effectuer une détection prétest des vulnérabilités potentielles basée sur l’analyse prétest et à réaliser des tests conçus pour déterminer l’exploitabilité des vulnérabilités. Toutes les parties doivent convenir des règles d’engagement avant le début des scénarios de test d’intrusion. Il faut établir une corrélation entre ces règles d’engagement et les outils, les techniques ainsi que les procédures dont on prévoit l’utilisation par les adversaires qui lanceront les attaques. Les tests d’intrusion peuvent mener à l’exposition de l’information qui est protégée par des lois ou de la réglementation, pour les personnes effectuant les tests. Des règles d’engagement, des contrats ou d’autres mécanismes appropriés peuvent être utilisés pour communiquer les attentes sur la façon de protéger cette information. Les évaluations des risques permettent de guider les décisions relatives au niveau d’indépendance exigé du personnel chargé des tests d’intrusion.

CA-08(01) — Équipe, agente ou agent indépendant chargé des tests d’intrusion (---)

Énoncés :

Faire appel à une équipe, agente ou agent indépendant chargé des tests d’intrusion pour effectuer des tests d’intrusion sur le système ou les composants du système.

Responsable : Aucun

Discussion :

Les équipes ou les agentes et agents indépendants chargés des tests d’intrusion sont des personnes ou des groupes qui effectuent des tests d’intrusion impartiaux sur les systèmes organisationnels. L’impartialité sous-entend que ces équipes ou agentes et agents ne doivent en aucun cas se trouver en un conflit d’intérêts, subjectif ou réel, en ce qui a trait au développement, aux opérations ou à la gestion des systèmes organisationnels qui font l’objet des tests d’intrusion. Le contrôle CA-02(01) fournit d’autres renseignements sur les évaluations indépendantes qui peuvent s’appliquer aux tests d’intrusion.

CA-08(02) — Exercices effectués par l'équipe de testeuses et testeurs (---)

Énoncés :

Avoir recours à des exercices effectués par l'équipe de testeuses et testeurs pour simuler des tentatives de compromission des systèmes organisationnels lancées par des adversaires conformément aux règles d'engagement : [Affectation : exercices effectués par l'équipe de testeuses et testeurs définie par l'organisation].

Responsable : Aucun

Discussion :

Les exercices effectués par l'équipe de testeuses et testeurs vont au-delà des objectifs liés aux tests d'intrusion en permettant d'examiner la posture de sécurité et de protection de la vie privée des organisations et leur capacité à mettre en place des contrôles de cyberdéfense efficaces. Les exercices qu'effectue l'équipe de testeuses et testeurs sont menés de manière à simuler des tentatives lancées par des adversaires qui cherchent à compromettre des fonctions opérationnelles ou liées à la mission de l'organisation afin d'évaluer de façon exhaustive la posture de sécurité et de protection de la vie privée du système et de l'organisation. De telles tentatives comprennent les attaques axées sur la technologie de même que les attaques axées sur l'ingénierie sociale. Les attaques axées sur la technologie comprennent les interactions avec des composants matériels, logiciels ou micrologiciels et avec des processus opérationnels ou liés à la mission. Quant aux attaques axées sur l'ingénierie sociale, elles comprennent les interactions à l'aide de courriels, d'appels téléphoniques, d'espionnage par-dessus l'épaule ou de conversations personnelles. Les exercices effectués par l'équipe de testeuses et testeurs sont plus efficaces lorsqu'ils sont menés par des agentes et agents ou des équipes chargés des tests d'intrusion qui ont des connaissances et de l'expérience des tactiques, des techniques, des procédures et des outils utilisés par les adversaires. Bien que les tests de pénétration se fassent surtout dans des laboratoires, les organisations se servent des exercices qu'effectue l'équipe de testeurs afin de mener des évaluations exhaustives qui reflètent les conditions réelles. Les organisations peuvent utiliser les résultats des exercices effectués par l'équipe de testeuses et testeurs pour améliorer la sensibilisation à la sécurité et à la protection de la vie privée, la formation sur la sécurité et la protection de la vie privée et pour évaluer l'efficacité des contrôles.

CA-08(03) — Tests d'intrusion des installations (---)

Énoncés :

Utiliser un processus de tests d'intrusion qui comprend [Affectation : fréquence définie par l'organisation] tentatives [Sélection (un choix ou plus) : prévues; inopinées] de contournement des contrôles associés aux points d'accès physique de l'installation.

Responsable : Aucun

Discussion :

Des tests d'intrusion de points d'accès physique peuvent fournir de l'information sur des vulnérabilités critiques dans les environnements d'exploitation des systèmes organisationnels. Une telle information peut servir à corriger les faiblesses ou lacunes des contrôles physiques qui sont nécessaires à la protection des systèmes de l'organisation.

CA-09 — Connexions des systèmes internes (---)

Énoncés :

a. Autoriser les connexions internes de [Affectation : composants de système ou types de composants définis par l'organisation] au système
b. Consigner, pour chaque connexion interne, les caractéristiques d'interface, les exigences de sécurité et de protection de la vie privée, et la nature de l'information communiquée
c. Interrompre les connexions des systèmes internes après [Affectation : modalités définies par l'organisation]
d. Examiner [Affectation : fréquence définie par l'organisation] la nécessité de chaque connexion interne

Responsable : Aucun

Discussion :

Les connexions des systèmes internes sont des connexions entre les systèmes organisationnels et des composants constitutifs du système distincts (par exemple, des connexions entre les composants qui font partie d'un même système) y compris les composants utilisés pour le développement des systèmes. Les connexions intrasystèmes comprennent des connexions à des appareils mobiles, à des ordinateurs de bureau ou à des ordinateurs portatifs, à des tablettes, à des imprimantes, à des photocopieurs, à des télécopieurs, à des numériseurs, à des capteurs et à des serveurs. Plutôt que d'autoriser chacune des connexions systèmes internes individuellement, les organisations peuvent autoriser des connexions internes pour un type de composants de systèmes qui ont des caractéristiques ou des configurations communes, y compris les imprimantes, les numériseurs et les photocopieurs numériques ayant une capacité de traitement, de stockage et de transmission précise ou les téléphones intelligents et les tablettes ayant une configuration de référence précise. La nécessité permanente d'avoir des connexions aux systèmes internes est examinée afin d'établir si ces connexions viennent appuyer les fonctions liées à la mission et aux activités de l'organisation.

CA-09(01) — Vérifications de la conformité (---)

Énoncés :

Vérifier la conformité des composants aux exigences de sécurité avant d'établir une connexion interne.

Responsable : Aucun

Discussion :

Les vérifications de conformité aux exigences comprennent la vérification de la configuration de référence pertinente.

CM

Gestion sécurisée des configurations système

Configuration Management

CM-01 — Politique et procédures de gestion des configurations (---)

Énoncés :

a. Développer, consigner et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :

1. une politique de gestion des configurations [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables

2. des procédures pour faciliter la mise en oeuvre des politiques de gestion des configurations et des contrôles de gestion des configurations connexes

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à la gestion des configurations

c. Passer en revue et mettre à jour, par rapport à la gestion des configurations :

1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La politique et les procédures de gestion des configurations abordent les contrôles de la famille CM qui ont été mis en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à l'élaboration de la politique et des procédures de gestion des configurations. En règle générale, les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin pour des politiques et des procédures propres à la mission ou au système. La politique peut être intégrée à la politique générale de sécurité et de protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures de gestion des configurations comprennent, sans s'y limiter, les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, à la jurisprudence, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.

CM-02 — Configuration de référence (Nc--)

Énoncés :

a. Élaborer, consigner et tenir à jour, dans le cadre du contrôle des configurations, une configuration de référence du système
b. Passer en revue et mettre à jour la configuration de référence du système :
1. [Affectation : fréquence définie par l'organisation]
2. le cas échéant, selon [Affectation : circonstances définies par l'organisation]
3. lorsque des composants du système sont installés ou modifiés

Responsable : Aucun

Discussion :

Les configurations de référence pour les systèmes et les composants de systèmes incluent les éléments associés à la connectivité, à l'utilisation et aux communications. Les configurations de référence sont des spécifications des systèmes et des éléments de configuration connexes documentés dont on a convenu et qui font officiellement l'objet d'examens. Les versions, les publications ou les changements à venir concernant les systèmes reposent sur les configurations de référence. Elles comprennent des mises en oeuvre des contrôles de sécurité et de protection de la vie privée, des procédures opérationnelles, de l'information sur les composants de système, la topologie de réseau et la disposition logique des composants au sein de l'architecture du système. La tenue à jour de ces configurations requiert la création de nouvelles bases de référence à mesure que les systèmes organisationnels évoluent. Les configurations de référence des systèmes sont conformes à l'architecture d'entreprise. Si le système facilite la collecte ou l'utilisation de renseignements personnels, les configurations de référence devraient inclure un énoncé de confidentialité fourni aux utilisatrices et utilisateurs.

CM-02(01) — Examens et mises à jour (---)

Énoncés :

Annulé : Intégré au contrôle CM-02.

Responsable : Aucun

CM-02(02) — Automatisation du soutien aux fins d'exactitude et d'actualité (---)

Énoncés :

Assurer l'actualité, le caractère exhaustif, l'exactitude et la disponibilité de la configuration de références pour le système en se servant de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Les outils de gestion des configurations, les outils d'inventaire de logiciels, de matériel et de micrologiciels, et les outils de gestion de réseau sont des mécanismes automatisés qui permettent de maintenir l'uniformité des configurations de référence des systèmes. Des outils d'automatisation peuvent être utilisés au niveau organisationnel, au niveau du processus lié à la mission et aux activités; au niveau du système sur les postes de travail, les serveurs, les ordinateurs blocs-notes, les composants réseau ou les appareils mobiles. Ils peuvent servir à faire le suivi des numéros de version des applications et des types de logiciel installés sur les systèmes d'exploitation de même que des niveaux des correctifs actuels. Les organisations qui choisissent de combiner l'inventaire de composants de système et des activités de configuration de référence peuvent répondre à l'automatisation du soutien aux fins d'exactitude et d'actualité en mettant en place le contrôle CM-08(02).

CM-02(03) — Conservation des configurations antérieures (---)

Énoncés :

Conserver [Affectation : nombre défini par l'organisation] versions de configurations de référence antérieures du système pour permettre le retour à la version précédente.

Responsable : Aucun

Discussion :

La conservation de versions de configurations de référence antérieures du système pour permettre le retour à la version précédente implique de garder le matériel, les logiciels, les micrologiciels, et les fichiers et données de configuration ainsi que les documents connexes.

CM-02(04) — Logiciels non autorisés (---)

Énoncés :

Annulé : Intégré au contrôle CM-07(04).

Responsable : Aucun

CM-02(05) — Logiciels autorisés (---)

Énoncés :

Annulé : Intégré au contrôle CM-07(05).

Responsable : Aucun

CM-02(06) — Environnements de test et de développement (---)

Énoncés :

Conserver pour les environnements de développement et de tests des systèmes une configuration de référence gérée séparément de la configuration de référence opérationnelle.

Responsable : Aucun

Discussion :

L'établissement de configurations de référence distinctes pour les environnements opérationnels, de développement et de tests protège les systèmes contre les événements imprévus liés aux activités de développement et de tests. Les configurations de référence distinctes permettent aux organisations d'adopter la gestion de configuration qui convient le plus à chaque type de configuration. Par exemple, la gestion des configurations pour les environnements opérationnels est axée sur le besoin de stabilité, tandis que la gestion des configurations pour les environnements de développement et de tests requiert une flexibilité accrue. Les configurations utilisées dans un environnement de tests et dans un environnement opérationnel doivent se ressembler dans la mesure du possible afin que les résultats des tests soient représentatifs des changements que l'on propose d'apporter aux systèmes d'exploitation. Les configurations de référence distinctes n'ont pas nécessairement besoin d'environnements physiques séparés.

CM-02(07) — Configuration des systèmes et des composants pour des zones à risque élevé (---)

Énoncés :

a. Remettre [Affectation : systèmes, composants de système désignés par l'organisation] dotés de [Affectation : configurations définies par l'organisation] aux personnes qui se rendent dans des endroits que l'organisation juge très risqués
b. Appliquer les contrôles suivants aux systèmes ou aux composants de systèmes lorsque les personnes reviennent de voyage : [Affectation : contrôles définis par l'organisation]

Responsable : Aucun

Discussion :

Lorsque l'on sait que des systèmes ou des composants de systèmes se retrouveront dans des secteurs à risque élevé extérieurs à l'organisation, il est possible de mettre en place des contrôles supplémentaires pour contrer la menace accrue associée à ces endroits. Par exemple, les organisations peuvent prendre des mesures pour les ordinateurs blocs-notes qu'utilisent les personnes qui partent en voyage et qui en reviennent. Les mesures comprennent de déterminer les lieux préoccupants, de définir les configurations requises pour les composants, de s'assurer que les composants sont configurés adéquatement avant le voyage et d'appliquer des contrôles aux composants au retour du voyage. Les ordinateurs blocs-notes spécialement configurés comprennent les ordinateurs dont le disque dur a été nettoyé, qui sont dotés d'un nombre limité d'applications et de paramètres de configuration plus stricts. Les contrôles appliqués aux appareils mobiles au retour du voyage comprennent un examen de l'appareil mobile afin de détecter des signes physiques de tentatives de modification, le nettoyage de la mémoire ou la recréation de l'image des lecteurs de disque. La protection de l'information contenue dans les appareils mobiles est traitée dans la famille Protection des supports (MP pour Media Protection).

CM-03 — Contrôle des changements de configuration (---)

Énoncés :

a. Déterminer et consigner les types de changements apportés au système qui sont contrôlés par la configuration
b. Examiner les changements proposés au système qui sont contrôlés par la configuration et les approuver ou les refuser en tenant compte explicitement des répercussions sur la sécurité et la protection de la vie privée
c. Consigner les décisions liées aux changements de configuration du système
d. Mettre en oeuvre les changements approuvés au système qui sont contrôlés par la configuration
e. Conserver les dossiers sur les changements contrôlés par la configuration du système pendant [Affectation : délais définis par l'organisation]
f. Surveiller et examiner les activités associées aux changements contrôlés par la configuration visant le système
g. Coordonner et surveiller les activités de contrôle des changements de configuration effectuées par [Affectation : élément de contrôle des changements de configuration défini par l'organisation] qui se réunit [Sélection (un choix ou plus) : {Affectation : fréquence définie par l'organisation}; lorsque {Affectation : conditions de changement de configuration définies par l'organisation}]

Responsable : Aucun

Discussion :

Le contrôle des changements apportés à la configuration des systèmes organisationnels comprend la proposition systématique, la justification, la mise en oeuvre, les tests, l'examen et l'application de changements aux systèmes, y compris leurs mises à niveau et leurs modifications. Le contrôle des changements apportés à la configuration comprend les changements liés aux configurations de référence, les éléments de configuration des systèmes, les procédures opérationnelles, les paramètres de configuration pour les composants du système, les vulnérabilités atténuées et les changements non prévus ou non autorisés. Les processus liés à la gestion des changements apportés à la configuration des systèmes comprennent les conseils de gestion des configurations ou les comités consultatifs sur les changements qui examinent et approuvent les changements proposés. Pour les nouveaux systèmes ou les mises à jour majeures, les organisations considèrent d'inclure des représentantes et représentants des organisations de développement aux conseils de gestion des configurations ou aux comités consultatifs sur les changements. La vérification des changements comprend les activités qui ont eu lieu avant ou qui auront lieu après que les changements soient apportés aux systèmes et que les activités de vérification nécessaires appliquent ces changements. Prière de consulter le contrôle SA-10.

CM-03(01) — Automatisation concernant la documentation, les avis et les interdictions de changements (---)

Énoncés :

Utiliser des [Affectation : mécanismes automatisés définis par l'organisation] pour :
a. consigner les changements proposés au système
b. aviser [Affectation : autorités d'approbation définies par l'organisation] des changements proposés au système et des demandes de changement approuvées
c. souligner les changements proposés au système qui n'ont pas été approuvés ou qui ont été jugés défavorables avant [Affectation : délais définis par l'organisation]
d. interdire tout changement au système jusqu'à l'obtention des approbations requises
e. documenter tous les changements proposés au système
f. aviser [Affectation : liste des employées et employés définie par l'organisation] des changements au système approuvés

Responsable : Aucun

CM-03(02) — Tests, validation et documentation des changements (---)

Énoncés :

Tester, valider et consigner les changements au système avant de les mettre en oeuvre dans le système.

Responsable : Aucun

Discussion :

Les changements aux systèmes englobent les modifications aux composants matériels, logiciels ou micrologiciels ainsi qu'aux paramètres de configuration définis dans le contrôle CM-

06. Les organisations veillent à ce que les tests n'interfèrent pas avec les opérations du système. Les personnes ou les groupes chargés des tests comprennent les stratégies et les procédures de sécurité et de protection de la vie privée, les stratégies et les procédures de sécurité et de protection de la vie privée liées au système et les risques propres à la santé, à la sécurité et à l'environnement qui sont associés à certaines installations ou à certains processus. Il peut arriver que l'on doive mettre hors ligne des systèmes d'exploitation, ou les reproduire autant que possible, avant de pouvoir effectuer des tests. Si les systèmes doivent être mis hors ligne, il faut que ce soit durant une période d'interruption prévue, dans la mesure du possible. S'il est impossible de mener des tests sur les systèmes d'exploitation, les organisations doivent utiliser des contrôles de compensation.

CM-03(03) — Mise en oeuvre automatisée des changements (---)

Énoncés :

Apporter des changements au système de référence actuel et les déployer ensuite dans tout le système au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Des outils automatisés peuvent accroître l'exactitude, la cohérence et la disponibilité de l'information de référence sur la configuration. L'automatisation peut aussi fournir des capacités en matière d'agrégation et de corrélation de données, des mécanismes d'alerte et des tableaux de bord pour soutenir la prise de décisions fondée sur le risque au sein de l'organisation.

CM-03(04) — Représentantes et représentants de la sécurité et de la protection de la vie privée (---)

Énoncés :

Exiger [Affectation : qu'une représentante ou un représentant de la sécurité et de la protection de la vie privée défini par l'organisation] soit membre de [Affectation : élément de contrôle des changements de configuration défini par l'organisation].

Responsable : Aucun

Discussion :

Les représentantes et représentants en matière de sécurité et de protection de la vie privée de l'information comprennent les responsables de la sécurité des systèmes, les cadres supérieures et supérieurs de la gouvernance en matière de sécurité du ministère, les gardiennes et gardiens de la sécurité ou les hautes et hauts fonctionnaires ou cadres supérieures et supérieurs en matière de protection de la vie privée. Il est important d'avoir parmi le personnel des représentantes et représentants qui sont dotés d'une expertise en sécurité de l'information, car les changements aux configurations des systèmes peuvent avoir des répercussions imprévues, dont certaines pouvant avoir trait à la sécurité ou à la protection de la vie privée. La détection rapide de ces changements permet d'éviter des conséquences négatives inattendues qui pourraient avoir des conséquences sur l'état de sécurité et de protection de la vie privée des systèmes. L'élément de contrôle des changements de configuration dont il est question dans le second paramètre défini par l'organisation reflète ceux définis par l'organisation dans le contrôle CM-03G.

CM-03(05) — Mesures de sécurité automatisées (---)

Énoncés :

Mettre automatiquement en place les mesures de sécurité suivantes lorsque des configurations de référence sont modifiées sans autorisation : [Affectation : mesures de sécurité définies par l'organisation].

Responsable : Aucun

Discussion :

Les mesures de sécurité automatisées comprennent l'interruption du traitement du système et de certaines fonctions du système ou la publication d'avis ou d'alertes à l'intention du personnel de l'organisation lorsqu'un élément de configuration est modifié sans autorisation.

CM-03(06) — Gestion de la cryptographie (---)

Énoncés :

S'assurer que les mécanismes cryptographiques utilisés pour fournir les contrôles suivants soient intégrés à la gestion des configurations : [Affectation : contrôles définis par l'organisation].

Responsable : Aucun

Discussion :

Les contrôles mentionnés dans l'amélioration du contrôle font référence aux contrôles de sécurité et de protection de la vie privée tirés du catalogue des contrôles. Peu importe les mécanismes cryptographiques employés, des processus et des procédures sont en place pour gérer ceux-ci. Par exemple, si des composants de systèmes utilisent des certificats aux fins d'identification et d'authentification, il faut mettre en place un processus pour prendre des mesures concernant l'expiration de ces certificats.

CM-03(07) — Examen des changements apportés au système (---)

Énoncés :

Passer en revue les changements apportés au système [Affectation : fréquence définie par l'organisation] et [Affectation : circonstances définies par l'organisation] pour déterminer si des changements non autorisés ont été apportés.

Responsable : Aucun

Discussion :

Des indications qui justifient l'examen des changements au système et les circonstances précises qui justifient ce besoin peuvent découler d'activités menées par des organisations durant le processus de changement de configuration ou le processus de surveillance continue. Pour les systèmes qui facilitent la collecte ou l'utilisation de renseignements personnels, des changements importants apportés au système quant au processus opérationnel ou à la logique applicative peuvent donner lieu à l'exigence relative à une EFVP.

CM-03(08) — Empêcher ou limiter les changements de configuration (---)

Énoncés :

Empêcher ou limiter les changements à la configuration du système dans les situations suivantes : [Affectation : circonstances définies par l'organisation].

Responsable : Aucun

Discussion :

Les changements apportés à la configuration du système peuvent nuire aux fonctions de sécurité et de protection de la vie privée des systèmes essentiels. Les restrictions liées aux changements peuvent être appliquées au moyen de mécanismes automatisés.

CM-04 — Analyses des répercussions (---)

Énoncés :

Analyser les changements visant le système pour déterminer les répercussions possibles sur la sécurité et la protection de la vie privée avant leur mise en oeuvre.

Responsable : Aucun

Discussion :

Le personnel de l'organisation qui assume des responsabilités liées à la sécurité et à la protection de la vie privée procède aux analyses des répercussions. Ces personnes possèdent les compétences et l'expertise technique nécessaires pour analyser les changements apportés aux systèmes et leurs ramifications sur le plan de la sécurité et de la protection de la vie privée. Les analyses des répercussions comprennent les éléments suivants : examiner les plans, les stratégies et les procédures de sécurité et de protection de la vie privée afin de comprendre les exigences en matière de contrôle; examiner la documentation de conception et les procédures opérationnelles du système afin de comprendre la mise en oeuvre des contrôles et les répercussions qu'ils pourraient avoir sur les changements apportés au système; examiner les répercussions que peuvent entraîner les changements de partenaires de la chaîne d'approvisionnement sur les parties prenantes; et déterminer la manière dont les changements potentiels apportés au système peuvent créer de nouveaux risques pour la vie privée des personnes. Les analyses des répercussions peuvent également comprendre les évaluations des risques visant à bien saisir l'incidence des changements et à déterminer si des contrôles de sécurité supplémentaires sont requis. La réalisation d'une EFVP permet de vérifier la conformité des mesures de protection de la vie privée en faisant appel aux principes de traitement équitable de l'information afin de déterminer en quoi les changements potentiels apportés au système peuvent créer de nouveaux risques pour la vie privée des personnes et la capacité des contrôles mis en oeuvre d'atténuer ces risques.

CM-04(01) — Environnements de test distincts (---)

Énoncés :

Analyser les changements apportés au système dans un environnement de test distinct avant de les appliquer dans un environnement opérationnel afin de déceler toute lacune, faiblesse, incompatibilité ou intention malveillante susceptible d'influer sur la sécurité et la protection de la vie privée.

Responsable : Aucun

Discussion :

Un environnement de test distinct doit être physiquement et logiquement séparé et distinct de l'environnement opérationnel. La séparation suffit à faire en sorte que les activités menées dans l'environnement de test n'influent aucunement sur les activités effectuées dans l'environnement opérationnel, et l'information se trouvant dans l'environnement opérationnel n'est pas transmise à l'environnement de test par inadvertance. Il est possible de distinguer les environnements de façon physique ou logique. Lorsque les environnements de tests séparés physiquement ne sont pas appliqués, les organisations déterminent la force du mécanisme qui est requise lorsqu'elles appliquent la séparation de façon logique.

CM-04(02) — Vérification des contrôles (---)

Énoncés :

Après les changements apportés au système, s'assurer que les contrôles ont été mis en oeuvre correctement, qu'ils fonctionnent comme prévu et qu'ils produisent les résultats escomptés tout en respectant les exigences relatives à la sécurité et à la protection de la vie privée du système.

Responsable : Aucun

Discussion :

Dans ce contexte, on entend par mise en oeuvre l'installation du code modifié dans le système opérationnel pouvant avoir une incidence sur les contrôles de sécurité et de protection de la vie privée.

CM-05 — Restrictions d’accès associées aux changements (---)

Énoncés :

Définir, documenter, approuver et appliquer les restrictions d’accès physiques et logiques associées aux changements apportés au système.

Responsable : Aucun

Discussion :

Les changements apportés aux composants matériels, logiciels ou micrologiciels des systèmes ou aux procédures opérationnelles associées au système peuvent avoir des répercussions importantes sur la sécurité du système ou la vie privée des personnes. Les organisations doivent donc accorder l’accès aux systèmes seulement aux personnes qualifiées et autorisées et seulement pour effectuer les changements. Les restrictions d’accès incluent les contrôles d’accès physiques et logiques (voir AC-03 et PE-03), les bibliothèques de logiciels, l’automatisation de flux de travaux, les médiathèques, les couches abstraites (c’est-à-dire les changements mis en oeuvre dans les interfaces externes plutôt que directement dans les systèmes) et les fenêtres de changement (c’est-à-dire les changements sont appliqués seulement à des moments précis).

CM-05(01) — Enregistrements de vérification et d'application des restrictions d'accès automatisées (---)

Énoncés :

a. Appliquer les restrictions d'accès à l'aide de [Affectation : mécanismes automatisés définis par l'organisation]
b. Générer automatiquement des enregistrements de vérification des mesures appliquées

Responsable : Aucun

Discussion :

Les organisations assurent la journalisation des accès au système associés à l'application des changements de configuration pour s'assurer que le contrôle de ces changements est en place et pour appuyer les interventions après coup dans l'éventualité où les organisations détecteraient un changement non autorisé au système.

CM-05(02) — Examen des changements apportés au système (---)

Énoncés :

Annulé : Intégré au contrôle CM-03(07).

Responsable : Aucun

CM-05(03) — Composants signés (---)

Énoncés :

Annulé : Transféré sous le contrôle CM-14.

Responsable : Aucun

CM-05(04) — Double autorisation (---)

Énoncés :

Appliquer le principe d'autorisation double avant d'apporter des changements à [Affectation : information système et composants du système définis par l'organisation].

Responsable : Aucun

Discussion :

Les organisations ont recours au principe d'autorisation double pour veiller à ce qu'aucun changement ne soit apporté à certains composants de système et aux données système à moins que deux personnes qualifiées mettent en oeuvre les changements voulus. Ces deux personnes doivent posséder les compétences et l'expertise pour déterminer si les changements proposés représentent des applications adéquates des changements approuvés. Les personnes sont également imputables des changements. La double autorisation est également appelée le contrôle par deux personnes. Pour réduire le risque de collusion, les organisations considèrent la rotation des tâches à double autorisation avec d'autres particuliers. L'information au niveau du système comprend les procédures opérationnelles.

CM-05(05) — Limite des privilèges pour la production et l'opération (---)

Énoncés :

a. Limiter les privilèges relatifs à la modification des composantes du système ainsi que de l'information relative au système dans un environnement opérationnel ou de production
b. Examiner et réévaluer les privilèges [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

Dans bon nombre d'organisations, les systèmes appuient plusieurs fonctions essentielles liées à la mission et aux activités de l'organisation. Il faut limiter les privilèges liés aux changements à apporter aux composants de système des systèmes d'exploitation, car le fait d'apporter des changements à un composant de système peut avoir de graves conséquences sur les processus liés à la mission et aux activités que prend en charge le système. Parfois, les développeuses et développeurs ne connaissent pas les liens qui existent entre les systèmes et les processus liés à la mission et aux activités de l'organisation. L'information liée au système comprend les procédures opérationnelles.

CM-05(06) — Privilèges de bibliothèque limités (---)

Énoncés :

Limiter les privilèges permettant de changer les logiciels résidants de la bibliothèque de logiciels.

Responsable : Aucun

Discussion :

Les bibliothèques de logiciels comportent des programmes privilégiés.

CM-05(07) — Automatisation de la mise en oeuvre de mécanismes de sécurité (---)

Énoncés :

Annulé : Intégré au contrôle SI-07.

Responsable : Aucun

CM-06 — Paramètres de configuration (---)

Énoncés :

a. Établir et documenter les paramètres de configuration des composants employés dans le système qui cadrent avec le mode le plus rigoureux sur le plan des exigences opérationnelles à l'aide de [Affectation : configurations sécurisées communes définies par l'organisation]
b. Mettre en oeuvre les paramètres de configuration
c. Déterminer, documenter et approuver tout écart en ce qui a trait aux paramètres de configuration établis pour [Affectation : composants de système définis par l'organisation] en tenant compte de [Affectation : exigences opérationnelles définies par l'organisation]
d. Surveiller et contrôler les changements apportés aux paramètres de configuration conformément à ses stratégies et procédures

Responsable : Aucun

Discussion :

Les paramètres de configuration représentent les paramètres pouvant être modifiés dans les composants matériels, logiciels ou micrologiciels du système et qui affectent la posture de sécurité ou de protection de la vie privée ou encore le fonctionnement du système. Les produits de technologie de l'information pour lesquels il est possible de définir les paramètres de configuration comptent les ordinateurs centraux, les serveurs, les postes de travail, les systèmes d'exploitation, les appareils mobiles, les périphériques d'entrée et de sortie, les protocoles et les applications. Les paramètres qui ont une incidence sur la posture de sécurité des systèmes comprennent les paramètres de registre, les paramètres d'autorisation pour les comptes, les fichiers et les répertoires et les paramètres pour les fonctions, les ports, les services et les connexions distantes. Les paramètres de protection de la vie privée sont les paramètres qui ont une incidence sur la posture de protection de la vie privée des systèmes, y compris les paramètres nécessaires pour répondre à d'autres contrôles de protection de la vie privée. Les paramètres de protection de la vie privée incluent les exigences liées au contrôle d'accès, aux renseignements personnels, à la précision des données, aux capacités de manipulation des données, aux préférences de traitement des données et aux permissions de traitement et de rétention de l'information. Les organisations doivent établir des paramètres de configuration à l'échelle de l'organisation et par la suite des paramètres de configuration particuliers pour les systèmes. Les paramètres établis deviennent des éléments de la base de référence de la configuration pour le système. Les configurations sécurisées communes (que l'on appelle également les listes de vérification concernant la configuration de sécurité, les guides de confinement et de renforcement, et les guides de référence pour la sécurité) fournissent des points de repère reconnus, normalisés et établis qui stipulent les paramètres de configuration sécurisée associés à des plateformes ou à des produits de technologies de l'information ainsi que des instructions pour la configuration de ces produits afin de répondre aux exigences opérationnelles. Diverses organisations peuvent développer des configurations sécurisées communes, y compris les développeuses et développeurs de produits TI, les fabricants, les fournisseurs, les organismes gouvernementaux, les consortiums, le milieu universitaire, l'industrie ainsi que d'autres organisations des secteurs public et privé. La mise en oeuvre de configurations sécurisées communes peut être demandée au niveau organisationnel, au niveau du processus lié à la mission et aux activités; au niveau du système, ou à un niveau supérieur, y compris par un organisme de réglementation. Les configurations sécurisées communes comprennent les exigences de base en matière de sécurité pour les zones de sécurité de réseau (ITSP.80.022), les Common Criteria Evaluated Configuration Guides (en anglais), et les Security Technical Implementation Guides (STIG) du Department of Defense (DoD) des États-Unis, qui touchent la mise en oeuvre du contrôle CM-06 ainsi que d'autres contrôles comme AC-19 et CM-

07. Le protocole SCAP (pour Security Content Automation Protocol) et les normes qu'il définit offrent une méthode efficace et unique d'identification, de suivi et de contrôle des paramètres de configuration.

CM-06(01) — Gestion, application et vérification automatisées (Nc--)

Énoncés :

Gérer, appliquer et vérifier les paramètres de configuration pour [Affectation : composants de systèmes définis par l'organisation] au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Des outils automatisés (par exemple, outils de renforcement, outils de configuration de base) peuvent accroître l'exactitude, la cohérence et la disponibilité de l'information des paramètres de configuration. L'automatisation peut aussi fournir des capacités en matière de regroupement de données et de corrélation de données, des mécanismes d'alerte et des tableaux de bord pour soutenir la prise de décisions fondée sur le risque au sein de l'organisation.

CM-06(02) — Intervention lorsque des changements non autorisés sont apportés (Nc--)

Énoncés :

Prendre les mesures suivantes pour intervenir lorsque des changements non autorisés sont apportés aux [Affectation : paramètres de configuration définis par l'organisation] : [Affectation : actions définies par l'organisation].

Responsable : Aucun

Discussion :

Les interventions en cas de changement non autorisé des paramètres de configuration comprennent le signalement au personnel désigné par l'organisation, la restauration des paramètres de configuration établis ou, dans des cas extrêmes, l'interruption du traitement du système en cause.

CM-06(03) — Détection de changement non autorisé (---)

Énoncés :

Annulé : Intégré au contrôle SI-07.

Responsable : Aucun

CM-06(04) — Démonstration de conformité (---)

Énoncés :

Annulé : Intégré au contrôle CM-04.

Responsable : Aucun

CM-07 — Fonctionnalité minimale (---)

Énoncés :

a. Configurer le système pour fournir uniquement des [Affectation : capacités essentielles à la mission définies par l'organisation]
b. Interdire ou restreindre l'utilisation des fonctions, des ports, des protocoles, des logiciels et des services suivants : [Affectation : fonctions, ports, protocoles, logiciels ou services du système interdits ou restreints définis par l'organisation]

Responsable : Aucun

Discussion :

Les systèmes peuvent offrir une grande variété de fonctions et de services. Il se peut que certaines des fonctions et certains des services fournis régulièrement par défaut ne soient pas nécessaires pour appuyer la mission, les fonctions ou les opérations essentielles de l'organisation. Il est en outre parfois utile d'offrir plusieurs services à partir d'un composant de système unique. Or, cette façon de faire représente un risque accru comparativement au fait de limiter les services fournis par ce seul composant. Dans la mesure du possible, les organisations doivent limiter la fonctionnalité des composants à une seule fonction par composant. Les organisations doivent envisager de désactiver les protocoles et les ports physiques et logiques inutilisés ou qui ne sont pas nécessaires afin d'empêcher les connexions non autorisées des composants, les transferts d'information et la tunnellisation. Elles ont recours à des outils d'analyse de réseau, à des systèmes de détection et de prévention d'intrusions et à des technologies de protection de point terminal (pare-feu, systèmes de détection d'intrusions intégré, etc.) pour identifier les fonctions, les protocoles, les ports et les services interdits et en empêcher l'utilisation. Une fonctionnalité minimale peut aussi être atteinte dans le cadre de la conception et de l'élaboration fondamentales du système (voir les contrôles SA-08, SC-02 et SC-03). Pour ce qui est du concept de la fonctionnalité minimale, il faut s'efforcer de limiter le volume de renseignements personnels à ce que le système exige pour ainsi réduire les répercussions advenant une violation.

CM-07(01) — Examen périodique (---)

Énoncés :

a. Examiner le système tous les [Affectation : fréquence définie par l'organisation] afin d'établir les fonctions, les ports, les protocoles, les logiciels et les services non nécessaires
b. Désactiver ou retirer [Affectation : fonctions, ports, protocoles et services du système jugés inutiles ou non sécurisés définis par l'organisation]

Responsable : Aucun

Discussion :

Les organisations doivent examiner les fonctions, les ports, les protocoles et les services fournis par le système ou les composants de systèmes afin de déterminer ceux qui peuvent être éliminés. Ces examens sont particulièrement importants lors de la période de transition pour passer des anciennes technologies aux nouvelles technologies (par exemple, le passage des protocoles IPv4 à IPv6). Ces transitions de technologiques peuvent nécessiter de mettre en oeuvre de manière simultanée les anciennes et les nouvelles technologies pendant la période de transition et de retourner à des fonctions, à des ports, à des protocoles et à des services essentiels minimums dans les meilleurs délais. Les organisations peuvent déterminer la sécurité relative de la fonction, du port, du protocole ou du service ou baser sa décision en matière de sécurité sur l'évaluation d'autres entités. Les services Bluetooth, FTP et pair à pair sont des exemples de protocoles non sécurisés.

CM-07(02) — Prévention de l'exécution des programmes (---)

Énoncés :

Empêcher l'exécution des programmes conformément à [Sélection (un choix ou plus) : {Affectation : stratégies, règles de conduite et ententes d'accès sur l'utilisation de programmes informatiques et restrictions connexes définies par l'organisation}; règles d'autorisation des modalités d'utilisation d'un programme informatique].

Responsable : Aucun

Discussion :

La prévention de l'exécution des programmes définit les stratégies, les règles de conduite ou les ententes d'accès de l'organisation qui limitent l'utilisation des logiciels et les conditions générales d'utilisation imposées par le développeur ou le fabricant, y compris l'octroi de licences de logiciel et les droits d'auteur. Les restrictions impliquent d'empêcher l'auto-exécution de fonctionnalités, de restreindre les rôles autorisés pour l'approbation de l'exécution des programmes, d'autoriser ou d'interdire des programmes informatiques précis, ou de restreindre le nombre d'instances de programmes exécutés simultanément.

CM-07(03) — Conformité aux exigences d’enregistrement (---)

Énoncés :

Assurer la conformité avec [Affectation : exigences d’enregistrement définies par l’organisation pour des fonctions, des ports, des protocoles et des services].

Responsable : Aucun

Discussion :

Les organisations utilisent le processus d’enregistrement pour gérer, faire le suivi et surveiller les systèmes et les fonctions, les ports, les protocoles et les services mis en oeuvre.

CM-07(04) — Logiciel non autorisé – Interdire par exception (---)

Énoncés :

a. Identifier les [Affectation : programmes informatiques ne pouvant pas être exécutés sur le système définis par l'organisation]
b. Recourir à une stratégie tout permettre, interdire par exception pour empêcher l'exécution des programmes informatiques non autorisés sur le système
c. Passer en revue et mettre à jour la liste des programmes informatiques autorisés tous les [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

Les programmes informatiques non autorisés peuvent être limités à des versions ou à des sources particulières. Le concept visant à interdire l'exécution de logiciels non autorisés pourrait également s'appliquer à des actions propres aux utilisatrices et utilisateurs, à des ports et protocoles de système, à des adresses IP ou à des plages d'adresses IP, à des sites Web et à des adresses MAC.

CM-07(05) — Logiciels autorisés – Autorisation par exception (---)

Énoncés :

a. Identifier les [Affectation : programmes informatiques pouvant être exécutés sur le système définis par l'organisation]
b. Recourir à une stratégie tout interdire, autoriser par exception pour permettre l'exécution des programmes informatiques autorisés sur le système
c. Passer en revue et mettre à jour la liste des programmes informatiques autorisés tous les [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

Les programmes informatiques autorisés peuvent être limités à des versions ou à des sources particulières. Afin de favoriser un processus complet de gestion des logiciels autorisés et de renforcer la protection contre les attaques qui contournent les logiciels autorisés au niveau de l'application, les programmes informatiques peuvent être décomposés en différents niveaux de détail et surveillés. Ces niveaux incluent les applications, les interfaces de programmation d'applications (API pour Application Programming Interface), les modules d'application, les scripts, les processus système, les services système, les fonctions noyau, les registres, les pilotes et les bibliothèques de liens dynamiques. Le concept visant à autoriser l'exécution de logiciels autorisés pourrait également s'appliquer à des actions propres aux utilisatrices et utilisateurs, à des ports et protocoles de système, à des adresses IP ou à des plages d'adresses IP, à des sites Web et à des adresses MAC. Les organisations doivent envisager de vérifier l'intégrité des programmes informatiques autorisés à l'aide de signatures numériques, de totaux de contrôle cryptographique ou de fonctions de hachage. La vérification des logiciels peut s'effectuer avant l'exécution du système ou au démarrage du système. L'identification d'adresses URL autorisées pour des sites Web est abordée dans les contrôles CA-03(05) et SC-07.

CM-07(06) — Environnements clos aux privilèges restreints (---)

Énoncés :

Exiger que les logiciels installés par l'utilisatrice ou utilisateur désignés soient exécutés dans un environnement physique clos ou un environnement clos de machine virtuelle dont les privilèges sont restreints :[Affectation : logiciels installés par les utilisatrices ou utilisateurs désignés par l'organisation].

Responsable : Aucun

Discussion :

Les organisations déterminent quels sont les logiciels dont la provenance est une source de préoccupations ou qui pourraient contenir du code malveillant. Pour ce type de logiciel, l'installation par l'utilisatrice ou utilisateur a lieu dans un environnement opérationnel clos pour limiter ou contenir les dommages des programmes malveillants qui pourraient être exécutés.

CM-07(07) — Exécution de code dans des environnements protégés (---)

Énoncés :

Permettre l'exécution de code binaire ou exécutable sur machine uniquement dans un environnement physique clos ou dans un environnement clos de machine virtuelle avec l'approbation explicite de [Affectation : personnel ou rôles définis par l'organisation] lorsqu'un tel code :
a. provient de sources qui n'offrent pas de garantie ou qui offrent une garantie limitée
b. dans les cas où ils n'offrent pas le code source

Responsable : Aucun

Discussion :

L'exécution de code dans des environnements protégés s'applique à toutes les sources de code binaire ou exécutable sur machine, notamment, les logiciels et micrologiciels commerciaux et les logiciels de source ouverte.

CM-07(08) — Code binaire ou exécutable sur machine (---)

Énoncés :

a. Interdire l'utilisation de code binaire ou exécutable sur machine provenant de sources qui n'offrent pas de garantie ou qui offrent une garantie limitée dans les cas où il n'y a pas de code source
b. Permettre des exceptions uniquement dans situations urgentes liées à la mission ou aux besoins opérationnels et avec le consentement écrit exprès de l'autorité responsable

Responsable : Aucun

Discussion :

Le code binaire ou exécutable sur machine s'applique à toutes les sources de code binaire ou exécutable sur machine, notamment, les logiciels et micrologiciels commerciaux et les logiciels de source ouverte. Les produits logiciels sans code source ou provenant de fournisseurs qui n'offrent pas de garantie ou qui offrent une garantie limitée, sont évalués sur le plan de leurs répercussions potentielles sur la sécurité. Les évaluations tiennent compte du fait que ces produits logiciels sont difficiles à examiner, à réparer ou à développer. De plus, il pourrait n'y avoir aucune ou aucun propriétaire en mesure d'effectuer ces réparations au nom de l'organisation. Si des logiciels de source ouverte sont utilisés, les évaluations tiennent compte du fait qu'il n'y a pas de garantie, que les logiciels de source ouverte pourraient contenir des portes dérobées ou des maliciels, et qu'il pourrait ne pas y avoir de soutien offert.

CM-07(09) — Empêcher l'utilisation de composants matériels non autorisés (---)

Énoncés :

a. Identifier [Affectation : composants matériels autorisés définis par l'organisation pour l'utilisation du système]
b. Empêcher l'utilisation ou la connexion de composants matériels non autorisés
c. Passer en revue et mettre à jour la liste des composants matériels autorisés tous les [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

Les composants matériels fournissent la base pour les systèmes de l'organisation et la plateforme permettant l'exécution des programmes informatiques. Gérer l'inventaire des composants matériels et contrôler les composants matériels qui sont autorisés à être installés ou connectés aux systèmes de l'organisation est essentiel pour assurer une sécurité adéquate.

CM-08 — Inventaire des composants de système (Nc--)

Énoncés :

a. Élaborer et documenter un inventaire des composants de systèmes qui :
- **1.** illustre exactement le système
- **2.** comprend tous les composants dans le système
- **3.** ne comprend aucune comptabilisation en double des composants ou des composants attribués à un autre système
- **4.** est au niveau de granularité jugé nécessaire aux fins de suivi et de production de rapports
- **5.** comprend l'information suivante pour assurer la comptabilisation des composants de systèmes : [Affectation : information définie par l'organisation et jugée nécessaire à la comptabilisation efficace des composants de système]

b. Passer en revue et mettre à jour l'inventaire des composants du système tous les [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

Les composants des systèmes sont des biens de TI discrets et identifiables qui comprennent le matériel, les logiciels et les micrologiciels. Les organisations peuvent choisir de mettre en place des inventaires de composants des systèmes centralisés qui contiennent les composants de tous les systèmes organisationnels. Dans de telles situations, les organisations doivent s'assurer que les inventaires comportent de l'information propre au système requise pour la comptabilisation des composants. L'information nécessaire pour une comptabilisation efficace des composants du système comprend le nom du système, les propriétaires des logiciels, les numéros de version des logiciels, les spécifications de l'inventaire du matériel, l'information sur les licences de logiciels, les composants réseau, les noms des machines et les adresses réseau pour tous les protocoles mis en oeuvre (par exemple, IPv4 et IPv6). Les spécifications de l'inventaire comprennent la date de réception, le coût, le modèle, le numéro de série, le fabricant, les données sur le fournisseur, le type de composant et l'emplacement physique. Prévenir la comptabilisation en double des composants d'un système permet de remédier au manque de comptabilisation qui se produit lorsque la propriété des composants et l'association au système ne sont pas connues, plus particulièrement dans des vastes ou complexes systèmes connectés. Une prévention efficace de la comptabilisation en double des composants d'un système nécessite le recours à un identifiant unique pour chaque composant. Pour l'inventaire des logiciels, les logiciels gérés de manière centralisée et dont l'accès se fait par d'autres systèmes sont traités comme un composant du système sur lequel il est installé et géré. Les logiciels installés sur plusieurs systèmes organisationnels et gérés au niveau du système sont traités pour chaque système individuel et ils peuvent apparaître plus d'une fois dans un inventaire centralisé de composants, ce qui nécessite une association au système pour chaque instance logicielle dans l'inventaire centralisé pour éviter une comptabilisation en double des composants. Analyser des systèmes qui mettent en oeuvre plusieurs protocoles réseau (par exemple, IPv4 et IPv6) peut faire en sorte que des composants en double peuvent être répertoriés dans différents espaces d'adresses. La mise en oeuvre du contrôle CM-08(07) peut aider à éliminer la comptabilisation en double de composants.

CM-08(01) — Mises à jour durant l'installation et le retrait (---)

Énoncés :

Faire de la mise à jour de l'inventaire des composantes du système une étape de l'installation ou du retrait de composantes ainsi que de la mise à jour du système.

Responsable : Aucun

Discussion :

Les organisations peuvent accroître l'exactitude, le caractère exhaustif, la cohérence des inventaires de composants des systèmes si les inventaires sont mis à jour dans le cadre de l'installation ou du retrait de composantes ainsi que de la mise à jour du système. Si les inventaires ne sont pas mis à jour à des périodes clés, il est fort probable que l'information ne sera pas correctement saisie et consignée. Les mises à jour de systèmes touchent les composants matériels, logiciels et micrologiciels.

CM-08(02) — Automatisation de la maintenance (---)

Énoncés :

Assurer l'actualité, le caractère exhaustif, l'exactitude et la disponibilité de l'inventaire des composants du système au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Dans la mesure du possible, les organisations tiennent à jour les inventaires des systèmes. Par exemple, il peut s'avérer difficile de surveiller les machines virtuelles, car elles sont invisibles dans le réseau lorsqu'elles ne sont pas utilisées. Dans ces situations, les organisations tiennent le plus possible l'inventaire raisonnablement à jour, complet et exact. L'automatisation de la maintenance peut être réalisée en mettant en place le contrôle CM-02(02) pour les organisations qui choisissent de combiner l'inventaire de composants de système et des activités de configuration de référence.

CM-08(03) — Détection automatisée de composants non autorisés (---)

Énoncés :

a. Détecter la présence de composants matériels, logiciels et micrologiciels non autorisés dans le système au moyen de [Affectation : mécanismes automatisés définis par l'organisation] [Affectation : fréquence définie par l'organisation]
b. Prendre les mesures suivantes lorsque des composants non autorisés sont détectés : [Sélection (un choix ou plus) : désactiver l'accès réseau de ces composants; isoler les composants; aviser {Affectation : personnel ou rôles définis par l'organisation}]

Responsable : Aucun

Discussion :

La détection automatisée de composants non autorisés est appliquée en plus de surveiller les connexions à distance et les appareils mobiles non autorisés. La surveillance des composants de systèmes non autorisés peut être effectuée de façon continue ou lors d'analyses périodiques des systèmes menées à cette fin. Les mécanismes automatisés peuvent également être utilisés de façon à empêcher la connexion de composants non autorisés (voir le contrôle CM-07(09)). Des mécanismes automatisés peuvent être mis en place dans les systèmes ou dans des composants de système distincts. Lors de l'acquisition et de la mise en oeuvre de mécanismes automatisés, les organisations doivent déterminer si de tels mécanismes dépendent de la capacité des composants du système à prendre en charge un agent ou du programme demandeur à détecter étant donné que certains composants n'ont pas d'agents ou ne peuvent pas en prendre en charge (par exemple, des dispositifs de l'Internet des objets ou des capteurs). On peut isoler les composants de système non autorisés en les plaçant dans des domaines ou des sous-réseaux séparés ou en les mettant en quarantaine. On appelle souvent ce type d'isolation le principe du bac à sable.

CM-08(04) — Information sur la responsabilisation (---)

Énoncés :

L'organisation inclut dans l'information liée à l'inventaire de composants de système d'information une façon d'identifier par [Sélection (un choix ou plus) : nom; poste; rôle] les personnes responsables de l'administration de ces composants.

Responsable : Aucun

Discussion :

L'identification des personnes responsables de l'administration des composants de système permet de faire en sorte que les composants concernés sont bien administrés et que les organisations peuvent communiquer avec les personnes désignées si des mesures doivent être prises (par exemple, on détermine qu'un composant est source de manquement, ce composant doit être rappelé ou remplacé, ou encore relocalisé).

CM-08(05) — Aucune comptabilisation en double des composants (---)

Énoncés :

Annulé : Intégré au contrôle CM-08.

Responsable : Aucun

CM-08(06) — Configurations évaluées et écarts approuvés (---)

Énoncés :

Inclure dans l'inventaire des composants du système les configurations de composants évaluées et les écarts approuvés en ce qui a trait aux configurations déjà déployées.

Responsable : Aucun

Discussion :

Les configurations évaluées et écarts approuvés sont axés sur les paramètres de configuration qu'ont établis les organisations concernant les composants de système, sur les composants précis qui ont été évalués afin de vérifier leur conformité aux paramètres de configuration requis et sur tous les écarts approuvés des paramètres de configuration établis.

CM-08(07) — Référentiel centralisé (---)

Énoncés :

Fournir un référentiel centralisé contenant l'inventaire des composants de système.

Responsable : Aucun

Discussion :

Les organisations peuvent mettre en oeuvre des inventaires de composants de systèmes centralisés qui comprennent des composants de tous les systèmes. Les référentiels centralisés des inventaires de composants de système permettent d'améliorer l'efficience de la comptabilisation des biens matériels, logiciels et micrologiciels. Grâce à ces référentiels, les organisations peuvent rapidement trouver l'emplacement des composants de système ayant fait l'objet d'une compromission ou d'une intrusion ou pour lesquels il faut prendre des mesures d'atténuation, de même que déterminer les personnes qui sont responsables de ces composants. Les organisations s'assurent que ces inventaires centralisés comportent l'information propre au système qui est nécessaire à la comptabilisation des composants.

CM-08(08) — Localisation automatisée (---)

Énoncés :

Appuyer le suivi des composants de système par géolocalisation des composants de système au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

L'utilisation de mécanismes automatisés pour géolocaliser les composants de système permet d'améliorer la précision des inventaires de composants. Grâce à cette capacité, les organisations peuvent rapidement trouver l'emplacement des composants de système ayant fait l'objet d'une compromission ou d'une intrusion ou pour lesquels il faut prendre des mesures d'atténuation, de même que déterminer les personnes qui sont responsables de ces composants. L'utilisation de mécanismes de suivi devrait être coordonnée avec les hauts fonctionnaires ou cadres supérieures et supérieurs étant donné qu'il pourrait y avoir des implications pouvant toucher la vie privée des personnes.

CM-08(09) — Attribution de composants à des systèmes (---)

Énoncés :

a. Attribuer des composants à un système
b. Recevoir un avis de cette affectation de la part de [Affectation : personnel ou rôles définis par l'organisation]

Responsable : Aucun

Discussion :

Les composants du système qui ne sont pas attribués à un système peuvent être non gérés, manquer de protection et devenir une vulnérabilité pour l'organisation.

CM-09 — Plan de gestion des configurations (---)

Énoncés :

Élaborer, documenter et mettre en oeuvre un plan de gestion des configurations pour le système qui :
a. traite les rôles, les responsabilités ainsi que les processus et procédures de gestion des configurations
b. établit un processus pour déterminer les éléments de configuration tout au long du cycle de développement des systèmes et pour gérer la configuration des éléments de configuration
c. définit les éléments de configuration pour le système et intègre les éléments de configuration à la gestion des configurations
d. est examiné et approuvé par [Affectation : personnel ou rôles définis par l'organisation]
e. protège le plan de gestion des configurations contre toute divulgation ou modification non autorisée

Responsable : Aucun

Discussion :

Les activités de gestion des configurations se produisent tout au long du cycle de développement des systèmes. Ainsi, il y a des activités de développement de la gestion des configurations (par exemple, le contrôle de code et les bibliothèques de logiciels) et des activités opérationnelles de gestion des configurations (par exemple, le contrôle de composants installés et la façon de configurer les composants). Les plans de gestion des configurations répondent aux exigences des politiques de gestion des configurations tout en étant adaptés aux systèmes individuels. Les plans de gestion des configurations définissent les processus et les procédures d'utilisation de la gestion des configurations pour appuyer les activités du cycle de développement du système. Les plans de gestion des configurations sont élaborés durant la phase de développement ou d'acquisition du cycle de développement du système. Les plans décrivent comment apporter un changement à l'aide des processus de gestion des changements, mettre à jour les mesures de configuration et les configurations de référence, tenir des inventaires des composants de système, contrôler les environnements de développement, de tests et d'opérations et, enfin, diffuser et mettre à jour les documents clés. Les organisations peuvent utiliser des modèles pour veiller à l'élaboration et à la mise en oeuvre uniformes et rapides des plans de gestion des configurations. Les modèles peuvent être un plan de gestion des configurations pour l'organisation; les sous-ensembles du plan peuvent être appliqués à un système, en fonction du système visé. Les processus d'approbation de la gestion des configurations comprennent la nomination d'intervenantes et intervenants clés chargés d'examiner et d'approuver les changements proposés aux systèmes et du personnel chargé d'analyser les incidences sur la sécurité et le respect de la vie privée avant d'apporter les changements aux systèmes. Les éléments de configuration sont des composants des systèmes comme le matériel, les logiciels, les micrologiciels et la documentation dont la configuration doit être gérée. Durant les cycles de vie de développement des systèmes, de nouveaux éléments de configuration peuvent être signalés et certains éléments de configuration peuvent ne plus être nécessaires dans le cadre du contrôle des configurations.

CM-09(01) — Attribution des responsabilités (---)

Énoncés :

Confier la responsabilité du développement du processus de gestion des configurations à des employées et employés de l'organisation qui ne participent pas directement au développement du système.

Responsable : Aucun

Discussion :

En l'absence d'équipe de gestion des configurations spécialisée au sein des organisations, les développeurs de systèmes peuvent se voir assigner l'élaboration des processus de gestion de la configuration et devoir faire appel à des employées et employés qui ne participent pas directement au développement ou à l'intégration de systèmes. Cette séparation des tâches permet de veiller à ce que les organisations établissent et maintiennent un degré suffisant d'indépendance entre les processus de développement et d'intégration du système et les processus de gestion des configurations afin de faciliter le contrôle de la qualité et d'améliorer l'efficacité de la surveillance.

CM-10 — Restrictions relatives à l'utilisation des logiciels (---)

Énoncés :

a. Utiliser les logiciels et la documentation connexe conformément aux ententes contractuelles et aux lois sur le droit d'auteur
b. Faire le suivi de l'utilisation des logiciels et de la documentation connexe qui sont protégés par des licences limitant la copie et la diffusion du produit
c. Contrôler et documenter l'utilisation de la technologie de partage de fichiers pair à pair pour s'assurer qu'elle n'est pas utilisée à des fins non autorisées de distribution, d'affichage, d'exécution ou de reproduction d'oeuvres protégées par le droit d'auteur

Responsable : Aucun

Discussion :

Le suivi des licences d'utilisation de logiciel peut s'effectuer de façon manuelle ou automatique, selon les besoins de l'organisation. Des exemples d'ententes contractuelles comprennent des contrats de licence de logiciels et des accords de non-divulgation.

CM-10(01) — Logiciels ouverts (---)

Énoncés :

Établir les restrictions suivantes sur l'utilisation de logiciel à source ouverte : [Affectation : restrictions définies par l'organisation].

Responsable : Aucun

Discussion :

On entend, par logiciels de source ouverte, les logiciels offerts sous forme de code source. Certains droits d'utilisation de logiciels normalement réservés aux détenteurs de droits d'auteur sont habituellement accordés conformément à des contrats de licence et autorisent des personnes à étudier, modifier ou améliorer le logiciel. Au chapitre de la sécurité, l'avantage principal des logiciels de source ouverte est le fait qu'ils offrent aux organisations la possibilité d'étudier le code source. Dans certains cas, il y a une communauté en ligne associée aux logiciels qui inspecte, teste, met à jour et signale en permanence les problèmes détectés dans les logiciels. Toutefois, corriger des vulnérabilités dans des logiciels de source ouverte peut s'avérer problématique. Il peut y avoir divers enjeux liés aux licences de logiciels de source ouverte, comme les contraintes associées à l'utilisation dérivée de ces logiciels.

CM-11 — Logiciels installés par les utilisatrices et utilisateurs (---)

Énoncés :

a. Établir [Affectation : stratégies définies par l'organisation] qui régissent l'installation de logiciels par des utilisatrices et utilisateurs
b. Appliquer des stratégies d'installation de logiciels au moyen des méthodes suivantes : [Affectation : stratégies définies par l'organisation]
c. Surveiller le respect des stratégies [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

S'ils détiennent les privilèges nécessaires, les utilisatrices et utilisateurs peuvent installer des logiciels sur les systèmes organisationnels. Afin de garder le contrôle sur les logiciels installés, les organisations doivent déterminer les opérations permises et interdites concernant l'installation de logiciels. Les installations de logiciels autorisées comprennent les mises à jour et l'application de correctifs de sécurité aux logiciels existants, ainsi que le téléchargement de nouvelles applications à partir des magasins d'application approuvés par l'organisation. Les installations non autorisées comprennent les logiciels dont la provenance est inconnue ou suspecte, ou les logiciels qui sont potentiellement malveillants d'après les organisations. Les stratégies sélectionnées pour régir les logiciels installés par les utilisatrices et utilisateurs peuvent être développées par l'organisation ou fournies par une entité externe. Les méthodes d'application des stratégies peuvent inclure des méthodes procédurales et des méthodes automatisées.

CM-11(01) — Alertes pour les installations non autorisées (---)

Énoncés :

Annulé : Intégré au contrôle CM-08(03).

Responsable : Aucun

CM-11(02) — Installation de logiciels avec statut privilégié (---)

Énoncés :

Autoriser l'installation de logiciel par les utilisatrices et utilisateurs qui ont un accès privilégié explicite.

Responsable : Aucun

Discussion :

Il est possible d'obtenir un statut privilégié en assumant par exemple des fonctions d'administrateur système.

CM-11(03) — Application et surveillance automatisées (---)

Énoncés :

Appliquer et surveiller la conformité aux stratégies d'installation de logiciels au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Les organisations appliquent et surveillent la conformité aux stratégies d'installation de logiciels au moyen de mécanismes automatisés, ce qui permet une détection et une intervention plus rapides en cas d'installation de logiciels non autorisés; une telle situation peut indiquer la présence d'une attaque hostile interne ou externe.

CM-12 — Localisation de l'information (---)

Énoncés :

a. Établir et consigner la localisation de [Affectation : information désignée par l'organisation] et des composants de systèmes particuliers où l'information est traitée et stockée
b. Établir et consigner les utilisatrices et utilisateurs qui ont accès au système et à ses composants où l'information est traitée et stockée
c. Consigner les changements de la localisation (par exemple, le système ou les composants du système) où l'information est traitée et stockée

Responsable : Aucun

Discussion :

La localisation de l'information répond au besoin de bien comprendre où l'information est traitée et stockée, et reflète les exigences en matière de résidence de données. La localisation de l'information implique de déterminer où résident des types spécifiques d'information ainsi que l'information dans les composants des systèmes et comprend également comment l'information est traitée de manière à bien comprendre le flux d'information et à fournir une protection et une gestion adéquates de cette information et de ces composants des systèmes. La localisation de l'information et des composants des systèmes entre aussi en compte dans l'architecture et la conception du système (voir SA-04, SA-08, SA-17). Il pourrait y avoir des implications relatives à la localisation de l'information pour les systèmes qui traitent les renseignements personnels.

CM-12(01) — Outils automatisés associés à la localisation de l'information (---)

Énoncés :

Utiliser des outils automatisés pour identifier [Affectation : information définie par l'organisation selon le type d'information] sur des [Affectation : composants de système définis par l'organisation] pour assurer que des contrôles sont mis en place pour protéger l'information de l'organisation et la vie privée des personnes.

Responsable : Aucun

Discussion :

L'utilisation d'outils automatisés aide à accroître l'efficacité et l'efficience de la capacité liée à la localisation de l'information mise en oeuvre dans le système. L'automatisation aide également les organisations à gérer les données produites pendant les activités de localisation de l'information et à échanger l'information dans l'ensemble de l'organisation. Les résultats obtenus par les outils de localisation de l'information automatisés peuvent être utilisés afin d'orienter et d'éclairer sur les décisions en matière d'architecture et de conception des systèmes.

CM-13 — Mappage des actions de données (---)

Énoncés :

Élaboration et documentation d'un plan des actions de données du système.

Responsable : Aucun

Discussion :

Les actions de données sont des opérations système, et certaines des actions de données impliquent des renseignements personnels. La gestion de tels renseignements englobe le cycle de vie complet de l'information, ce qui comprend la collecte, la création, la transformation, l'utilisation, la divulgation, la conservation et l'élimination. Un plan d'action de données du système comprend les actions de données discrètes qui déterminent les éléments des renseignements personnels utilisés pour les actions de données, les composants des systèmes impliqués dans les actions de données, les gardiennes et gardiens de l'information, et les propriétaires ou les exploitants des composants des systèmes. Comprendre quels renseignements personnels sont traités (par exemple, la sensibilité des renseignements personnels), comment les renseignements personnels sont traités (par exemple, si l'action de données est visible pour la personne ou est traitée dans une autre partie du système) et par qui, permet de fournir des facteurs contextuels qui sont importants à l'évaluation du niveau de risque d'atteinte à la vie privée associé au système. Les plans de données peuvent être utilisés de différentes façons, et le degré de détails peut varier en fonction des besoins liés à la mission et aux activités de l'organisation. Le plan de données peut représenter une superposition de tout artéfact de conception du système qu'utilise une organisation. L'élaboration de ce plan peut nécessiter une coordination entre les programmes de sécurité et de protection de la vie privée concernant les actions de données couvertes et les composants qui sont déterminés comme faisant partie du système. Les utilisatrices et utilisateurs dont les activités sont mises en correspondance devraient être mis au courant de l'activité.

CM-14 — Composants signés (---)

Énoncés :

Empêcher l'installation de [Affectation : éléments logiciels et micrologiciels définis par l'organisation] sans vérification de leur signature électronique par l'intermédiaire d'un certificat reconnu ou approuvé par l'organisation.

Responsable : Aucun

Discussion :

Les mises à niveau des versions de logiciels et de micrologiciels, les correctifs, les ensembles de modifications provisoires, les pilotes de périphérique et les mises à niveau de systèmes d'entrée-sortie de base sont des de composants logiciels et micrologiciels impossibles à installer s'ils n'ont pas été signés numériquement à l'aide de certificats reconnus et approuvés. Les organisations peuvent classer les composants logiciels et micrologiciels applicables par type ou élément particulier ou encore selon une combinaison des deux. Les signatures numériques et la vérification de ces signatures par l'organisation sont des méthodes d'authentification.

CP

Planification de la continuité d'activité

Contingency Planning

CP-01 — Politique et procédures de planification d'urgence (---)

Énoncés :

a. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :

1. une politique de planification d'urgence [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables

2. des procédures pour faciliter la mise en oeuvre des politiques de gestion de planification d'urgence et des contrôles de planification d'urgence connexes

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à la planification d'urgence

c. Passer en revue et mettre à jour, par rapport à la planification d'urgence :

1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La politique et les procédures de planification d'urgence abordent les contrôles de la famille Planification d'urgence qui ont été mis en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à l'élaboration de la politique et des procédures de planification d'urgence. En règle générale, les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin pour des politiques et des procédures propres à la mission ou au système. La politique peut être intégrée à une politique générale sur la sécurité et la protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures de planification d'urgence comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, à la jurisprudence, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.

CP-02 — Plan d'urgence (Nc--)

Énoncés :

a. Élaborer un plan d'urgence pour le système qui :
- **1.** identifie les fonctions opérationnelles et de mission essentielles et les exigences connexes en matière d'urgence
- **2.** définit les objectifs de reprise, les priorités de restauration et les paramètres
- **3.** identifie les rôles et responsabilités liés aux urgences et les personnes assignées à ces fonctions, y compris leurs coordonnées
- **4.** souligne le besoin de maintenir les fonctions opérationnelles et de mission essentielles en dépit de toute perturbation, compromission ou défaillance du système
- **5.** traite de la restauration complète du système sans détérioration des contrôles initialement prévus et mis en oeuvre
- **6.** traite de l'intégrité des données conservées dans le système, y compris les renseignements personnels
- **7.** traite des répercussions, des préjudices ou des conséquences de la compromission d'un système, y compris en ce qui a trait aux renseignements personnels
- **8.** décrit les modalités d'échange d'information
- **9.** est examiné et approuvé par [Affectation : personnel ou rôles définis par l'organisation]

b. Distribuer des exemplaires du plan d'urgence à [Affectation : liste (par nom ou rôle) définie par l'organisation des principales et principaux responsables des mesures d'urgence et des éléments organisationnels]
c. S'assurer que les personnes qui assument des responsabilités examinent le plan d'urgence et comprennent leurs rôles
d. Coordonner les activités de planification d'urgence avec les activités de traitement des incidents
e. Examiner le plan d'urgence pour le système [Affectation : fréquence définie par l'organisation]
f. Mettre à jour le plan d'urgence pour tenir compte des changements apportés à l'organisation, au système ou à l'environnement d'exploitation et des problèmes survenus lors de la mise en oeuvre, de l'exécution ou des tests du plan
g. Communiquer les changements apportés au plan d'urgence à [Affectation : liste (par nom ou rôle) définie par l'organisation des principales et principaux responsables des mesures d'urgence et des éléments organisationnels]
h. Intégrer les leçons apprises tirées des essais du plan d'urgence, de la formation ou des activités d'urgence concrètes aux essais et à la formation sur les mesures d'urgence a
a. Protéger le plan d'urgence contre les divulgations ou les modifications non autorisées

Responsable : Aucun

Discussion :

La planification d'urgence pour les systèmes fait partie du programme global sur la continuité des fonctions liées à la mission et aux activités de l'organisation. En cas de compromission ou de violation des systèmes, la planification d'urgence tient compte de la restauration des systèmes, de la mise en oeuvre de processus de secours liés à la mission et aux activités. La planification d'urgence est prise en compte tout au long du cycle de développement des systèmes et est une partie fondamentale de la conception des systèmes. Les systèmes peuvent être conçus aux fins de redondance, pour fournir des capacités de secours, et aux fins de résilience. Les plans d'urgence correspondent à l'effort requis pour la restauration des systèmes organisationnels puisque ceux-ci ne doivent pas tous être nécessairement complètement restaurés pour assurer le niveau de continuité des opérations requis. Les objectifs de récupération des systèmes tiennent compte des lois applicables, des décrets applicables, des directives, des règlements, de la jurisprudence, des politiques, des normes, des lignes directrices, de la tolérance aux risques de l'organisation et du niveau d'incidence sur le système. Les actions prévues dans les plans d'urgence incluent la dégradation progressive, la mise hors tension des systèmes, le passage en mode manuel, l'utilisation de flux d'information de secours et le fonctionnement en modes réservés aux situations d'attaque contre les systèmes. En coordonnant la planification d'urgence et les activités de traitement des incidents, les organisations veillent à ce que les activités nécessaires de planification soient en place et mises en oeuvre en cas d'incident. Les organisations devraient déterminer si la continuité des opérations durant un incident entre en conflit avec la capacité à désactiver automatiquement le système, conformément à l'IR-04(05). La planification d'intervention en cas d'incident fait partie de la planification d'urgence et est traitée dans la famille IR (intervention en cas d'incident).

CP-02(01) — Coordination avec les plans connexes (---)

Énoncés :

Coordonner le développement du plan d'urgence avec les éléments organisationnels responsables des plans connexes.

Responsable : Aucun

Discussion :

Les plans connexes aux plans d'urgence comprennent les suivants : plans de continuité des activités, plans de reprise après sinistre, plans de continuité des opérations, plans des communications en temps de crise, plans de mise en oeuvre en cas de menace interne, plans d'intervention en cas de violation de données, protocoles sur les atteintes à la vie privée, plans d'intervention en cas de cyberincident, d'intervention en cas de violation et plans de mesures d'urgence pour les occupants.

CP-02(02) — Planification de la capacité (---)

Énoncés :

Planifier la capacité de manière à disposer des ressources nécessaires pour traiter l'information, utiliser les télécommunications et soutenir l'environnement durant les opérations d'urgence.

Responsable : Aucun

Discussion :

Une planification de la capacité est requise puisque différentes menaces peuvent nuire à la capacité de traitement, à l'utilisation des télécommunications et aux services de soutien prévus à l'appui des fonctions liées à la mission et aux activités. Les organisations doivent prévoir une dégradation des opérations durant la mise en oeuvre d'opérations d'urgence et doivent tenir compte de cette dégradation lors de la planification de la capacité. Pour ce qui est de la planification de la capacité, la prise en charge de l'environnement fait référence à tout facteur environnemental pour lequel l'organisation estime qu'il est nécessaire de fournir un soutien dans une situation d'urgence, même dans un état de dégradation. De tels faits sont basés sur une évaluation organisationnelle des risques, une catégorisation des systèmes (niveau d'incidence) et la tolérance au risque de l'organisation.

CP-02(03) — Reprise de la mission et des activités (---)

Énoncés :

Planifier la reprise des [Sélection (un choix) : toutes; essentielles] fonctions liées à la mission et aux activités essentielles dans un délai de [Affectation : délais définis par l'organisation] suivant l'activation du plan d'urgence.

Responsable : Aucun

Discussion :

Les organisations peuvent opter pour des activités de planification d'urgence pour la reprise des fonctions liées à la mission et aux activités dans le cadre de la planification de la continuité des activités ou d'analyses de reprise de la mission et des activités. Les organisations accordent la priorité à la reprise des fonctions liées à la mission et aux activités. Le délai de reprise des fonctions liées à la mission et aux activités peut dépendre de la gravité et de la portée des perturbations aux systèmes et à l'infrastructure d'appui. Des précautions doivent être prises en évaluant de possibles modifications aux renseignements personnels se trouvant dans un système compromis.

CP-02(04) — Reprise de toutes les fonctions liées à la mission et aux activités de l'organisation (---)

Énoncés :

Annulé : Intégré au contrôle CP-02(03).

Responsable : Aucun

CP-02(05) — Continuer les fonctions liées à la mission et aux activités (---)

Énoncés :

Planifier la continuité des [Sélection (un choix) : toutes; essentielles] fonctions liées à la mission et aux activités avec peu ou pas de perte sur le plan de la continuité opérationnelle et maintenir cet état jusqu'à la restauration complète du système dans les sites principaux de traitement ou de stockage.

Responsable : Aucun

Discussion :

Les organisations peuvent opter pour des activités de planification d'urgence pour la continuité des fonctions liées à la mission et aux activités dans le cadre de la planification de la continuité des activités ou d'analyses des répercussions sur les activités. Les sites de traitement et de stockage définis par l'organisation dans le cadre de la planification d'urgence peuvent changer en fonction des circonstances liées à l'urgence.

CP-02(06) — Sites de traitement et de stockage auxiliaires (---)

Énoncés :

Prévoir le transfert des [Sélection (un choix) : toutes; essentielles] fonctions liées à la mission et aux activités essentielles vers des sites de traitement ou de stockage auxiliaires avec peu ou pas de perte sur le plan de la continuité des activités, et maintenir cet état pendant la restauration complète des sites principaux de traitement ou de stockage.

Responsable : Aucun

Discussion :

Les organisations peuvent opter pour des activités de planification d'urgence pour des sites de traitement et de stockage auxiliaires dans le cadre de la planification de la continuité des activités ou d'analyses des répercussions sur les activités. Les sites de traitement et de stockage définis par l'organisation dans le cadre de la planification d'urgence peuvent changer en fonction des circonstances liées à l'urgence.

CP-02(07) — Coordination avec les fournisseurs de services externes (---)

Énoncés :

Coordonner son plan d'urgence avec ceux des fournisseurs de services externes pour veiller à répondre aux exigences des plans d'urgence.

Responsable : Aucun

Discussion :

Il peut être difficile pour une organisation d'élaborer un plan d'urgence complet et opportun si sa capacité d'exécuter ses fonctions opérationnelles et de mission principales dépend de ses fournisseurs de services externes. Lorsque les fonctions liées à la mission et aux activités de l'organisation dépendent des fournisseurs de services externes, il vaut mieux pour les organisations de coordonner leurs activités de planification d'urgence avec les entités externes pour veiller à ce que le plan de chaque organisation et de chaque entité réponde à ses besoins globaux en cas d'urgence. S'assurer que le mécanisme de passation de marchés inclut des clauses exigeant que les fournisseurs de services externes avisent et collaborent avec l'organisation advenant la compromission d'un système détenant des renseignements personnels.

CP-02(08) — Désignation des biens essentiels (Nc--)

Énoncés :

Désigner les biens essentiels du système qui soutiennent [Sélection (un choix) : toutes les fonctions; les fonctions essentielles] liées à la mission et aux activités.

Responsable : Aucun

Discussion :

Les organisations peuvent choisir de déterminer des biens essentiels dans le cadre d'une analyse de criticité, de la planification de continuité des activités ou d'analyses des répercussions sur les activités. Les organisations désignent les biens essentiels en matière de systèmes afin que des contrôles additionnels puissent être utilisés (bien au-delà des contrôles régulièrement mis en oeuvre) pour veiller à ce que les fonctions liées à la mission et aux activités de l'organisation puissent se poursuivre lors des opérations d'urgence. La désignation des biens essentiels en matière d'information facilite également la priorisation des ressources organisationnelles. Les biens essentiels en matière de systèmes comprennent des éléments techniques et opérationnels. Les aspects techniques comprennent les composants des systèmes, les services de TI, les produits informatiques et les mécanismes. Les éléments opérationnels comprennent les procédures (par exemple, les opérations exécutées manuellement) et le personnel (par exemple, des personnes opérant des contrôles techniques ou exécutant des procédures manuelles). Les plans de protection des programmes organisationnels peuvent faciliter la désignation des biens essentiels. Si des biens essentiels se trouvent dans l'organisation ou sont pris en charge par des fournisseurs de services externes, l'organisation devrait songer à mettre en oeuvre le contrôle CP-02(07) pour l'amélioration du contrôle.

CP-03 — Formation en mesure d'urgence (---)

Énoncés :

a. Fournir une formation en mesure d'urgence aux utilisatrices et utilisateurs du système en fonction des rôles et des responsabilités attribués :

1. dans [Affectation : délais définis par l'organisation] après avoir été affecté à un rôle ou à des responsabilités
2. lorsque des changements apportés au système l'exigent
3. tous les [Affectation : fréquence définie par l'organisation] par la suite

b. Passer en revue et mettre à jour le contenu de la formation en mesure d'urgence tous les [Affectation : fréquence définie par l'organisation] et à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La formation en mesure de sécurité offerte par l'organisation correspond aux responsabilités et aux rôles assignés à son personnel de sorte à assurer un contenu et un niveau de détails appropriés. Par exemple, des personnes ont peut-être seulement besoin de savoir quand et où elles doivent se présenter pour le travail lors d'opérations d'urgence et si ces mesures auront une incidence sur l'exécution de leurs fonctions normales; les administratrices et administrateurs de systèmes pourraient avoir besoin d'une formation additionnelle sur l'installation et le paramétrage de systèmes aux sites de traitement et de stockage auxiliaires; les responsables des organisations pourraient requérir plus de formation précise sur l'exécution de fonctions essentielles à la mission depuis des emplacements hors site et sur l'établissement de modes de communication avec d'autres entités gouvernementales aux fins de coordination des activités connexes au plan d'urgence. La formation sur les mesures d'urgence adaptée aux rôles et aux responsabilités répond à des besoins précis de continuité relevés dans le plan d'urgence. Les événements qui peuvent précipiter une mise à jour du contenu de la formation comprennent la mise à l'essai du plan d'urgence ou une urgence concrète (leçons retenues), les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, à la jurisprudence, aux politiques, aux normes et aux lignes directrices applicables. À la discrétion de l'organisation, une participation à l'exercice ou à la mise à l'essai du plan d'urgence, y compris les séances consacrées aux leçons retenues à la suite de la mise à l'essai ou de l'exercice, pourrait répondre aux exigences en matière de formation sur le plan d'urgence.

CP-03(01) — Événements simulés (---)

Énoncés :

Intégrer des événements simulés à la formation en mesure d'urgence pour faciliter l'intervention efficace du personnel en situation de crise.

Responsable : Aucun

Discussion :

Le recours à des événements simulés crée un environnement permettant au personnel de faire l'expérience de réelles menaces informatiques, y compris des cyberattaques qui désactivent des sites Web, des attaques par rançongiciel qui chiffrent les données de l'organisation sur les serveurs, des ouragans qui endommagent ou détruisent les installations organisationnelles ou des pannes matérielles ou logicielles.

CP-03(02) — Mécanismes utilisés dans des environnements de formation (---)

Énoncés :

Employer des mécanismes utilisés dans des opérations pour offrir un environnement de formation en mesure d'urgence plus approfondi et réaliste.

Responsable : Aucun

Discussion :

Les mécanismes opérationnels font référence aux processus qui ont été établis pour atteindre un objectif d'une organisation ou à un système qui soutient un objectif particulier de la mission et des activités de l'organisation. De véritables processus, systèmes ou installations liés à la mission et aux activités peuvent être utilisés pour générer des événements simulés et accroître le réalisme des événements simulés pendant la formation en mesure d'urgence.

CP-04 — Mise à l'essai du plan d'urgence (Nc--)

Énoncés :

a. Mettre à l'essai le plan d'urgence pour les systèmes [Affectation : fréquence définie par l'organisation] en utilisant les tests suivants pour en déterminer l'efficacité et établir la mesure dans laquelle il est prêt à être exécuté : [Affectation : tests définis par l'organisation]
b. Étudier les résultats des tests du plan d'urgence
c. Prendre les mesures correctives nécessaires

Responsable : Aucun

Discussion :

Il existe plusieurs méthodes pour tester les plans d'urgence en vue de déterminer leur efficacité et de relever des faiblesses possibles, dont les listes de vérification, les exercices de révision structurée et d'analyse des documents, les simulations en parallèle et en état d'arrêt complet ou les exercices détaillés. Les tests effectués par les organisations visent à vérifier les exigences établies dans les plans d'urgence et à déterminer les répercussions sur les opérations organisationnelles, les biens et les personnes découlant des opérations d'urgence. Les organisations disposent d'une certaine souplesse et discrétion quant à la portée, l'étendue et le calendrier des mesures correctives.

CP-04(01) — Coordination avec les plans connexes (---)

Énoncés :

Coordonner la mise à l'essai du plan d'urgence avec les éléments organisationnels responsables des plans connexes.

Responsable : Aucun

Discussion :

Les plans connexes aux plans d'urgence pour les systèmes de l'organisation comprennent les suivants : plans de continuité des activités, plans de reprise après sinistre, plans de continuité des opérations, plans des communications en temps de crise, plans des infrastructures essentielles, plans d'intervention en cas de cyberincident et plans de mesures d'urgence pour les occupants. La coordination de la mise à l'essai du plan d'urgence n'exige pas des organisations qu'elles créent des éléments organisationnels pour traiter des plans connexes ni qu'elles ne lient ces éléments avec les plans particuliers. Toutefois, cela exige que de tels éléments organisationnels soient responsables des plans connexes et une coordination entre ces éléments et l'organisation.

CP-04(02) — Site de traitement auxiliaires (---)

Énoncés :

Tester le plan d'urgence au site de traitement auxiliaire pour :
a. familiariser le personnel participant au plan d'urgence pour qu'il connaisse mieux l'installation et les ressources qui y sont accessibles
b. évaluer si celui-ci peut prendre en charge les opérations d'urgence

Responsable : Aucun

Discussion :

Les conditions au site de traitement auxiliaire peuvent être largement différentes des conditions au site principal. Avoir l'occasion de visiter le site de traitement auxiliaire et d'expérimenter les réelles capacités disponibles au site peut donner des renseignements utiles sur les vulnérabilités possibles pouvant toucher les fonctions liées à la mission et aux activités de l'organisation. La visite sur le site peut aussi donner l'occasion d'ajuster le plan d'urgence pour traiter les vulnérabilités détectées durant le test.

CP-04(03) — Tests automatisés (---)

Énoncés :

Tester le plan d'urgence au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Des mécanismes automatisés permettent de tester plus le plan d'urgence de manière plus détaillée et efficace en assurant une couverture plus complète des situations d'urgence; en sélectionnant des scénarios et des environnements de test plus réalistes; en soumettant les systèmes et les fonctions liées à la mission et aux activités de l'organisation à des contraintes.

CP-04(04) — Reprise et reconstitution complètes (---)

Énoncés :

Inclure dans les tests du plan d'urgence une reprise et une reconstitution complètes du système à un état connu.

Responsable : Aucun

Discussion :

La reprise consiste à exécuter les activités du plan d'urgence pour restaurer les fonctions liées à la mission et aux activités de l'organisation. La reconstitution suit la reprise et englobe les activités de restauration des systèmes à un état opérationnel complet. Les organisations établissent un état connu pour les systèmes qui comprend de l'information d'état pour les programmes matériels et informatiques, et les données. La protection de l'information d'état du système facilite le redémarrage du système et le retour au mode opérationnel des organisations tout en perturbant le moins possible les processus liés à la mission ou aux opérations.

CP-04(05) — Se mettre au défi (---)

Énoncés :

Employer [Affectation : mécanismes définis par l'organisation] pour [Affectation : système ou composant de système désigné par l'organisation] pour perturber et nuire au système ou au composant du système.

Responsable : Aucun

Discussion :

Souvent, la meilleure méthode d'évaluation de la résilience d'un système est en quelque sorte de perturber le système. Les mécanismes utilisés par l'organisation pourraient perturber les fonctions du système ou les services du système de plusieurs façons, y compris par la mise hors fonction ou la désactivation de composants essentiels du système, le changement de configuration des composants du système, la dégradation de la fonctionnalité critique (par exemple, limiter la bande passante du réseau) ou la modification de privilèges. Des cyberattaques et des perturbations de services automatisées, continues et simulées peuvent révéler des dépendances fonctionnelles inattendues et aider l'organisation à déterminer sa capacité à assurer sa résilience face à une réelle cyberattaque.

CP-05 — Mise à jour du plan d’urgence (---)

Énoncés :

Annulé : Intégré au contrôle CP-02.

Responsable : Aucun

CP-06 — Site de stockage auxiliaire (---)

Énoncés :

a. Établir un site de stockage auxiliaire, y compris les ententes nécessaires pour permettre le stockage et la récupération de l'information de sauvegarde des systèmes
b. S'assurer que le site de stockage auxiliaire offre des contrôles équivalents à ceux du site principal

Responsable : Aucun

Discussion :

Les sites de stockage de secours se distinguent sur le plan géographique des sites de stockage principaux et ils conservent des copies des renseignements et des données si le site de stockage principal n'est pas accessible. De même, un site de traitement auxiliaire offre une capacité de traitement si le site de traitement principal n'est pas accessible. Des architectures réparties dans d'autres régions qui soutiennent des exigences connexes en matière d'urgence peuvent être considérées comme des sites de stockage auxiliaires. Les conventions d'utilisation des sites de stockage auxiliaires comprennent des dispositions traitant des conditions environnementales du site auxiliaire, des règles d'accès pour les systèmes et les installations, des exigences de protection environnementale et physique et de la coordination de la livraison et de la récupération des supports de sauvegarde. Les sites de stockage auxiliaires répondent à l'exigence, inscrite dans les plans d'urgence, selon laquelle les organisations doivent maintenir la capacité d'exécuter les fonctions essentielles liées à la mission et aux activités de l'organisation en dépit de toute perturbation, compromission ou défaillance des systèmes organisationnels.

CP-06(01) — Séparation du site principal (---)

Énoncés :

Identifier un site de stockage auxiliaire suffisamment distinct du site principal afin de réduire sensiblement l'exposition aux mêmes menaces.

Responsable : Aucun

Discussion :

Les menaces auxquelles sont susceptibles les sites de stockage auxiliaires sont définies dans les évaluations des risques de l'organisation et comprennent les désastres naturels, les défaillances structurales, les cyberattaques hostiles et les erreurs par omission ou par action. Les organisations déterminent la distance géographique suffisante entre les sites de stockage principaux et auxiliaires en fonction des types de menaces auxquelles elles font face. Dans le cas de menaces comme des attaques hostiles, la séparation entre les sites est moins pertinente.

CP-06(02) — Objectifs de délai de rétablissement et de point de rétablissement (---)

Énoncés :

Configurer le site auxiliaire de manière à faciliter les opérations de reprise conformément aux objectifs de délai et de point de rétablissement.

Responsable : Aucun

Discussion :

Les organisations établissent des objectifs de délai de rétablissement et de point de rétablissement dans le cadre de la planification d'urgence. La configuration du site de stockage auxiliaire comprend les installations physiques et les systèmes qui soutiennent les opérations de reprise qui assurent l'accessibilité et une exécution adéquate.

CP-06(03) — Accessibilité (---)

Énoncés :

Identifier les problèmes d'accessibilité potentiels du site stockage auxiliaire dans l'éventualité d'une perturbation ou d'un désastre majeurs et énoncer des mesures d'atténuation explicites.

Responsable : Aucun

Discussion :

Les perturbations touchant à toute la région sont des perturbations dont l'étendue géographique est vaste. Une organisation doit identifier elle-même les problèmes d'accessibilité en fonction de son évaluation des risques. Des mesures d'atténuation explicites comprennent de copier l'information de sauvegarde à d'autres sites de stockage auxiliaires si un problème d'accessibilité survient aux sites auxiliaires originaux ou de planifier l'accès physique en prévision d'une récupération de l'information de sauvegarde au cas où l'accessibilité électronique au site auxiliaire est perturbée.

CP-07 — Site de traitement auxiliaire (---)

Énoncés :

a. Établir un site de traitement auxiliaire, y compris les ententes nécessaires pour permettre le transfert et la reprise [Affectation : opérations des systèmes définies par l'organisation] pour les fonctions opérationnelles et de mission essentielles dans un délai de [Affectation : durée conforme aux objectifs de délai et de point de reprise définis par l'organisation], lorsque les capacités de traitement principales ne sont pas accessibles
b. Rendre accessibles au site de traitement auxiliaire l'équipement et les fournitures nécessaires pour transférer et permettre une reprise des activités ou mettre des contrats pour assurer leur livraison au site, et ce, dans les délais définis par l'organisation pour le transfert ou la reprise des activités
c. Fournir des contrôles au site de traitement auxiliaire qui sont équivalents à ceux du site principal

Responsable : Aucun

Discussion :

Les sites de traitement auxiliaires se distinguent sur le plan géographique des sites de traitement principal et ils donnent une capacité de traitement si le site de traitement principal n'est pas accessible. La capacité de traitement auxiliaire peut être communiquée à l'aide d'un site de traitement physique ou d'autres solutions, comme le basculement à un fournisseur de services infonuagiques ou à un autre service interne ou externe de traitement. Des architectures réparties dans d'autres régions qui soutiennent des exigences connexes en matière d'urgence peuvent être considérées comme des sites de traitement auxiliaires. Les contrôles couverts par des conventions d'utilisation des sites de traitement auxiliaires comprennent des dispositions traitant des conditions environnementales du site auxiliaire, des règles d'accès, des exigences de protection environnementale et physique et de la coordination du transfert et de l'affectation du personnel. Les plans d'urgence font état d'exigences attribuées à des sites de traitement auxiliaires précis afin que les organisations maintiennent les fonctions essentielles liées à la mission et aux activités de l'organisation en dépit de toute perturbation, compromission ou défaillance des systèmes organisationnels.

CP-07(01) — Séparation du site principal (---)

Énoncés :

Identifier un site de traitement auxiliaire suffisamment distinct du site principal afin de réduire sensiblement l'exposition aux mêmes menaces.

Responsable : Aucun

Discussion :

Les menaces auxquelles sont susceptibles les sites de traitement auxiliaires sont définies dans les évaluations des risques de l'organisation et comprennent les désastres naturels, les défaillances structurales, les cyberattaques hostiles et les erreurs par omission ou par action. Les organisations déterminent la distance géographique suffisante entre les sites de traitement principaux et auxiliaires en fonction des types de menaces auxquelles elles font face. Dans le cas de menaces comme des attaques hostiles, la séparation entre les sites est moins pertinente.

CP-07(02) — Accessibilité (---)

Énoncés :

Identifier les problèmes d'accessibilité potentiels des sites traitement auxiliaires dans l'éventualité d'une perturbation ou d'un désastre majeurs et énoncer des mesures d'atténuation explicites.

Responsable : Aucun

Discussion :

Les perturbations touchant à toute la région sont des perturbations dont l'étendue géographique est vaste. Une organisation doit identifier elle-même les problèmes d'accessibilité en fonction de son évaluation des risques.

CP-07(03) — Priorité de service (---)

Énoncés :

Élaborer, pour le site de traitement auxiliaire, des conventions qui prévoient des dispositions de priorité de service conformément aux exigences d'accessibilité (y compris les objectifs de délai de récupération).

Responsable : Aucun

Discussion :

Les conventions de priorité de services sont des ententes négociées avec des fournisseurs de services pour veiller à ce que l'organisation reçoive une priorité de service qui reflète ses exigences d'accessibilité et la disponibilité des ressources d'information pour le traitement de secours logique ou au site de traitement auxiliaire physique. Les organisations établissent des objectifs de délai de rétablissement dans le cadre de la planification d'urgence.

CP-07(04) — Préparation en vue de l’utilisation (---)

Énoncés :

Préparer le site de traitement auxiliaire de manière à ce qu’il serve comme site opérationnel pour le traitement des fonctions opérationnelles et de mission essentielles.

Responsable : Aucun

Discussion :

La préparation du site auxiliaire comprend de déterminer les paramètres de configuration des systèmes de sorte qu’ils correspondent aux exigences établies au site principal; d’approvisionner le site des fournitures essentielles; de veiller à mettre en place tous les éléments de logistique.

CP-07(05) — Protections équivalentes de sécurité de l'information (---)

Énoncés :

Annulé : Intégré au contrôle CP-07.

Responsable : Aucun

CP-07(06) — Impossibilité de retourner au site principal (---)

Énoncés :

Planifier et se préparer pour des circonstances qui empêchent de retourner au site de traitement principal.

Responsable : Aucun

Discussion :

Il peut y avoir des situations qui empêchent une organisation de retourner au site de traitement principal, comme si une catastrophe naturelle (inondation ou ouragan, par exemple) endommageait ou détruisait une installation et qu'il avait été déterminé qu'il n'était pas prudent de reconstruire l'installation au même endroit.

CP-08 — Services de télécommunications (---)

Énoncés :

Établir des services de télécommunications de secours, y compris les conventions nécessaires pour permettre la reprise de [Affectation : opérations des systèmes désignés par l'organisation] pour les fonctions opérationnelles et de mission essentielles dans [Affectation : délais définis par l'organisation] lorsque les capacités de télécommunications de première ligne ne sont pas accessibles aux sites de stockage ou de traitement principaux ou auxiliaires.

Responsable : Aucun

Discussion :

Les services de télécommunications (pour les données et la voix) pour les sites de traitement et de stockage principaux et auxiliaires sont dans la portée du contrôle CP-

08. Les services de télécommunications de secours répondent aux exigences de continuité des activités établies dans les plans de secours et permettent le maintien des fonctions essentielles liées à la mission et aux activités de l'organisation en dépit de la perte des services de télécommunications principaux. Les organisations peuvent préciser des délais différents pour les sites principaux ou auxiliaires. Les services de télécommunications de secours comprennent des lignes ou circuits terrestres commerciaux, des approches au niveau du réseau pour les télécommunications, ou l'utilisation de satellites. Les organisations tiennent compte de facteurs comme la disponibilité, la qualité de service et l'accès lorsqu'elles signent des conventions de télécommunications de secours.

CP-08(01) — Dispositions de priorité de service (---)

Énoncés :

a. Élaborer des conventions de services de télécommunications de première ligne et de secours qui prévoient des dispositions de priorité de service conformément aux exigences d'accessibilité (y compris les objectifs de délai de récupération)
b. Demander un accès prioritaire à la composition pour tous les services de télécommunications utilisés dans le cadre de préparatifs d'urgence en cas d'événement portant atteinte à la sécurité nationale dans l'éventualité où les services de télécommunications principaux ou de secours sont assurés par une entreprise de télécommunications

Responsable : Aucun

Discussion :

Les organisations devraient évaluer l'incidence possible sur les opérations et la mission si les fournisseurs de services de télécommunications offrent des services à d'autres organisations ayant des dispositions de priorité de service semblables.

CP-08(02) — Points de défaillance uniques (---)

Énoncés :

Obtenir les services de télécommunication de secours pour réduire la probabilité de partage d'un point de défaillance unique avec les services de télécommunication de première ligne.

Responsable : Aucun

Discussion :

Dans certains cas, les fournisseurs de services de télécommunications ou les services peuvent partager les mêmes lignes physiques, ce qui augmente la vulnérabilité d'un point de défaillance unique. Il est important d'assurer la transparence du fournisseur pour ce qui est des réelles capacités de transmission physique pour les services de télécommunications.

CP-08(03) — Séparation des fournisseurs principaux et auxiliaires (---)

Énoncés :

Obtenir des services de télécommunications de secours auprès de fournisseurs distincts des fournisseurs principaux afin de réduire la vulnérabilité aux mêmes menaces.

Responsable : Aucun

Discussion :

Les menaces auxquelles font face les services de télécommunications sont définies dans les évaluations des risques de l'organisation et comprennent les désastres naturels, les défaillances structurales, les attaques cyberphysiques et les erreurs par omission ou par action. Les organisations peuvent réduire les vulnérabilités communes en minimisant l'utilisation, par les fournisseurs de services de télécommunications, d'une infrastructure partagée et en sélectionnant des services ayant une séparation géographique adéquate. Les organisations peuvent considérer l'utilisation d'un seul fournisseur de services lorsque celui-ci peut fournir des services de télécommunications de secours qui répondent aux exigences de séparation établies dans l'évaluation des risques.

CP-08(04) — Plan d'urgence des fournisseurs (---)

Énoncés :

a. Exiger des fournisseurs de services de télécommunications de première ligne et de secours qu'ils possèdent des plans d'urgence
b. Examiner les plans d'urgence des fournisseurs pour s'assurer que ces plans répondent aux exigences de l'organisation en matière d'urgence
c. Obtenir des preuves des tests du plan d'urgence et des formations de la part des fournisseurs [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

L'examen des plans d'urgence des fournisseurs devrait tenir compte du caractère exclusif de ces plans. Un résumé des plans d'urgence des fournisseurs peut parfois constituer une preuve suffisante des plans d'urgence et satisfaire à l'exigence d'examen.

CP-08(05) — Test des services de télécommunications de secours (---)

Énoncés :

Tester les services de télécommunications de secours [Affectation : fréquence définie par l'organisation].

Responsable : Aucun

Discussion :

La mise à l'essai des services de télécommunications de secours se fait par le biais d'ententes contractuelles avec les fournisseurs de services. Les tests peuvent être effectués parallèlement aux activités normales pour assurer qu'il n'y a pas de dégradation des fonctions liées à la mission ou aux activités de l'organisation.

CP-09 — Sauvegarde du système (Nc--)

Énoncés :

a. Effectuer des sauvegardes des données utilisateur contenues dans le système [Affectation : composants de système définis par l'organisation] [Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise]
b. Effectuer des sauvegardes des données système contenues dans le système [Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise]
c. Effectuer des sauvegardes de la documentation liée au système d'information, y compris la documentation sur la sécurité et la protection de la vie privée [Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise]
d. Protéger la confidentialité, l'intégrité et la disponibilité de l'information de sauvegarde a
a. L'organisation détermine les périodes de conservation de l'information opérationnelle essentielle et des sauvegardes archivées

Responsable : Aucun

Discussion :

L'information système comprend l'information d'état, les logiciels du système d'exploitation, les intergiciels, les logiciels d'application, de même que les licences. L'information utilisatrice ou utilisateur comprend l'information qui n'est pas de l'information système. Les mécanismes utilisés pour la protection de l'intégrité des sauvegardes des systèmes comprennent les signatures numériques et le hachage cryptographique. La protection de l'information sur les sauvegardes système en transit est abordée dans les contrôles MP-05 et SC-

08. Les sauvegardes de systèmes répondent aux exigences établies dans les plans d'urgence ainsi qu'aux exigences organisationnelles concernant la sauvegarde d'information. Les organisations peuvent être assujetties aux lois, aux décrets, aux directives, aux règlements ou aux politiques applicables concernant des catégories particulières de renseignements (par exemple, les renseignements médicaux). Le personnel de l'organisation consulte la haute ou le haut fonctionnaire ou cadre supérieure ou supérieur et la conseillère ou le conseiller juridique en matière de protection de la vie privée concernant de telles exigences.

CP-09(01) — Tests de fiabilité et d'intégrité (---)

Énoncés :

Effectuer des tests de l'information de sauvegarde [Affectation : fréquence définie par l'organisation] pour vérifier la fiabilité des supports et l'intégrité de l'information.

Responsable : Aucun

Discussion :

Les organisations doivent avoir l'assurance que l'information de sauvegarde peut être récupérée de manière fiable. La fiabilité concerne les systèmes et les composants des systèmes dans lesquels l'information de sauvegarde est stockée, les opérations utilisées pour récupérer l'information, et l'intégrité de l'information faisant l'objet de la récupération. Des tests indépendants et spécialisés peuvent être utilisés pour chacun des aspects de la fiabilité. Par exemple, décrypter et transporter (ou transmettre) un échantillon aléatoire de fichiers de sauvegarde du site de sauvegarde ou de stockage auxiliaire et comparer l'information à la même information au site de traitement principal peut procurer une telle assurance.

CP-09(02) — Essai de restauration au moyen de l'échantillonnage (---)

Énoncés :

Utiliser un échantillon de l'information de sauvegarde pour restaurer certaines fonctions du système dans le cadre des tests du plan d'urgence.

Responsable : Aucun

Discussion :

Les organisations doivent avoir l'assurance que les fonctions du système peuvent être récupérées correctement et qu'elles peuvent appuyer les missions organisationnelles établies. Pour s'assurer que les fonctions de système sélectionnées sont exécutées minutieusement pendant les tests relatifs au plan d'urgence, un échantillonnage de l'information de sauvegarde est récupéré afin de déterminer si les fonctions fonctionnent comme prévu. Les organisations peuvent déterminer la taille de l'échantillon pour les fonctions et l'information de sauvegarde en fonction du niveau d'assurance nécessaire.

CP-09(03) — Stockage distinct pour l'information essentielle (---)

Énoncés :

Conserver des copies de sauvegarde [Affectation : information liée à la sécurité et aux logiciels des systèmes essentiels définis par l'organisation], dans une installation distincte ou un conteneur résistant au feu situé hors de l'emplacement du système opérationnel.

Responsable : Aucun

Discussion :

Un stockage distinct pour l'information essentielle s'applique à toute l'information essentielle indépendamment du type de support de stockage de sauvegarde. Les logiciels des systèmes essentiels comprennent les systèmes d'exploitation, les systèmes de gestion de clés cryptographiques et les systèmes de détection d'intrusions. L'information liée à la sécurité comprend les inventaires de composants matériels, logiciels et micrologiciels des systèmes. Les sites de stockage auxiliaires, y compris les architectures réparties dans d'autres régions, servent à titre d'installation de stockage distincte pour les organisations. Les organisations peuvent fournir des stockages distincts en mettant en oeuvre des processus de sauvegarde automatisés dans des sites de stockage de auxiliaires (par exemple, des centres de données). La Gendarmerie royale du Canada (GRC) établit des normes et des spécifications relatives à la sécurité et aux conteneurs résistant au feu.

CP-09(04) — Protection contre une modification non autorisée (---)

Énoncés :

Annulé : Intégré au contrôle CP-09.

Responsable : Aucun

CP-09(05) — Transfert vers un site de stockage auxiliaire (---)

Énoncés :

Transférer l'information de sauvegarde du système dans un site de stockage auxiliaire [Affectation : délais et taux de transfert définis par l'organisation et conformes aux objectifs de délai et de point de reprise].

Responsable : Aucun

Discussion :

L'information de stockage de sauvegarde du système peut être transférée vers des sites de stockage auxiliaires de manière électronique ou par envoi physique du support de stockage, veillant au respect des protocoles de sécurité pour le traitement et la transmission.

CP-09(06) — Système secondaire redondant (---)

Énoncés :

Effectuer la sauvegarde du système au moyen d'un système secondaire redondant n'étant pas situé au même endroit que le système principal et pouvant être activé sans perte d'information ou perturbation des opérations.

Responsable : Aucun

Discussion :

L'effet de la sauvegarde du système peut s'obtenir au moyen d'un système secondaire redondant qui reflète le système principal, y compris la duplication de l'information. Si ce type de redondance est en place et s'il y a une séparation géographique adéquate entre les deux systèmes, le système secondaire peut également servir de site de traitement auxiliaire.

CP-09(07) — Double autorisation pour la suppression ou la destruction (---)

Énoncés :

Appliquer l'exigence de double autorisation pour la suppression ou la destruction [Affectation : information de sauvegarde définie par l'organisation].

Responsable : Aucun

Discussion :

La double autorisation fait en sorte qu'il est impossible de supprimer ou de détruire l'information de sauvegarde à moins que deux personnes qualifiées le fassent. Les personnes responsables de la suppression ou de la destruction de l'information de sauvegarde détiennent les compétences nécessaires pour déterminer si la suppression ou la destruction de l'information de sauvegarde respecte les stratégies et les procédures organisationnelles. La double autorisation est également appelée le contrôle par deux personnes. Pour réduire le risque de collusion, les organisations considèrent la rotation des tâches à double autorisation avec d'autres particuliers.

CP-09(08) — Protection cryptographique (---)

Énoncés :

Appliquer des mécanismes cryptographiques pour empêcher la divulgation et la modification non autorisées de [Affectation : l'information de sauvegarde définie par l'organisation].

Responsable : Aucun

Discussion :

La sélection des mécanismes cryptographiques se fonde sur le besoin de protéger la confidentialité et l'intégrité de l'information sauvegardée. La robustesse des mécanismes sélectionnés correspond à la catégorie de sécurité et à la classification de l'information. La protection cryptographique s'applique à l'information de sauvegarde du système en stockage dans l'emplacement principal et d'autres emplacements. Les organisations qui mettent en oeuvre des mécanismes cryptographiques dans le but de protéger l'information inactive envisagent également les solutions de gestion de clés cryptographiques.

CP-10 — Reprise et reconstitution du système (---)

Énoncés :

S'occuper de rendre à un état connu la reprise et la reconstitution du système dans [Affectation : un délai conforme aux objectifs de délai et de point de reprise définis par l'organisation] après une perturbation, une compromission ou une défaillance du système.

Responsable : Aucun

Discussion :

La reprise consiste à exécuter les activités du plan d'urgence pour restaurer les fonctions liées à la mission et aux activités de l'organisation. La reconstitution suit la reprise et englobe les activités de restauration des systèmes à un état opérationnel complet. Les opérations de reprise et de reconstitution correspondent aux priorités opérationnelles et de la mission, aux objectifs de délai ou de point de reprise et de reconstitution, ainsi qu'aux paramètres organisationnels lesquels sont conformes aux exigences du plan d'urgence. La reconstitution inclut la désactivation de toute capacité intérimaire du système qui aurait pu servir durant les opérations de reprise. Elle comprend également des évaluations des capacités des systèmes restaurés, du rétablissement des activités de surveillance continue, de la réautorisation du système (le cas échéant), et des activités visant à préparer le système et l'organisation à l'éventualité de perturbations, de violations, de compromissions ou de défaillances. Les capacités de reprise et de reconstitution peuvent comprendre des mécanismes automatiques et des procédures manuelles. Les organisations établissent des objectifs de délai de rétablissement et de point de rétablissement dans le cadre de la planification d'urgence.

CP-10(01) — Tests relatifs au plan d’urgence (---)

Énoncés :

Annulé : Intégré au contrôle CP-04.

Responsable : Aucun

CP-10(02) — Reprise des transactions (---)

Énoncés :

Appliquer un processus de reprise des transactions pour les systèmes de traitement transactionnel.

Responsable : Aucun

Discussion :

Les systèmes transactionnels comprennent les systèmes de gestion des bases de données et les systèmes de traitement des transactions. Les mécanismes d'annulation et de journalisation de transactions comprennent des mécanismes à l'appui de la reprise de transactions.

CP-10(03) — Contrôles de sécurité compensatoires (---)

Énoncés :

Annulé : Traité par adaptation.

Responsable : Aucun

CP-10(04) — Restauration dans les délais précisés (---)

Énoncés :

Assurer la capacité permettant de rétablir les composants du système en dedans de [Affectation : délais de restauration définis par l'organisation] en utilisant l'information dont la configuration est contrôlée et l'intégrité, protégée représentant les composants dans un état sécurisé et opérationnel.

Responsable : Aucun

Discussion :

La restauration des composants des systèmes comprend le reformatage, lequel restaure les composants à un état opérationnel connu.

CP-10(05) — Capacité de basculement (---)

Énoncés :

Annulé : Intégré au contrôle SI-13.

Responsable : Aucun

CP-10(06) — Protection des composants (---)

Énoncés :

Protéger les composants du système utilisés pour la reprise et la reconstitution.

Responsable : Aucun

Discussion :

La protection des composants de la reprise et de la reconstitution du système (c'est-à-dire composants matériels, logiciels et micrologiciels) comprend les contrôles physiques et techniques. Les composants de sauvegarde et de restauration utilisés pour la reprise et la reconstitution comprennent les routeurs, les compilateurs et d'autres systèmes logiciels.

CP-11 — Protocoles de communications de secours (---)

Énoncés :

Permettre l'utilisation [Affectation : protocoles de communications de secours définis par l'organisation] afin de maintenir la continuité des opérations.

Responsable : Aucun

Discussion :

Les plans de secours, ainsi que la formation et les tests liés aux plans, intègrent la capacité de protocoles de communications de secours dans le cadre du renforcement de la résilience des systèmes organisationnels. L'utilisation d'un différent protocole de communications peut perturber les applications logicielles et les aspects opérationnels des systèmes. Les organisations évaluent les effets secondaires de l'introduction de protocoles de communications de secours avant la mise en oeuvre de cette mesure.

CP-12 — Mode sans échec (---)

Énoncés :

Le système passe au mode sans échec [Affectation : contraintes du mode d'opération sans échec définies par l'organisation] lorsqu'il détecte [Affectation : conditions définies par l'organisation].

Responsable : Aucun

Discussion :

Lorsque les systèmes sont utilisés pour exécuter des fonctions liées à la mission et aux activités de l'organisation, y compris les opérations militaires, les activités spatiales civiles, l'exploitation de centrales nucléaires et les activités de contrôle de la circulation aérienne (surtout lorsqu'il s'agit d'environnements opérationnels en temps réel), les organisations peuvent choisir de déterminer quelles conditions entraîneront un passage au mode d'opération sans échec prédéfini. Le mode d'opération sans échec, lequel peut être déclenché manuellement ou automatiquement, limite les opérations qu'un système peut exécuter si certaines conditions sont présentes. Le système pourrait forcer une réduction de l'alimentation ou de la bande passante avant de permettre l'exécution de certaines fonctions.

CP-13 — Mécanismes de sécurité de secours (---)

Énoncés :

Utiliser [Affectation : mécanismes de sécurité de secours ou additionnels définis par l'organisation] en vue d'exécuter [Affectation : fonctions de sécurité définies par l'organisation] lorsque le mode principal d'exécution de la fonction de sécurité est compromis ou n'est pas disponible.

Responsable : Aucun

Discussion :

L'utilisation de mécanismes de sécurité de secours soutient la résilience des systèmes, la planification d'urgence et la continuité des opérations. Afin de veiller à la continuité des opérations et de la mission, les organisations peuvent mettre en oeuvre des mécanismes de sécurité de secours ou additionnels. Ces mécanismes pourraient être moins efficaces que les mécanismes primaires. Toutefois, la facilité d'accès aux mécanismes additionnels ou de secours rehausse la capacité d'une organisation d'assurer la continuité de la mission et des opérations qui pourraient être touchées si l'organisation devait suspendre ses opérations jusqu'à la reprise du mode d'exécution primaire des fonctions. Étant donné le coût et l'effort global requis pour assurer de telles capacités de secours, les mécanismes additionnels ou de secours ne s'appliquent qu'aux fonctions de sécurités critiques assurées par les systèmes, les composants du système ou les services de systèmes. Une organisation pourrait, par exemple, donner un carnet de clés à usage unique aux cadres supérieures et supérieurs, aux responsables et aux administratrices et administrateurs de systèmes leur permettant d'être authentifiés de manière sûre au cas où il y avait une compromission du mode d'authentification habituel de l'organisation.

IA

Contrôle de l’identité et de l’authentification

Identification and Authentication

IA-01 — Politique et procédures d'identification et d'authentification (---)

Énoncés :

a. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :

1. une politique d'identification et d'authentification [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, à la jurisprudence, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables

2. des procédures pour faciliter la mise en oeuvre de la politique d'identification et d'authentification ainsi que des contrôles d'identification et d'authentification

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures d'identification et d'authentification

c. Passer en revue et mettre à jour, par rapport à l'identification et l'authentification :

1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La politique et les procédures d'identification et d'authentification abordent les contrôles de la famille IA qui ont été mis en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement des telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à l'élaboration de la politique et des procédures d'identification et d'authentification. En règle générale, les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin pour des politiques et des procédures propres à la mission ou au système. La politique peut être intégrée à la politique générale de sécurité et de protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures d'identification et d'authentification comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, y compris ceux liés au respect de la vie privée, et des changements apportés aux lois, à la jurisprudence, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle. La Loi sur la protection des renseignements personnels dans le secteur privé prévoit une mesure exceptionnelle qui stipule que le nom et les coordonnées des personnes au travail ne sont pas considérés comme étant des renseignements personnels.

IA-02 — Identification et authentification (utilisatrices et utilisateurs de l'organisation) (---)

Énoncés :

Identifier de façon unique et authentifier les utilisatrices et utilisateurs organisationnels, puis associer cet identifiant unique aux processus agissant en leur nom.

Responsable : Aucun

Discussion :

Les utilisatrices et utilisateurs organisationnels comprennent les employées, les employés ou les personnes dont le statut est considéré par leur organisation comme étant équivalent à celui d'une employée ou un employé (par exemple, entrepreneures, entrepreneurs et chercheuses et chercheurs invités). L'identification unique et l'authentification des utilisatrices et utilisateurs s'appliquent à tous les accès autres que ceux qui sont explicitement mentionnés dans le contrôle AC-14 et qui s'effectuent dans le cadre de l'utilisation autorisée d'authentifiants de groupe sans nécessiter d'authentification individuelle. Puisque les processus sont exécutés au nom de groupes et de rôles, les organisations peuvent exiger l'identification individuelle de chacune des personnes appartenant à un compte de groupe pour rendre compte en détail des activités qu'elle mène sur le système. Les organisations utilisent des mots de passe, des authentifiants physiques ou la biométrie pour authentifier les identités d'utilisateur, ou encore une combinaison de ces méthodes pour l'authentification multifacteur (AMF). Les justificatifs d'identité et les authentifiants biométriques peuvent à l'occasion être considérés comme étant des renseignements personnels. Afin de considérer le concept de la nécessité du point de vue de la protection de la vie privée par rapport à sa proportionnalité, les organisations doivent collecter juste assez de renseignements personnels pour garantir une authentification précise. L'accès aux systèmes organisationnels est soit local, soit réseau. Par accès local, on entend tout accès à des systèmes de l'organisation, par des utilisatrices ou utilisateurs ou par un processus exécuté en leur nom, effectué par l'entremise d'une connexion directe, sans recours à un réseau. L'accès réseau est tout accès aux systèmes organisationnels, par des utilisatrices ou utilisateurs ou un processus exécuté au nom de ces derniers, effectué au moyen de connexions réseau (c'est-à-dire des accès non locaux). L'accès à distance est un type d'accès réseau qui requiert une communication au moyen de réseaux externes. Les réseaux internes incluent les réseaux locaux et les réseaux élargis. Les RPV chiffrés utilisés pour établir des connexions réseau entre des points terminaux contrôlés par l'organisation et des points terminaux contrôlés par une autre entité peuvent être traités comme des réseaux internes du point de vue de protection de la confidentialité et de l'intégrité de l'information transmise sur ces réseaux. Les exigences d'identification et d'authentification pour des utilisatrices et utilisateurs non organisationnels sont décrites dans le contrôle IA-08.

IA-02(01) — AMF robustes pour les comptes privilégiés (Nc--)

Énoncés :

Appliquer des AMF robustes pour l'accès à des comptes privilégiés.

Responsable : Aucun

Discussion :

L'authentification multifactorielle (AMF) exige l'utilisation de deux facteurs différents ou plus aux fins d'authentification. Les facteurs d'authentification sont définis comme suit : une information connue (par exemple, un numéro d'identification personnel [NIP]), une possession (par exemple, un authentifiant physique comme une clé cryptographique privée) ou un attribut personnel (par exemple, une authentification biométrique). Les solutions d'AMF qui présentent des authentifiants physiques comprennent les authentifiants matériels qui fournissent des sorties à durée limitée ou de type défi-réponse ainsi que des cartes à puce. En plus de permettre l'authentification des utilisatrices et utilisateurs au niveau du système (c'est-à-dire, au moment de l'ouverture de session), les organisations peuvent utiliser des mécanismes d'authentification au niveau de l'application, à leur discrétion, pour accroître la sécurité. Quel que soit le type d'accès (c'est-à-dire, local, réseau, à distance), les comptes privilégiés sont authentifiés au moyen d'options d'authentification multifacteur adéquates pour le niveau de risque. Les organisations peuvent ajouter des mesures de sécurité, comme des mécanismes d'authentification supplémentaires et plus rigoureux pour des types d'accès spécifiques.

IA-02(02) — AMF pour comptes non privilégiés (Nc--)

Énoncés :

Appliquer l'AMF pour l'accès à des comptes non privilégiés.

Responsable : Aucun

Discussion :

L'authentification multifactorielle (AMF) exige l'utilisation de deux facteurs différents ou plus aux fins d'authentification. Les facteurs d'authentification sont définis comme suit : une information connue (par exemple, un NIP), une possession (par exemple, un authentifiant physique comme une clé cryptographique privée) ou un attribut personnel (par exemple, une authentification biométrique). Les solutions d'AMF qui présentent des authentifiants physiques comprennent les authentifiants matériels qui fournissent des sorties à durée limitée ou de type défi-réponse ainsi que des cartes à puce. En plus d'authentifier les utilisatrices et utilisateurs au niveau du système, les organisations peuvent également, à leur discrétion, avoir recours à des mécanismes d'authentification au niveau de l'application pour accroître la sécurité de l'information. Quel que soit le type d'accès (c'est-à-dire, local, réseau, à distance), les comptes privilégiés sont authentifiés au moyen d'options d'authentification multifacteur adéquates pour le niveau de risque. Les organisations peuvent fournir des mesures de sécurité, comme des mécanismes d'authentification supplémentaires et plus rigoureux pour des types d'accès spécifiques.

IA-02(03) — Accès local aux comptes privilégiés (---)

Énoncés :

Annulé : Intégré au contrôle IA-02(01).

Responsable : Aucun

IA-02(04) — local aux comptes non privilégiés (---)

Énoncés :

Annulé : Intégré au contrôle IA-02(02).

Responsable : Aucun

IA-02(05) — Authentification individuelle avec authentification de groupe (---)

Énoncés :

Lorsque des authentifiants ou des comptes partagés sont utilisés, il faut que les utilisatrices et utilisateurs soient authentifiés individuellement avant d'obtenir l'accès aux ressources ou aux comptes partagés.

Responsable : Aucun

Discussion :

L'authentification individuelle avant l'authentification de groupe a pour effet d'atténuer le risque lié à l'utilisation de comptes de groupe et d'authentifiants.

IA-02(06) — Accès aux comptes – Dispositif distinct (---)

Énoncés :

Mettre en oeuvre l'AMF pour l'accès [Sélection (un choix ou plus) : local; réseau; à distance] aux [Sélection (un choix ou plus) : comptes privilégiés; comptes non privilégiés] de façon à ce que :
a. l'un des facteurs soit fourni par un dispositif distinct du système qui obtient un accès
b. le dispositif satisfasse [Affectation : exigences de la force du mécanisme définies par l'organisation]

Responsable : Aucun

Discussion :

Il est possible de réduire la probabilité de compromission des justificatifs d'authentification stockés sur le système auquel l'utilisatrice ou utilisateur accède en exigeant l'utilisation, pour un des facteurs lors d'une authentification multifactorielle, d'un dispositif distinct du système. Les adversaires peuvent avoir des exploits axés sur les dispositifs d'extrémité qui leur permettent de compromettre de tels secrets et par la suite d'usurper l'identité d'utilisatrices et utilisateurs autorisés. Appliquer l'un de ces facteurs sur un dispositif distinct (par exemple, un jeton d'authentification matériel), ajoute des éléments matériels qui renforcent le mécanisme et un niveau d'assurance accru au processus d'authentification en demandant aux exploits hétérogènes de compromettre simultanément les secrets traités par le dispositif d'extrémité et par le dispositif distinct. À l'occasion, l'utilisation d'un dispositif distinct peut impliquer la collecte de renseignements personnels comme la biométrie. Afin de considérer le concept de la nécessité du point de vue de la protection de la vie privée par rapport à sa proportionnalité, les organisations doivent collecter juste assez de renseignements personnels pour garantir une authentification précise.

IA-02(07) — Accès réseau aux comptes non privilégiés – Dispositif distinct (---)

Énoncés :

Annulé : Intégré au contrôle IA-02(06).

Responsable : Aucun

IA-02(08) — Accès aux comptes – Résistant à la réinsertion (---)

Énoncés :

Mettre en oeuvre des mécanismes d'authentification résistant à la réinsertion pour l'accès aux [Sélection (un choix ou plus) : comptes privilégiés; comptes non privilégiés].

Responsable : Aucun

Discussion :

Les processus d'authentification résistent aux attaques par réinsertion lorsqu'il n'est pas pratique de réaliser une authentification réussie en réinsérant un message d'authentification antérieur. Les techniques résistant à la réinsertion incluent les protocoles qui utilisent des nonces ou des défis, comme des authentifiants à usage unique synchrones ou cryptographiques.

IA-02(09) — Accès réseau aux comptes non privilégiés – Résistance à la réinsertion (---)

Énoncés :

Annulé : Intégré au contrôle IA-02(08).

Responsable : Aucun

IA-02(10) — Authentification unique (---)

Énoncés :

Offrir une fonctionnalité d'authentification unique des [Affectation : services et comptes du système définis par l'organisation].

Responsable : Aucun

Discussion :

L'authentification unique permet aux utilisatrices et utilisateurs d'ouvrir une session une seule fois et d'accéder à multiples ressources du système. Les organisations doivent évaluer l'efficacité opérationnelle offerte par la fonctionnalité d'authentification unique ainsi que l'augmentation du risque en accordant l'accès à plusieurs systèmes par un événement d'authentification unique. L'authentification unique peut présenter des occasions de renforcer la sécurité du système, par exemple en offrant la capacité d'ajouter l'AMF aux applications et aux systèmes (existants et nouveaux) qui pourraient ne pas être en mesure de prendre en charge nativement l'AMF.

IA-02(11) — Accès à distance – Dispositif distinct (---)

Énoncés :

Annulé : Intégré au contrôle IA-02(06).

Responsable : Aucun

IA-02(12) — Utilisation de jeton matériel basé sur des justificatifs d'identité d'ICP (---)

Énoncés :

Accepter et vérifier électroniquement le jeton matériel basé sur des justificatifs d'identité d'ICP.

Responsable : Aucun

IA-02(13) — Authentification hors bande (---)

Énoncés :

Mettre en oeuvre les mécanismes d'authentification hors bande suivants en vertu des [Affectation : conditions définies par l'organisation] : [Affectation : authentification hors bande définie par l'organisation].

Responsable : Aucun

Discussion :

Par authentification hors bande, on entend l'utilisation de deux chemins de communication distincts pour identifier et authentifier les utilisatrices et utilisateurs ou les dispositifs auprès d'un système d'information. Le premier chemin (c'est-à-dire le chemin en bande) sert à identifier et authentifier les utilisatrices et utilisateurs ou les dispositifs, et est généralement le chemin par lequel est transmise l'information. Le deuxième chemin (c'est-à-dire le chemin hors bande) sert à vérifier l'authentification de manière indépendante et à demander une action. Par exemple, une utilisatrice ou un utilisateur est authentifié au moyen d'un ordinateur portatif auprès d'un serveur à distance auquel l'utilisateur veut accéder et auquel il transmet une demande d'action en employant le même chemin de communication. Le serveur communique ensuite avec l'utilisatrice ou utilisateur au moyen de son téléphone cellulaire afin de confirmer que l'action demandée provenait de l'utilisateur. L'utilisatrice ou utilisateur peut confirmer l'action demandée directement à la personne l'ayant appelé, ou il peut fournir un code d'authentification au téléphone. Ce type d'authentification hors bande peut être utilisé pour atténuer les attaques par interception réelles ou soupçonnées. Les conditions ou critères d'activation peuvent inclure des activités suspectes, de nouveaux indicateurs de menace, des niveaux de menace élevés, l'incidence d'une divulgation ou le niveau de classification de l'information transmise par les transactions.

IA-02(400) — AMF pour accès à distance aux comptes privilégiés (---)

Énoncés :

Annulé : Intégré aux contrôles IA-02(01) et IA-02(06).

Responsable : Aucun

IA-03 — Identification et authentification des dispositifs (---)

Énoncés :

Identifier et authentifier, de manière unique [Affectation : dispositifs ou types de dispositifs définis par l'organisation] avant d'établir une connexion [Sélection (un choix ou plus) : locale; à distance; réseau].

Responsable : Aucun

Discussion :

Les dispositifs qui exigent une identification et une authentification dispositif à dispositif unique sont définis en fonction du type, du dispositif ou d'une combinaison des deux. Les types de dispositifs définis par l'organisation incluent les dispositifs qui n'appartiennent pas à l'organisation. Les systèmes utilisent de l'information connue partagée (par exemple, des adresses MAC ou Transmission Control Protocol/Internet Protocol [TCP/IP]) pour l'identification des dispositifs ou encore des solutions d'authentification organisationnelles (par exemple, les protocoles Institute of Electrical and Electronics Engineers [IEEE] 802.1x et Extensible Authentication Protocol [EAP], un serveur RADIUS avec l'authentification EAP-TLS ou Kerberos) pour identifier et authentifier les dispositifs sur les réseaux locaux et étendus. Les organisations déterminent la robustesse requise des mécanismes d'authentification en fonction des catégories de sécurité des systèmes et des exigences liées à la mission et aux activités. Compte tenu des défis posés par la mise en oeuvre à grande échelle de l'authentification des dispositifs, les organisations peuvent restreindre l'application du contrôle à un nombre limité ou à un type de dispositifs selon les besoins liés à la mission ou aux activités

IA-03(01) — Authentification bidirectionnelle cryptographique (---)

Énoncés :

Authentifier [Affectation : dispositifs ou types de dispositifs définis par l'organisation] avant d'établir une connexion [Sélection (un choix ou plus) : locale; à distance; réseau] utilisant l'authentification bidirectionnelle reposant sur la cryptographie.

Responsable : Aucun

Discussion :

Une connexion locale est toute connexion à un dispositif communiquant sans utiliser de réseau. Une connexion réseau est toute connexion à un dispositif communiquant par un réseau. Une connexion distante est toute connexion effectuée à un appareil communiquant au moyen d'un réseau externe. L'authentification bidirectionnelle offre des mesures de protection plus robustes afin de valider l'identité d'autres dispositifs pour les connexions comportant un risque plus élevé.

IA-03(02) — Authentification réseau bidirectionnelle cryptographique (---)

Énoncés :

Annulé : Intégré au contrôle IA-03(01).

Responsable : Aucun

IA-03(03) — Attribution dynamique des adresses (---)

Énoncés :

a. Où les adresses sont attribuées de manière dynamique, l'information de location de l'attribution dynamique des adresses ainsi que la durée de la location attribuée aux dispositifs conformément à [Affectation : information sur la location et durée de la location définies par l'organisation]
b. Vérifier l'information de location lorsqu'elle est attribuée à un dispositif

Responsable : Aucun

Discussion :

Le protocole DHCP (Dynamic Host Configuration Protocol) est un exemple de moyen par lequel la clientèle peut recevoir de manière dynamique des attributions d'adresses réseau.

IA-03(04) — Attestation de dispositifs (---)

Énoncés :

Traiter l'identification et l'authentification des dispositifs conformément à une attestation au moyen [Affectation : processus de gestion des configurations défini par l'organisation].

Responsable : Aucun

Discussion :

L'attestation des dispositifs signifie l'identification et l'authentification d'un dispositif en fonction de sa configuration et de son état d'exploitation connu. Cette attestation peut être déterminée au moyen d'un hachage cryptographique du dispositif. Si l'attestation d'un dispositif est le mode d'identification et d'authentification, il est important d'appliquer les correctifs et d'effectuer les mises à niveau du dispositif au moyen d'un processus de gestion des configurations pour assurer que l'application de correctifs et les mises à niveau soient effectuées de manière sûre et sans perturber l'identification et l'authentification des autres dispositifs.

IA-04 — Gestion des identifiants (---)

Énoncés :

Gérer les identifiants de système des façons suivantes :
a. recevoir une autorisation de [Affectation : personnel ou rôles de l'organisation] pour attribuer un identifiant à une personne, à un groupe, à un rôle, à un service ou à un dispositif
b. sélectionner et déterminer un identifiant qui identifie une personne, un groupe, un rôle, un service ou un dispositif
c. attribuer l'identifiant à la personne, au groupe, au rôle, au service ou au dispositif prévu
d. prévenir la réutilisation d'identifiant pendant [Affectation : délai défini par l'organisation]

Responsable : Aucun

Discussion :

Les identifiants de dispositif courants comprennent les adresses MAC ou IP, ou les identifiants à jeton unique. La gestion des identifiants de personnes ne s'applique pas aux comptes de systèmes partagés. En règle générale, les identifiants de personnes correspondent aux noms d'utilisateur des comptes de système qui leur ont été attribués. Dans une telle situation, les activités de gestion de compte du contrôle AC-2 utilisent les noms de comptes fournis par le contrôle IA-04. La gestion des identifiants porte également sur les identifiants de personnes qui ne sont pas nécessairement associés aux comptes du système. Le fait de prévenir la réutilisation d'identifiant empêche d'attribuer à une autre entité des identifiants utilisés précédemment par une personne, un groupe, un rôle, un service ou un dispositif. À l'occasion, la gestion des identifiants peut exiger la collecte de renseignements personnels. Afin de considérer le concept de la nécessité du point de vue de la protection de la vie privée par rapport à sa proportionnalité, les organisations doivent collecter juste assez de renseignements personnels pour garantir une authentification précise.

IA-04(01) — Interdire l’utilisation d’identifiants de compte en tant qu’identifiants publics (---)

Énoncés :

Interdire l’utilisation d’identifiants de compte du système qui sont les mêmes que les identifiants publics pour les comptes individuels.

Responsable : Aucun

Discussion :

L’interdiction d’utiliser des identifiants de compte comme identifiants publics s’applique à tout identifiant de compte divulgué publiquement utilisé pour les communications, comme les courriels ou la messagerie instantanée. L’interdiction d’utiliser des identifiants de compte pour les systèmes pareils à certains identifiants publics tels que les sections d’identifiants personnels des adresses de courriel rend plus difficile pour les adversaires de deviner les identifiants des utilisatrices et utilisateurs. L’interdiction d’utiliser des identifiants de compte comme identifiants publics sans la mise en oeuvre d’autres contrôles associés ne fait que compliquer la façon de deviner les identifiants. Des protections supplémentaires sont nécessaires pour que les authentifiants et les justificatifs d’identité protègent le compte.

IA-04(02) — Autorisation de superviseure ou superviseur (---)

Énoncés :

Annulé : Intégré au contrôle IA-12(01).

Responsable : Aucun

IA-04(03) — Multiples formes de certification (---)

Énoncés :

Annulé : Intégré au contrôle IA-12(02).

Responsable : Aucun

IA-04(04) — Établissement du statut d'une utilisatrice ou d'un utilisateur (---)

Énoncés :

Gérer les identifiants personnels en identifiant de façon unique chaque personne à titre de [Affectation : caractéristique définie par l'organisation identifiant le statut de la personne].

Responsable : Aucun

Discussion :

Les caractéristiques qui identifient le statut d'une personne comprennent les utilisatrices et utilisateurs entrepreneurs, de nationalité étrangère et non organisationnels. L'identification du statut d'une personne au moyen de ces caractéristiques offre des renseignements à propos des personnes avec lesquelles le personnel de l'organisation communique.

IA-04(05) — Gestion dynamique (---)

Énoncés :

Gérer de manière dynamique les identifiants conformément à la [Affectation : stratégie sur les identifiants dynamiques définie par l'organisation].

Responsable : Aucun

Discussion :

Contrairement aux approches conventionnelles d'identification qui supposent des comptes statiques pour les utilisatrices et utilisateurs préenregistrés, plusieurs systèmes distribués établissent les identifiants en temps réel des entités inconnues. Lorsque les identifiants sont établis en temps réel dans le cas des entités jusque-là inconnues, les organisations prévoient l'établissement dynamique d'identifiants. Il est essentiel de pouvoir compter sur des relations de confiance préétablies et des mécanismes dotés de pouvoirs appropriés pour valider les justificatifs d'identité et identifiants connexes.

IA-04(06) — Gestion interorganisationnelle (---)

Énoncés :

Collaborer avec les organisations externes suivantes pour la gestion interorganisationnelle des identifiants : [Affectation : organisations externes désignées par l'organisation].

Responsable : Aucun

Discussion :

La gestion interorganisationnelle d'identificateurs permet d'identifier des personnes, des groupes, des rôles ou des dispositifs lorsqu'elles mènent des activités interorganisationnelles concernant le traitement, le stockage ou la transmission d'informations.

IA-04(07) — Inscription en personne (---)

Énoncés :

Annulé : Intégré au contrôle IA-12(04).

Responsable : Aucun

IA-04(08) — Identifiants pseudonymes par paires (---)

Énoncés :

Générer des identifiants pseudonymes par paires.

Responsable : Aucun

Discussion :

Un identifiant pseudonyme par paires est un identifiant d'abonnée ou abonné impossible à trouver qui est généré par un fournisseur d'identité pour utilisation par une partie de confiance. Générer des identifiants pseudonymes distincts par paires sans information d'identification concernant une abonnée ou un abonné peut décourager le suivi et le profilage de l'activité de l'abonnée ou abonné au-delà des exigences opérationnelles établies par une organisation. Les identifiants pseudonymes par paires sont uniques en soi par rapport à chaque partie de confiance sauf dans les situations où les parties de confiance peuvent démontrer un lien tangible justifiant un besoin opérationnel de corrélation, ou dans les situations où toutes les parties consentent à être mises en corrélation de cette manière.

IA-04(09) — Maintenance et protection d'attributs (---)

Énoncés :

Maintenir les attributs de chaque personne, dispositif ou service identifié de manière unique dans [Affectation : stockage central protégé défini par l'organisation].

Responsable : Aucun

Discussion :

Pour chacune des entités couvertes dans les contrôles IA-02, IA-03, IA-08 et IA-09, il est important de maintenir en permanence les attributs pour chacune des entités authentifiées dans un magasin central (protégé).

IA-04(400) — Protection de la biométrie (---)

Énoncés :

Maintenir une protection adéquate pour la biométrie conformément aux règlements sur la protection des renseignements personnels.

Responsable : Aucun

Discussion :

Les renseignements recueillis au sujet de la personne aux fins d'authentification peuvent constituer des renseignements personnels; un niveau de protection convenable doit donc être appliqué. Dans les cas où la biométrie est conservée sous forme de renseignements personnels identifiables et n'a pas de valeur de hachage, il est important de les protéger conformément aux règlements sur la protection des renseignements personnels. Il n'est pas recommandé de garder les données biométriques sous une forme permettant d'identifier la personne à des fins d'identification.

IA-04(401) — Intégrité de la biométrie (---)

Énoncés :

Assurer l'intégrité de la biométrie recueillie.

Responsable : Aucun

IA-05 — Gestion des authentifiants (Nc--)

Énoncés :

Gérer les authentifiants de système des façons suivantes :
a. vérifier, au moment de la distribution initiale d'un authentifiant, l'identité de l'utilisatrice ou utilisateur, du groupe, du rôle, du service ou du dispositif recevant l'authentifiant
b. établir le contenu de l'authentifiant initial pour les authentifiants émis par l'organisation
c. s'assurer que le mécanisme d'authentification est suffisamment robuste pour l'utilisation prévue
d. établir et mettre en oeuvre des procédures administratives pour la distribution initiale des authentifiants en cas de perte, de compromission, de corruption et de révocation
e. changer les authentifiants par défaut lors de la première utilisation
f. modifier ou actualiser les authentifiants [Affectation : durée définie par l'organisation selon le type d'authentifiant] ou quand [Affectation : événements définis par l'organisation] se produisent
g. protéger le contenu des authentifiants contre les divulgations ou les modifications non autorisées
h. exiger que les personnes et les dispositifs appliquent des contrôles particuliers de manière à protéger les authentifiants
i. modifier les authentifiants pour les comptes de groupes ou de rôles lorsque des changements sont apportés à leurs membres

Responsable : Aucun

Discussion :

Les authentifiants comprennent les mots de passe, les dispositifs de chiffrement, la biométrie, les certificats, les dispositifs avec mot de passe à usage unique et les cartes d'identité. Les authentifiants de dispositif comprennent les certificats et les mots de passe. Le contenu de l'authentifiant initial correspond au contenu réel de l'authentifiant (par exemple, le mot de passe initial). Comparativement, les exigences pour le contenu de l'authentifiant contiennent des caractéristiques ou critères particuliers (par exemple, longueur minimale des mots de passe). Les développeuses et développeurs peuvent livrer des composants de systèmes avec les justificatifs d'authentification (c'est-à-dire les mots de passe) pour l'installation et la configuration initiales. Les justificatifs d'authentification par défaut sont souvent bien connus, faciles à découvrir et présentent un risque important. Les exigences de protection des authentifiants de personnes peuvent être appliquées par les contrôles PL-04 ou PS-06 pour les authentifiants qui se trouvent dans la possession de personnes et par les contrôles AC-03, AC-06 et SC-28 pour ceux qui sont stockés dans les systèmes organisationnels, comme des mots de passe stockés sous forme hachée ou chiffrée, ou des fichiers contenant des mots de passe hachés ou chiffrés accessibles à l'aide de privilèges d'administrateurs. Les systèmes prennent en charge la gestion des authentifiants de personnes en fonction des paramètres et des restrictions définis par l'organisation pour différentes caractéristiques d'authentifiants (par exemple, la longueur minimale des mots de passe, la fenêtre de validation des jetons à utilisation unique et le nombre de rejets permis durant le stade de vérification d'une authentification biométrique). Il est possible de mettre en oeuvre des mesures pour protéger les authentifiants individuels, y compris garder les authentifiants en sa possession, ne pas les partager avec d'autres personnes et signaler immédiatement leur perte, leur vol ou leur compromission. La gestion des authentifiants comprend l'émission et la révocation des authentifiants pour un accès temporaire, qui ne sera plus nécessaire par la suite.

IA-05(01) — Authentification basée sur mot de passe (---)

Énoncés :

Pour l'authentification basée sur mot de passe :
a. créer une liste des mots de passe couramment utilisés, attendus ou compromis et la mettre à jour tous les [Affectation : fréquence définie par l'organisation] et lorsque l'on soupçonne que les mots de passe de l'organisation ont été compromis, directement ou indirectement
b. lorsque les utilisatrices et utilisateurs créent ou mettent à jour des mots de passe, vérifier que les mots de passe ne figurent pas sur la liste des mots de passe couramment utilisés, attendus ou compromis figurant au contrôle IA-05(01)a
c. transmettre les mots de passe uniquement par des canaux protégés par chiffrement
d. stocker les mots de passe au moyen de la fonction de dérivation de clé avec sel, de préférence avec hachage de clé
e. exiger la sélection immédiate d'un mot de passe dès la récupération du compte
f. autoriser les utilisatrices et utilisateurs à choisir de longs mots de passe et phrases de passe, y compris les espaces et les caractères imprimables
g. utiliser des outils automatisés pour aider l'utilisatrice ou utilisateur à sélectionner des authentifiants de mots de passe robustes
h. appliquer les règles de composition et de complexité suivantes : [Affectation : règles de composition et de complexité définies par l'organisation]

Responsable : Aucun

Discussion :

L'authentification basée sur mot de passe s'applique aux mots de passe, peu importe qu'ils soient utilisés pour l'authentification à un seul facteur ou multifacteur. Les longs mots de passe ou les phrases de passe sont préférables à des mots de passe courts. L'application de règles de composition offre certains avantages pour la sécurité, mais réduit l'utilisabilité. Les organisations peuvent choisir d'établir certaines règles pour la génération de mots de passe (par exemple, le nombre minimal de caractères pour les longs mots de passe) dans certaines circonstances et d'appliquer cette exigence au contrôle IA-05(01)(h). Par exemple, un mot de passe oublié peut mener à une récupération de compte. Des mots de passe protégés par chiffrement comprennent le hachage cryptographique unidirectionnel salé des mots de passe. La liste des mots de passe couramment utilisés, compromis ou attendus comprend les mots de passe provenant des corpus de violations précédentes, les mots du dictionnaire et les caractères répétitifs ou séquentiels. Cette liste comprend des mots s'appliquant au contexte, comme le nom du service, le nom de l'utilisateur et des dérivations de ces éléments. Les questions liées à la récupération demandent souvent aux utilisatrices et utilisateurs de fournir des renseignements personnels. Afin de considérer le concept de la nécessité du point de vue de la protection de la vie privée par rapport à sa proportionnalité, les organisations doivent collecter juste assez de renseignements personnels pour garantir une authentification précise. Le recours à des jetons de connaissance n'est pas recommandé pour la récupération d'un compte.

IA-05(02) — Authentification basée sur clé publique (---)

Énoncés :

a. Pour une authentification basée sur clé publique :
- **1.** appliquer la procédure d'accès autorisé à la clé privée correspondante
- **2.** associer l'identité authentifiée au compte d'une personne ou d'un groupe

b. Lorsque l'infrastructure à clé publique (ICP) est utilisée :
- **1.** valider les certificats en créant un chemin de certification avec l'information d'état vers un point d'ancrage de confiance autorisé, y compris la vérification de l'information d'état des certificats
- **2.** utiliser une mémoire cache locale de données de révocation afin de prendre en charge la découverte et la validation de chemins

Responsable : Aucun

Discussion :

La cryptographie à clé publique est un mécanisme d'authentification valide pour les personnes, les machines et les dispositifs. Pour ce qui est des solutions d'ICP, l'information d'état pour les chemins de certification comprend les listes de certificats révoqués ou les réponses du protocole d'état de certificat. Utiliser une mémoire cache locale de données de révocation afin de prendre en charge la découverte et la validation de chemins soutient également la disponibilité du système dans des situations où les organisations ne sont pas en mesure d'avoir accès à l'information révoquée par le réseau.

IA-05(03) — Enregistrement par tierce partie externe de confiance (---)

Énoncés :

Annulé : Intégré au contrôle IA-12(04).

Responsable : Aucun

IA-05(04) — Soutien automatisé aux fins de détermination de la robustesse du mot de passe (---)

Énoncés :

Annulé : Intégré au contrôle IA-05(01).

Responsable : Aucun

IA-05(05) — Changement des authentifiants avant la livraison (---)

Énoncés :

Exiger des développeuses et développeurs ou des installatrices et installateurs des fabricants des composants de système qu'ils fournissent des authentifiants uniques ou qu'ils changent les authentifiants par défaut avant la livraison ou l'installation.

Responsable : Aucun

Discussion :

Changer les authentifiants par défaut avant la livraison ou l'installation des composants de système élargit l'exigence selon laquelle les organisations doivent modifier les authentifiants par défaut au moment de l'installation du système en exigeant des développeuses et développeurs et des installatrices et installateurs qu'ils fournissent des authentifiants uniques ou qu'ils modifient les authentifiants par défaut des composants du système avant leur livraison et installation. Toutefois, cela ne s'applique pas généralement aux développeuses et développeurs de produits commerciaux sur étagère de sécurité des TI. L'exigence concernant les authentifiants uniques peut être ajoutée aux documents d'acquisition préparés par les organisations au moment de l'acquisition de systèmes ou de composants de ceux-ci.

IA-05(06) — Protection des authentifiants (---)

Énoncés :

Protéger les authentifiants au niveau de sécurité qui correspond à la catégorie de sécurité de l'information à laquelle l'authentifiant permet l'accès.

Responsable : Aucun

Discussion :

Les authentifiants permettant l'accès aux systèmes sont protégés au niveau de sécurité de la catégorie de classification de sécurité de l'information la plus élevée dans les systèmes contenant plusieurs catégories de sécurité de l'information sans séparation fiable physique ou logique entre celles-ci. Les catégories de sécurité de l'information sont déterminées dans le cadre du processus de catégorisation de la sécurité.

IA-05(07) — Aucun authentifiant statique intégré non chiffré (---)

Énoncés :

S'assurer que les authentifiants statiques non chiffrés ne sont pas intégrés dans les applications ou autres formes de stockage statique.

Responsable : Aucun

Discussion :

Outre les applications, d'autres formes de stockage statique comprennent des scripts d'accès et des touches de fonction. Les organisations doivent prendre soin de déterminer si les authentifiants intégrés ou stockés sont chiffrés ou non. Si les authentifiants sont utilisés de la manière qu'ils sont stockés, l'on considère que les représentations sont des authentifiants non chiffrés.

IA-05(08) — Comptes multiples des systèmes (---)

Énoncés :

Mettre en oeuvre [Affectation : contrôles de sécurité définis par l'organisation] pour gérer le risque de compromission que posent les utilisatrices et utilisateurs qui possèdent des comptes dans plusieurs systèmes.

Responsable : Aucun

Discussion :

Si les utilisatrices et utilisateurs ont des comptes dans plusieurs systèmes et utilisent les mêmes authentifiants, la compromission d'un compte pourrait mener à la compromission des autres comptes. D'autres approches comprennent l'utilisation de différents authentifiants sur chaque système (mots de passe), l'utilisation d'un mécanisme quelconque d'authentification unique ou l'utilisation de mots de passe à usage unique sur tous les systèmes. Les organisations peuvent aussi utiliser des règles de comportement (voir le contrôle PL-04) et des ententes d'accès (voir le contrôle PS-06) pour atténuer le risque lié aux comptes multiples des systèmes.

IA-05(09) — Gestion des justificatifs d'identité fédérés (---)

Énoncés :

Utiliser les organisations externes suivantes pour fédérer les justificatifs d'identité : [Affectation : organisations externes désignées par l'organisation].

Responsable : Aucun

Discussion :

La fédération donne aux organisations la capacité d'authentifier des personnes et des dispositifs lorsqu'elles mènent des activités interorganisationnelles concernant le traitement, le stockage ou la transmission d'informations. Utiliser une liste particulière d'organisations externes approuvées pour l'authentification permet de s'assurer que ces organisations ont été vérifiées et sont de confiance.

IA-05(10) — Liaison dynamique des justificatifs d'identité (---)

Énoncés :

Lier les identités et les authentifiants de manière dynamique au moyen des règles suivantes : [Affectation : règles de liaison définies par l'organisation].

Responsable : Aucun

Discussion :

L'authentification exige une liaison quelconque entre une identité et l'authentifiant utilisé pour confirmer l'identité. Dans les approches classiques, la liaison est établie en fournissant au préalable l'identité et l'authentifiant au système. La liaison entre un nom d'utilisateur (c'est-à-dire l'identité) et un mot de passe (c'est-à-dire l'authentifiant), par exemple, est réalisée en fournissant l'identité et l'authentifiant au système comme une paire. Les nouvelles techniques d'authentification permettent d'établir la liaison entre l'identité et l'authentifiant à l'extérieur du système. Par exemple, l'identité et l'authentifiant des justificatifs de cartes à puce sont liés sur la carte à puce. Les systèmes peuvent se servir de ces justificatifs pour authentifier les identités qui n'ont pas été fournies au préalable, et fournir l'identité de manière dynamique après l'authentification. Dans ces situations, les organisations peuvent anticiper la fourniture dynamique d'identités. Il est essentiel de pouvoir compter sur des relations de confiance préétablies et des mécanismes dotés de pouvoirs appropriés pour valider les identités et justificatifs connexes.

IA-05(11) — Authentification basée sur un jeton matériel (---)

Énoncés :

Annulé : Intégré aux contrôles IA-02(01) et IA-02(02).

Responsable : Aucun

IA-05(12) — Rendement de l'authentification biométrique (---)

Énoncés :

Pour l'authentification fondée sur la biométrie, utiliser des mécanismes qui répondent [Affectation : exigences en matière de qualité de la biométrie définies par l'organisation].

Responsable : Aucun

Discussion :

Contrairement à l'authentification fondée sur les mots de passe, laquelle repose sur la correspondance exacte entre les mots de passe entrés par les utilisateurs et les mots de passe stockés, la correspondance exacte ne figure pas dans l'authentification par biométrie. Dépendant du type de biométrie et du mécanisme de collecte, il peut y avoir certaines différences entre les données biométriques présentées et les données biométriques stockées aux fins de comparaison. La mise en correspondance du rendement correspond au taux auquel un algorithme biométrique donne lieu à une correspondance exacte pour une utilisatrice ou un utilisateur véritable, et au rejet des autres utilisatrices et utilisateurs. Les exigences en matière de rendement biométrique comprennent le taux de correspondance, lequel reflète la précision de l'algorithme de correspondance biométrique utilisé par un système.

IA-05(13) — Expiration d'authentifiants en mémoire cache (---)

Énoncés :

Interdire l'utilisation d'authentifiants en mémoire cache après [Affectation : délais définis par l'organisation].

Responsable : Aucun

Discussion :

Les authentifiants en mémoire cache sont utilisés pour l'authentification dans une machine locale lorsque le réseau n'est pas disponible. Si l'information d'authentification en mémoire cache est périmée, la validité de l'information d'authentification peut être mise en doute.

IA-05(14) — Gestion du contenu des magasins de confiance d'ICP (---)

Énoncés :

Pour l'authentification fondée sur l'ICP, utiliser une méthodologie de gestion du contenu des magasins de confiance d'ICP installés sur toutes les plateformes, y compris les réseaux, les systèmes d'exploitation, les navigateurs et les applications.

Responsable : Aucun

Discussion :

Une méthodologie de gestion du contenu des magasins de confiance d'ICP aide à améliorer l'exactitude et l'actualité des justificatifs d'identité pour l'authentification fondée sur l'ICP dans l'ensemble de l'organisation.

IA-05(15) — Produits et services conformes aux niveaux d’assurance de l’identité, des justificatifs et de l’authentification (---)

Énoncés :

Utiliser uniquement des produits et des services pour la gestion de l’identité, des justificatifs et de l’accès qui sont conformes aux niveaux d’assurance requis.

Responsable : Aucun

IA-05(16) — Émission d'un authentifiant en personne ou par tierce partie externe de confiance (---)

Énoncés :

Exiger que l'émission [Affectation : types d'authentifiant ou authentifiants spécifiques définis par l'organisation] soit effectuée [Sélection (un choix) : en personne; par une partie externe de confiance] auprès [Affectation : autorité d'enregistrement définie par l'organisation] avec l'autorisation de [Affectation : personnel ou rôles définis par l'organisation].

Responsable : Aucun

Discussion :

L'émission d'authentifiants en personne ou par tierce partie externe de confiance améliore et renforce la fiabilité du processus de confirmation de l'identité.

IA-05(17) — Détection des attaques de présentation pour les authentifiants biométriques (---)

Énoncés :

Utiliser des mécanismes de détection des attaques pour l'authentification fondée sur la biométrie.

Responsable : Aucun

Discussion :

Les caractéristiques biométriques ne constituent pas des secrets d'authentification. De telles caractéristiques s'obtiennent par des accès Web en ligne, en prenant une photo de quelqu'un à l'aide d'un téléphone-appareil photo pour recueillir des images faciales à son insu et sans sa permission, en saisissant des objets que quelqu'un a touchés (par exemple, une empreinte digitale latente) ou en saisissant une image à haute résolution (par exemple, le motif de l'iris). Les technologies de détection des attaques de présentation, y compris la technologie de détection du vivant, peuvent permettre d'atténuer les risques que posent ces types d'attaques en rendant difficile la production d'artéfacts conçus pour mettre en échec le capteur biométrique.

IA-05(18) — Gestionnaires de mots de passe (---)

Énoncés :

a. Utiliser [Affectation : gestionnaires de mots de passe définis par l'organisation] pour générer et gérer les mots de passe
b. Protéger les mots de passe au moyen de [Affectation : contrôles définis par l'organisation]

Responsable : Aucun

Discussion :

Il est souvent difficile pour les systèmes qui utilisent des mots de passe statiques d'assurer que les mots de passe sont suffisamment complexes et que les mêmes mots de passe ne sont pas employés dans plusieurs systèmes. Un gestionnaire de mots de passe est la solution à ce problème, car il génère et stocke automatiquement des mots de passe forts et variés pour divers comptes. Un risque possible associé à l'utilisation de gestionnaires de mots de passe est que les adversaires peuvent cibler la collecte des mots de passe générés par ce gestionnaire. Par conséquent, la collecte de mots de passe nécessite une protection, notamment le chiffrement de mots de passe (voir le contrôle IA-05(01)d) et le stockage de la collecte hors ligne dans un jeton.

IA-06 — Réinjection d’authentification (---)

Énoncés :

Obscurcir les rétroactions d'information lors du processus d’authentification afin de protéger l’information contre de possibles exploitations ou utilisations par des personnes non autorisées.

Responsable : Aucun

Discussion :

Les rétroactions d'information lors du processus d’authentification depuis des systèmes ne fournit aucune donnée qui permettrait à des personnes non autorisées de compromettre les mécanismes d’authentification. La menace (appelée l’espionnage par-dessus l’épaule) peut être non négligeable pour certains types de systèmes, comme les ordinateurs de bureau et blocs-notes dotés de grands moniteurs. Par contre, pour les autres types de systèmes, comme les appareils mobiles à petit écran, la menace peut être moins importante et faire contrepoids à la susceptibilité aux erreurs de frappe étant donné la petite taille des claviers. Les moyens pour masquer la réinjection d’authentification doivent donc être sélectionnés en conséquence. Le masquage de la réinjection d’authentification comprend l’affichage d’astérisques au moment où l’utilisatrice ou utilisateur entre son mot de passe sur l’appareil ou l’affichage d’une rétroaction seulement pendant une période très limitée avant l’application d’un masquage complet.

IA-07 — Authentification du module cryptographique (---)

Énoncés :

Mettre en place des mécanismes pour l'authentification auprès d'un module cryptographique qui répond aux exigences imposées par les lois, les décrets, les directives, les politiques, la réglementation, les normes et les lignes directrices applicables, pour une telle authentification.

Responsable : Aucun

Discussion :

Il pourrait être nécessaire d'intégrer des mécanismes d'authentification à un module cryptographique afin d'authentifier la personne accédant au module ainsi que de vérifier si cette dernière a le droit d'assumer le rôle demandé et d'effectuer des fonctions dans ce rôle.

IA-08 — Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) (---)

Énoncés :

Identifier de façon unique et authentifier les utilisatrices et utilisateurs non organisationnels ou les processus exécutés en leur nom.

Responsable : Aucun

Discussion :

Les utilisatrices et utilisateurs non organisationnels incluent les utilisatrices et utilisateurs du système autres que les utilisatrices et utilisateurs organisationnels explicitement mentionnés dans le contrôle IA-

02. Ils sont identifiés de façon unique et authentifiés pour tous les accès autres que ceux explicitement identifiés et documentés dans le contrôle AC-

14. On peut exiger l'identification et l'authentification des utilisatrices et utilisateurs non organisationnels qui accèdent aux systèmes gouvernementaux afin de protéger les renseignements gouvernementaux, exclusifs ou personnels (sauf les exceptions prévues pour les systèmes liés à la sécurité nationale). Les organisations considèrent plusieurs facteurs – la sécurité, la protection de la vie privée, l'extensibilité et l'aspect pratique – pour assurer un juste équilibre entre le besoin d'accéder facilement à l'information et aux systèmes gouvernementaux et le besoin de se protéger et d'atténuer le risque adéquatement.

IA-08(01) — Acceptation des justificatifs d'identité d'ICP d'autres organismes (---)

Énoncés :

Accepter et vérifier électroniquement les justificatifs d'identité d'ICP d'autres ministères et organismes.

Responsable : Aucun

IA-08(02) — Acceptation des authentifiants externes (---)

Énoncés :

a. Accepter uniquement des authentifiants externes qui sont conformes aux règles relatives à l'assurance de l'identité numérique selon le niveau d'assurance
b. Consigner et maintenir une liste d’authentifiants externes acceptés

Responsable : Aucun

IA-08(03) — Utilisation de produits approuvés par l'architecture FICAM (---)

Énoncés :

Annulé : Intégré au contrôle IA-08(02) et propre aux États-Unis.

Responsable : Aucun

IA-08(04) — Utilisation de profils définis (---)

Énoncés :

Se conformer aux profils suivants pour la gestion des identités [Affectation : profils de gestion des identités définis par l'organisation].

Responsable : Aucun

Discussion :

Les organisations définissent des profils pour la gestion des identités en fonction de normes de gestion des identités ouvertes. Pour s'assurer que les normes de gestion des identités ouvertes sont viables, robustes, fiables, durables et interopérables, comme il est documenté, le GC évalue et examine les normes et les mises en oeuvre technologiques par rapport aux lois, aux décrets, aux directives, aux politiques, à la réglementation, aux normes et aux lignes directrices applicables.

IA-08(05) — Acceptation des justificatifs de vérification de l'identité personnelle interopérables (PIV-I) (---)

Énoncés :

Accepter et vérifier les justificatifs fédérés ou d'ICP qui satisfont [Affectation : stratégie définie par l'organisation].

Responsable : Aucun

Discussion :

L'acceptation des justificatifs PIV-I peut être mise en oeuvre par des fournisseurs de PIV, de PIV-I et d'autres fournisseurs d'identité commerciaux ou externes. L'acceptation et la vérification des justificatifs conformes aux PIV-I au Canada ne sont possibles que pour les systèmes de contrôle d'accès logique. L'acceptation et la vérification de justificatifs PIV-I traitent les entités non fédérales émettrices de cartes d'identité qui désirent interopérer avec les systèmes fondés sur l'ICP du GC et auxquels peuvent avoir confiance les parties de confiance du GC. Les justificatifs PIV-I respectent les exigences en matière de jetons de la stratégie de certification X.509 pour la Charnière fédérale canadienne de l'ICP. Les justificatifs PIV-I sont les justificatifs qui sont attribués par un fournisseur de PIV-I dont la stratégie de certification PIV-I s'associe à la Charnière fédérale canadienne de l'ICP. Un fournisseur de PIV-I doit procéder à une cocertification avec la Charnière fédérale canadienne de l'ICP (directement ou par le biais d'un autre système ICP) avec des stratégies qui ont été associées et approuvées comme étant conformes aux exigences définies dans la stratégie de certification de la Charnière fédérale canadienne de l'ICP.

IA-08(06) — Dissociabilité (---)

Énoncés :

Mettre en oeuvre les mesures suivantes pour dissocier les attributs d'utilisatrice ou utilisateur ou les relations d'assertion d'identificateur parmi les personnes, les fournisseurs de justificatifs d'identité et les parties de confiance : [Affectation : mesures définies par l'organisation].

Responsable : Aucun

Discussion :

Les solutions d'identité fédérées peuvent entraîner des risques accrus d'atteinte à la vie privée en raison du suivi et du profilage de personnes. Utiliser des tableaux de mise en correspondance d'identificateurs ou des techniques cryptographiques pour isoler les fournisseurs de justificatifs d'identité et les parties de confiance les uns des autres ou pour rendre les attributs d'identité moins visibles face aux parties émettrices peut réduire ces risques d'atteinte à la vie privée.

IA-08(400) — Identité et assurance des justificatifs (---)

Énoncés :

Annulé : Intégré au contrôle IA-05(15).

Responsable : Aucun

IA-09 — Identification et authentification des services (---)

Énoncés :

Identifier de façon unique et authentifier les [Affectation : services et applications système définis par l'organisation] avant d'établir des communications avec des dispositifs, des utilisatrices, des utilisateurs ou d'autres services ou applications.

Responsable : Aucun

Discussion :

Les services susceptibles d'exiger une identification et une authentification comprennent les applications Web ayant recours à des certificats numériques ou les services ou applications qui interrogent une base de données. Les méthodes d'identification et d'authentification pour les services et applications système comprennent l'information ou la signature de code, les graphiques de provenance et les signatures électroniques qui indiquent les sources des services. Les décisions concernant la validation des déclarations d'identification et d'authentification peuvent être prises par des services distincts des services devant mettre en oeuvre ces décisions. Cela peut être le cas dans des architectures de systèmes distribués. Dans de telles situations, les décisions concernant l'identification et l'authentification (par opposition aux identifiants et aux authentifiants comme tels) sont fournies aux services devant les mettre en oeuvre.

IA-09(01) — Échange d’information (---)

Énoncés :

Annulé : Intégré au contrôle IA-09.

Responsable : Aucun

IA-09(02) — Transmission des décisions (---)

Énoncés :

Annulé : Intégré au contrôle IA-09.

Responsable : Aucun

IA-10 — Authentification adaptative (---)

Énoncés :

Exiger que les personnes accédant au système utilisent [Affectation : techniques ou mécanismes d'authentification supplémentaires définis par l'organisation] pour certaines situations particulières, dont notamment [Affectation : circonstances ou situations définies par l'organisation].

Responsable : Aucun

Discussion :

Les adversaires peuvent compromettre les mécanismes d'authentification individuels employés par les organisations pour ensuite tenter d'usurper l'identité d'utilisatrices et utilisateurs légitimes. Pour résister à cette menace, les organisations peuvent utiliser des techniques et des mécanismes précis ou établir des protocoles visant à évaluer les comportements suspects. Par comportement suspect, on entend des personnes accédant à de l'information à laquelle elles n'accèdent généralement pas dans le cadre de leurs fonctions, rôles ou responsabilités; les personnes accédant à un plus gros volume d'information que celui auquel elles accèdent habituellement; ou les personnes tentant d'accéder à de l'information au moyen d'adresses réseau suspectes. En présence de conditions préétablies ou d'un élément déclencheur, les organisations peuvent exiger que certaines personnes fournissent de l'information d'authentification supplémentaire. Une autre application potentielle de l'authentification adaptative est le renforcement des mécanismes selon le nombre et le type de dossiers faisant l'objet de la demande d'accès. L'authentification adaptative ne constitue pas un remplacement aux mécanismes d'authentification multifacteur et ne devrait pas être utilisée à cette fin. Elle peut toutefois renforcer les mises en oeuvre de l'AMF.

IA-11 — Réauthentification (---)

Énoncés :

Exiger la réauthentification des utilisatrices et utilisateurs lors de [Affectation : circonstances ou situations nécessitant une réauthentification définies par l'organisation].

Responsable : Aucun

Discussion :

En plus des exigences de réauthentification associées au verrouillage d'appareil, les organisations peuvent exiger que les personnes s'authentifient de nouveau dans certaines situations, notamment lorsque des changements sont apportés aux rôles, aux authentifiants ou aux justificatifs d'identité, lorsque les catégories de sécurité des systèmes changent, lors de l'exécution de fonctions privilégiées, après un délai déterminé ou périodiquement.

IA-12 — Confirmation de l’identité (---)

Énoncés :

a. Des utilisatrices et utilisateurs du processus de confirmation de l’identité qui ont besoin de comptes pour un accès logique aux systèmes en fonction d’exigences adéquates en matière de niveau d’assurance de l’identité comme il est précisé dans les normes et les lignes directrices applicables
b. Régler les identités d’utilisatrices et utilisateurs dans un compte individuel unique
c. Collecter, valider et vérifier la preuve d’identité

Responsable : Aucun

Discussion :

La confirmation de l’identité est le processus de collecte, de validation et de vérification de renseignements sur l’identité de l’utilisatrice ou utilisateur aux fins d’établissement des justificatifs d’identité donnant accès à un système. Les renseignements nécessaires à la confirmation de l’identité peuvent exiger la collecte ou la confirmation d’éléments des données de renseignements personnels, comme la date de naissance. La confirmation de l’identité permet d’atténuer les menaces liées à l’enregistrement des utilisatrices et utilisateurs et à l’établissement de leurs comptes. Les organisations peuvent être assujetties aux lois, aux décrets, aux directives, aux règlements ou aux politiques applicables qui portent sur la collecte de preuves d’identité. Le personnel de l’organisation devrait consulter la haute ou le haut fonctionnaire ou cadre supérieure ou supérieur et la conseillère ou le conseiller juridique en matière de protection de la vie privée concernant de telles exigences. Tout renseignement personnel demandé à des fins de confirmation de l’identité exige que l’organisation qui collecte les renseignements soit légalement autorisée à réaliser la collecte.

IA-12(01) — Autorisation de superviseure ou superviseur (---)

Énoncés :

Exiger que le processus d'enregistrement permettant de recevoir un compte pour l'accès logique comprenne une autorisation de superviseure ou superviseur ou d'autorité qui parraine.

Responsable : Aucun

Discussion :

Inclure une autorisation de superviseure ou superviseur ou d'autorité qui parraine dans le cadre du processus d'enregistrement peut fournir un degré de surveillance supplémentaire pour s'assurer que la chaîne de gestion de l'utilisatrice ou utilisateur est au courant du compte, lequel est essentiel pour réaliser les missions et les fonctions de l'organisation, et s'assurer que les privilèges de l'utilisatrice ou utilisateur sont appropriés pour les responsabilités et les autorités au sein de l'organisation.

IA-12(02) — Preuve d'identité (---)

Énoncés :

Exiger qu'une preuve d'identification d'une personne soit présentée à l'autorité d'enregistrement.

Responsable : Aucun

Discussion :

Preuve d'identité, comme une preuve documentaire ou une combinaison de documents et de biométrie réduit le risque qu'une personne souhaitant établir une identité utilise une forme d'identification frauduleuse, ou du moins, elle complexifie la tâche des adversaires potentiels. Les éléments de preuves acceptables sont conformes aux risques pesant sur les systèmes, les rôles et les privilèges associés au compte utilisateur. La plupart des éléments de preuve d'identité sont considérés comme des renseignements personnels; dans le cas de la biométrie, ces renseignements peuvent être assujettis à des mesures de protection. L'information biométrique, si elle est recueillie pour l'identification d'une personne, ne devrait être utilisée qu'aux fins pour lesquelles elle a été recueillie. Au moment d'envisager l'utilisation de la biométrie, l'autorité d'enregistrement devrait examiner si la collecte est nécessaire; si elle est susceptible d'être efficace; si elle tient compte de la perte de la vie privée d'une personne par rapport aux avantages à en tirer; et s'il y a une approche moins susceptible de porter atteinte à la vie privée qui permettrait d'arriver à la même confirmation de l'identité.

IA-12(03) — Validation et vérification de preuve d'identité (---)

Énoncés :

Exiger que la preuve d'identité présentée soit validée et vérifiée au moyen de [Affectation : méthodes de validation et de vérification définies par l'organisation].

Responsable : Aucun

Discussion :

La validation et la vérification de la preuve d'identité renforcent l'assurance que les comptes et les identifiants sont établis pour l'utilisatrice ou utilisateur approprié, et que les authentifiants sont liés à cette utilisatrice ou cet utilisateur. La validation fait référence au processus qui confirme que la preuve est légitime et authentique et que les données contenues dans la preuve sont correctes, à jour et en lien à une personne. La vérification confirme et établit un lien entre l'identité revendiquée et l'existence réelle de l'utilisatrice ou utilisateur présentant la preuve. Les méthodes acceptables pour la validation et la vérification de la preuve d'identité sont conformes aux risques pesant sur les systèmes, les rôles et les privilèges associés au compte utilisateur.

IA-12(04) — Validation et vérification en personne (---)

Énoncés :

Exiger que la validation et la vérification d'une preuve d'identité soient effectuées en personne auprès d'une autorité d'enregistrement désignée.

Responsable : Aucun

Discussion :

La confirmation en personne réduit la possibilité d'émission de justificatifs frauduleux puisqu'elle exige la présence physique de personnes, la présentation de documents d'identité physique, et une interaction en personne avec les autorités d'enregistrement désignées.

IA-12(05) — Confirmation d'adresse (---)

Énoncés :

Exiger que [Sélection (un choix) : code d'enregistrement; avis de confirmation] soit transmis par l'entremise d'une voie d'acheminement hors bande pour vérifier l'adresse de l'utilisatrice ou utilisateur (physique ou numérique) pour le dossier.

Responsable : Aucun

Discussion :

Pour qu'il soit plus difficile pour les adversaires de se faire passer pour des utilisatrices ou utilisateurs légitimes durant le processus de confirmation de l'identité, les organisations peuvent utiliser des méthodes hors bande pour s'assurer que la personne associée à l'adresse du dossier est la même personne qui a participé à l'enregistrement. La confirmation peut prendre la forme d'un code d'inscription temporaire ou d'un avis de confirmation. L'adresse de livraison de ces artéfacts provient de dossiers et non d'une affirmation de la part de l'utilisatrice ou utilisateur. L'adresse peut être une adresse physique ou numérique. Une adresse de domicile est un exemple d'adresse physique. Les adresses courriel et les numéros de téléphone sont quant à eux des exemples d'adresses numériques.

IA-12(06) — Accepter les identités confirmées externes (---)

Énoncés :

Accepter les identités confirmées externes au [Affectation : niveau d'assurance de l'identité défini par l'organisation].

Responsable : Aucun

Discussion :

Pour éviter une reconfirmation inutile des identités, particulièrement pour les utilisatrices et utilisateurs sans justificatifs d'identité d'ICP du gouvernement, les organisations acceptent la confirmation effectuée à un niveau adéquat d'assurance par d'autres organismes ou organisations. La confirmation est conforme à la stratégie de sécurité de l'organisation et au niveau d'assurance de l'identité approprié pour le système, l'application ou l'information obtenue. Accepter les identités confirmées est un composant fondamental de la gestion des identités fédérées dans divers organismes et organisations.

IA-13 — Fournisseurs d’identité et serveurs d’autorisation (---)

Énoncés :

Avoir recours à des fournisseurs d’identité et à des serveurs d’autorisation pour gérer les identités, les attributs et les droits d’accès des personnes, des dispositifs et des entités qui ne sont pas des personnes (NPE pour Non-Person Entity) de manière à soutenir les décisions en matière d’authentification et d’autorisation conformément à la [Affectation : stratégie d’identification et d’authentification définie par l’organisation] faisant appel aux [Affectation : mécanismes définis par l’organisation].

Responsable : Aucun

Discussion :

Qu’ils soient à l’intérieur ou à l’extérieur de l’organisation, les fournisseurs d’identité gèrent les authentifiants des personnes, des dispositifs et des NPE et publient les énoncés, souvent appelés « assertions d’identité », qui attestent des identités des autres systèmes ou composants des systèmes. Les serveurs d’autorisation créent et délivrent des jetons d’accès aux personnes et aux dispositifs identifiés et authentifiés, lesquels peuvent être utilisés pour accéder au système ou aux ressources d’information. Par exemple, l’authentification unique (SSO pour Single Sign-On) offre des fonctions propres au fournisseur d’identité et au serveur d’autorisation. La gestion des authentifiants (pour tenir compte de la gestion des informations d’identification) est abordée dans le contrôle IA-05.

IA-13(01) — Protection des clés cryptographiques (---)

Énoncés :

Les clés cryptographiques qui protègent les jetons d'accès sont générées, gérées et protégées contre toute divulgation et utilisation inappropriée.

Responsable : Aucun

Discussion :

Les assertions d'identité et les jetons d'accès sont habituellement signés numériquement. Les clés privées utilisées pour signer ces assertions et jetons bénéficient d'une protection correspondant à l'impact des ressources liées au système et à l'information accessibles.

IA-13(02) — Vérification des assertions d’identité et des jetons d’accès (---)

Énoncés :

La source et l’intégrité des assertions d’identité et des jetons d’accès sont vérifiées avant d’accorder l’accès au système et aux ressources d’information.

Responsable : Aucun

Discussion :

Cela comprend la vérification des signatures numériques qui protègent les assertions d’identité et les jetons d’accès, ainsi que les métadonnées incluses. Les métadonnées comprennent l’information sur la demande d’accès, comme de l’information propre à l’utilisatrice/utilisateur, au système ou aux ressources d’information auxquelles on accède, ou à la transaction même, comme l’heure. Le système et les ressources d’information protégés peuvent comprendre des réseaux, des applications et des API connectés.

IA-13(03) — Gestion des jetons (---)

Énoncés :

Conformément à la [Affectation : stratégie d'identification et d'authentification définie par l'organisation], les assertions et les jetons d'accès sont :
a. générés
b. diffusés
c. actualisés
d. révoqués
e. limités dans le temps
f. limités selon le public cible

Responsable : Aucun

Discussion :

Un jeton d'accès est une partie de données qui représente l'autorisation accordée à une utilisatrice ou un utilisateur ou à une entité qui n'est pas une personne d'accéder à des systèmes ou à des ressources d'information spécifiques. Les jetons d'accès permettent le contrôle d'accès aux services et aux ressources. Une gestion adéquate du cycle de vie des jetons d'accès, y compris leur émission, validation et révocation, est essentielle pour assurer la confidentialité des données et des systèmes. Limiter la validité des jetons à un public particulier – par exemple, une application ou un domaine de sécurité – et limiter la durée de vie de la validité des jetons s'avèrent des pratiques importantes. Les jetons d'accès sont révoqués ou invalidés s'ils sont compromis, perdus ou ne sont plus nécessaires pour atténuer les risques associés aux jetons volés ou utilisés de manière inappropriée.

IR

Gestion des incidents de cybersécurité

Incident Response

IR-01 — Politique et procédures d'intervention en cas d'incident (Nc--)

Énoncés :

a. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :

1. une politique d'intervention en cas d'incident [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables

2. des procédures pour faciliter la mise en oeuvre des politiques d'intervention en cas d'incident et des contrôles d'intervention en cas d'incidents connexes

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à l'intervention en cas d'incident

c. Passer en revue et mettre à jour, par rapport à l'intervention en cas d'incident :

1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La politique et les procédures d'intervention en cas d'incident abordent les contrôles de la famille IR qui ont été mis en oeuvre dans les systèmes et les organisations. L'intervention en cas d'incident doit comprendre des mesures particulières lorsque des renseignements personnels sont impliqués. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à l'élaboration de la politique et des procédures d'intervention en cas d'incident. En règle générale, les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin pour des politiques et des procédures propres à la mission ou au système. La politique peut être intégrée à la politique générale de sécurité et de protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la protection de la vie privée et des procédures d'intervention en cas d'incident comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle. Il est recommandé que la politique et les procédures d'intervention en cas d'incident de l'organisation facilitent l'intégration de niveaux relevés de préparation durant les urgences et les situations de cybermenace élevée.

IR-02 — Formation sur les interventions en cas d'incident (---)

Énoncés :

a. Fournir une formation pour intervenir en cas d'incident aux utilisatrices et utilisateurs du système en fonction des rôles et des responsabilités attribués :

1. dans [Affectation : délais définis par l'organisation] après avoir été affecté à un rôle ou à des responsabilités d'intervention en cas d'incident ou après avoir obtenu l'accès au système

2. lorsque des changements apportés au système l'exigent

3. tous les [Affectation : fréquence définie par l'organisation] par la suite

b. Passer en revue et mettre à jour le contenu de la formation d'intervention en cas d'incident tous les [Affectation : fréquence définie par l'organisation] et à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La formation d'intervention en cas d'incident est associée à des responsabilités et à des rôles affectés au personnel de l'organisation afin d'assurer un contenu et un niveau de détails appropriés. Par exemple, les utilisatrices et utilisateurs peuvent avoir seulement besoin de connaître avec qui communiquer ou comment reconnaître un incident; les administratrices et administrateurs de système peuvent nécessiter de la formation supplémentaire sur le traitement des incidents; et les intervenantes et intervenants en cas d'incident pourraient recevoir de la formation sur les techniques d'investigation informatique, de collecte de données, de signalement, de reprise et de restauration des systèmes. La formation d'intervention en cas d'incident comprend la formation offerte aux utilisatrices et utilisateurs pour reconnaître et signaler les activités suspectes provenant de sources externes ou internes. La formation d'intervention en cas d'incident pour les utilisatrices et utilisateurs peut être fournie dans le cadre des contrôles AT-02 ou AT-

03. Les événements qui peuvent précipiter une mise à jour du contenu de la formation sur l'intervention en cas d'incident comprennent la mise à l'essai du plan d'urgence ou l'intervention lors d'une urgence concrète (leçons retenues), les conclusions d'une évaluation ou d'une vérification, des changements apportés aux lois, à la jurisprudence, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables.

IR-02(01) — Événements simulés (---)

Énoncés :

Intégrer des événements simulés à la formation sur les interventions en cas d'incident pour faciliter l'intervention du personnel en situation de crise.

Responsable : Aucun

Discussion :

Les organisations établissent des exigences pour intervenir face aux incidents dans les plans d'intervention en cas d'incident. Intégrer des événements simulés à la formation sur les interventions en cas d'incident permet de s'assurer que le personnel comprend ses responsabilités et sait quelles sont les interventions particulières à prendre en situation de crise.

IR-02(02) — Environnements de formation automatisée (---)

Énoncés :

Fournir un environnement de formation sur les interventions en cas d'incident au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Les mécanismes automatisés peuvent offrir un environnement de formation en mesure d'urgence plus approfondi et réaliste. Cela est possible, par exemple, en fournissant une couverture plus complète des problèmes liés aux interventions en cas d'incident, en choisissant des scénarios de formation et des environnements plus réalistes, et en augmentant la capacité d'intervention.

IR-02(03) — Atteinte à la vie privée (---)

Énoncés :

Fournir une formation d'intervention en cas d'incident sur la façon d'identifier et d'intervenir lors d'atteintes à la vie privée, y compris le processus qu'utilise l'organisation pour signaler une atteinte à la vie privée.

Responsable : Aucun

Discussion :

La formation sur les interventions en cas d'incident met l'emphase sur l'obligation qu'ont les individus de signaler les atteintes confirmées et suspectées impliquant des renseignements sous quelque support ou format, y compris papier, oral et électronique. La formation sur les interventions en cas d'incident comprend les exercices de simulation qui simulent une atteinte à la vie privée. Prière de consulter le contrôle IR-02(01).

IR-03 — Tests d’intervention en cas d’incident (---)

Énoncés :

Tester l’efficacité de la capacité d’intervention en cas d’incident pour les systèmes [Affectation : fréquence définie par l’organisation] en utilisant : [Affectation : tests définis par l’organisation].

Responsable : Aucun

Discussion :

Les organisations doivent tester les capacités d’intervention en cas d’incident afin de déterminer leur efficacité et d’identifier les faiblesses ou les lacunes potentielles. Les tests d’intervention en cas d’incident incluent l’utilisation de listes de vérification, les exercices de revue générale, les exercices de table et les simulations (en parallèle et en état d’arrêt complet). Les tests d’intervention en cas d’incident peuvent aussi inclure la détermination de l’incidence des interventions en cas d’incident sur les opérations organisationnelles et les biens organisationnels et les personnes. L’emploi de données qualitatives et quantitatives peut aider à déterminer l’efficacité des processus d’intervention en cas d’incident.

IR-03(01) — Tests automatisés (---)

Énoncés :

Tester la capacité d'intervention en cas d'incident au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Les organisations ont recours à des mécanismes automatisés pour mettre à l'essai les capacités d'intervention en cas d'incident de manière plus détaillée et efficace. Cela est possible en fournissant une couverture plus complète des problèmes liés aux interventions en cas d'incident, en choisissant des scénarios de mise à l'essai et des environnements réalistes, et en augmentant la capacité d'intervention.

IR-03(02) — Coordination avec les plans connexes (---)

Énoncés :

Coordonner la mise à l'essai des interventions en cas d'incident avec les éléments organisationnels responsables des plans connexes.

Responsable : Aucun

Discussion :

Les plans organisationnels connexes aux essais des interventions en cas d'incident comprennent les plans de continuité des activités, les plans de reprise après sinistre, les plans de continuité des opérations, les plans d'urgence, les plans des communications en temps de crise, les plans des infrastructures essentielles et les plans de mesures d'urgence pour les occupants.

IR-03(03) — Amélioration continue (---)

Énoncés :

Employer des données qualitatives et quantitatives tirées des essais pour :
a. déterminer l'efficacité des processus d'intervention en cas d'incident
b. améliorer de façon continue les processus d'intervention en cas d'incident
c. fournir des mesures et des paramètres d'intervention en cas d'incident incident qui sont conformes, pertinents et dans un format reproductible
d. cerner les tendances pour faciliter l'identification de modèles sous-jacents en ce qui a trait aux pratiques de traitement des renseignements pour ainsi éviter que ne surviennent d'autres atteintes à la vie privée

Responsable : Aucun

Discussion :

Pour permettre aux activités d'intervention en cas d'incident de fonctionner comme prévu, les organisations peuvent faire appel à des paramètres et à des critères d'évaluation pour évaluer les programmes d'intervention en cas d'incident dans le cadre des efforts visant à continuellement améliorer le rendement des interventions. Ces efforts facilitent l'amélioration de l'efficacité des interventions en cas d'incident et diminuent les répercussions de l'incident.

IR-04 — Traitement des incidents (---)

Énoncés :

a. Mettre en oeuvre des capacités de traitement pour les incidents alignées sur le plan d'intervention en cas d'incident et y inclure les activités de préparation, de détection, d'analyse, de confinement, d'éradication et de reprise
b. Coordonner les activités de traitement des incidents avec les activités de planification d'urgence
c. Intégrer les leçons apprises découlant des activités de traitement aux procédures d'intervention en cas d'incident, à la formation et aux tests, et mettre en oeuvre les changements qui en résultent comme il se doit
d. S'assurer que la rigueur, l'intensité, la portée et les résultats des activités de traitement des incidents sont comparables et prévisibles dans l'ensemble de l'organisation

Responsable : Aucun

Discussion :

Les organisations reconnaissent que la capacité d'intervention en cas d'incident dépend des capacités des systèmes organisationnels et des processus liés à la mission et aux activités prises en charge par ces systèmes. Les organisations devraient tenir compte de l'intervention en cas d'incident lors de la définition, de la conception et du développement de processus opérationnels et de mission et des systèmes. L'information liée aux incidents peut provenir de différentes sources, y compris la surveillance des vérifications, des accès physiques et des réseaux, les rapports d'utilisatrice ou utilisateur et d'administratrice ou administrateur, et les plaintes du public ou d'organismes de surveillance, et signalés de la chaîne d'approvisionnement. L'efficacité des capacités de traitement des incidents comprend la coordination entre différentes entités organisationnelles (par exemple, les propriétaires des activités et de la mission, les propriétaires des systèmes, les autorités responsables, les ressources humaines, les bureaux de la sécurité physique et les bureaux de la sécurité du personnel, les services juridiques, le responsable de la gestion des risques, le personnel des opérations et les responsables de l'approvisionnement). Les incidents de sécurité soupçonnés comprennent la réception de courriels suspects susceptibles de contenir un programme malveillant. Les incidents d'approvisionnement incluent l'insertion de matériel malveillant ou de programme malveillant dans les systèmes organisationnels ou les composants des systèmes.

IR-04(01) — Processus de traitement des incidents automatisés (---)

Énoncés :

Prendre en charge le processus de traitement des incidents au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Les mécanismes automatisés qui soutiennent les processus de traitement des incidents comprennent des outils et des systèmes de gestion des incidents en ligne qui prennent en charge la collecte de données sur l'intervention en temps réel, la capture de paquets de réseau complète et l'analyse criminalistique.

IR-04(02) — Reconfiguration dynamique (---)

Énoncés :

Comprendre les types suivants de reconfiguration dynamique [Affectation : composants du système définis par l'organisation] à sa capacité d'intervention en cas d'incident : [Affectation : types de reconfiguration dynamique définis par l'organisation].

Responsable : Aucun

Discussion :

La reconfiguration dynamique comprend les modifications apportées aux règles du routeur, aux listes de contrôle d'accès, aux paramètres de système de détection ou de prévention d'intrusions, et aux règles de filtrage pour les pare-feu et les mécanismes de protection. Les organisations exécutent une reconfiguration dynamique de leurs systèmes pour arrêter les attaques, rediriger les attaquants et isoler les composants de systèmes de sorte à limiter les dommages créés par les atteintes à la sécurité et par les compromissions. Les organisations devraient inclure dans la définition des capacités de reconfiguration, des délais pour la réalisation de la configuration des systèmes qui tiennent compte du besoin possible d'une intervention rapide pour traiter efficacement des cybermenaces.

IR-04(03) — Continuité des opérations (---)

Énoncés :

Identifier les [Affectation : classes d'incident définies par l'organisation] et prendre les mesures d'intervention suivantes pour veiller à la continuité de ses missions et fonctions opérationnelles : [Affectation : mesures d'intervention appropriées aux classes d'incident définies par l'organisation].

Responsable : Aucun

Discussion :

Les classes d'incident comprennent les défectuosités dues aux erreurs ou aux omissions liées à la conception ou à la mise en oeuvre, de même que les attaques malveillantes ciblées et non ciblées. Les mesures d'intervention en cas d'incident comprennent la dégradation méthodique du système, l'arrêt du système, le passage au mode manuel ou l'activation d'une technologie de secours qui permet de faire fonctionner le système différemment, l'emploi de mesures de déception, l'utilisation de flux d'information différents, ou l'exploitation du système dans un mode réservé aux situations d'attaque. Les organisations devraient déterminer si la continuité des exigences opérationnelles durant un incident entre en conflit avec la capacité à désactiver automatiquement le système, conformément au contrôle IR-04(05).

IR-04(04) — Corrélation de l’information (---)

Énoncés :

Établir une corrélation entre l’information sur les incidents et les interventions individuelles pour obtenir une perspective organisationnelle de la sensibilisation et des interventions en matière d’incident.

Responsable : Aucun

Discussion :

Parfois, un événement de menace, comme une cyberattaque hostile, fait en sorte qu’il ne soit possible de le déceler qu’en rassemblant de l’information provenant de différentes sources, y compris divers rapports et procédures de production de rapports déterminés par les organisations.

IR-04(05) — Désactivation automatique du système (---)

Énoncés :

Mettre en oeuvre une capacité configurable pour désactiver automatiquement le système dans l'éventualité où [Affectation : atteintes à la sécurité définies par l'organisation] étaient détectées.

Responsable : Aucun

Discussion :

Les organisations devraient déterminer si la capacité à désactiver automatiquement le système entre en conflit avec la continuité des exigences opérationnelles, conformément aux contrôles CP-02 ou IR-04(03). Des infractions de sécurité comprennent les cyberattaques qui ont compromis l'intégrité du système ou exfiltré de l'information organisationnelle et des erreurs graves dans les programmes informatiques pouvant avoir des répercussions négatives sur les fonctions liées à la mission ou aux activités de l'organisation ou mettre en péril la sécurité des individus. La désactivation automatique d'un système peut servir de technique visant à confiner l'atteinte à la vie privée dans l'éventualité que l'incident implique la compromission des renseignements personnels que renferme le système.

IR-04(06) — Menace interne (---)

Énoncés :

Mettre en oeuvre une capacité de traitement des incidents pour les incidents impliquant des menaces internes.

Responsable : Aucun

Discussion :

Mettre l'accent explicitement sur le traitement d'incidents impliquant des menaces internes met en évidence la gravité de ce type de menace et la nécessité de faire appel à des capacités spécifiques de traitement des incidents pour intervenir adéquatement et en temps opportun.

IR-04(07) — Menace interne – Coordination au sein de l’organisation (---)

Énoncés :

Coordonner des capacités de traitement des incidents pour des menaces internes qui comprennent les entités organisationnelles suivantes [Affectation : entités définies par l’organisation].

Responsable : Aucun

Discussion :

Le traitement des incidents (par exemple, les activités de préparation, de détection, d’analyse, de confinement, d’éradication et de reprise) nécessite, pour les incidents liés à des menaces internes, une coordination entre différentes entités organisationnelles, y compris les propriétaires des activités et de la mission, les propriétaires des systèmes, les ressources humaines, les responsables de l’approvisionnement, les équipes de sécurité physique et du personnel, l’agente ou agent supérieur de la sécurité de l’information de l’organisme, le personnel des opérations, la fonction de gestion des risques, la haute ou le haut fonctionnaire ou cadre supérieure ou supérieur en matière de protection de la vie privée et la conseillère ou le conseiller juridique désignés. De plus, les organisations pourraient faire appel aux organismes fédéraux, provinciaux, territoriaux, municipaux et des Premières Nations responsables de l’application de la loi afin d’obtenir du soutien. Il y a des exigences particulières touchant la communication des renseignements personnels à des fins liées à l’application de la loi; communiquer avec la déléguée ou le délégué en matière de respect de la vie privée pour obtenir de plus amples renseignements.

IR-04(08) — Corrélation avec les organisations externes (---)

Énoncés :

Coordonner avec [Affectation : organisations externes définies par l'organisation] en vue d'échanger [Affectation : information liée à un incident définie par l'organisation] de sorte à obtenir une représentation interorganisationnelle de la sensibilisation à l'incident et d'intervenir plus efficacement après celui-ci.

Responsable : Aucun

Discussion :

D'importants avantages peuvent découler de l'échange d'information liée à un incident avec des organisations externes, y compris les partenaires opérationnels et de la mission, les partenaires de la coalition et militaires, les clientes et clients et les développeuses et développeurs. La coordination interorganisationnelle peut constituer une capacité de gestion du risque très importante. Cette capacité permet aux organisations de tirer profit d'informations provenant de diverses sources de manière à intervenir efficacement en cas d'incident et d'atteinte à la vie privée pouvant avoir une incidence sur les opérations, les biens et les employées et employés de ces organisations. Des précautions doivent être prises lorsque la collaboration nécessite une communication des renseignements personnels. Communiquer avec la déléguée ou le délégué en matière de respect de la vie privée pour obtenir de plus amples renseignements.

IR-04(09) — Capacités d'intervention dynamique (---)

Énoncés :

Utiliser [Affectation : capacités d'intervention dynamique définies par l'organisation] de sorte à intervenir en cas d'incident.

Responsable : Aucun

Discussion :

La capacité d'intervention dynamique aborde le déploiement en temps opportun de capacités organisationnelles nouvelles ou de remplacement en réponse aux incidents. Cela comprend les capacités mises en oeuvre au niveau du processus lié à la mission et aux activités.

IR-04(10) — Coordination relative à la chaîne d'approvisionnement (---)

Énoncés :

Coordonner les activités d'intervention en cas d'incident touchant aux événements d'approvisionnement avec d'autres organisations dans la chaîne d'approvisionnement.

Responsable : Aucun

Discussion :

Les organisations qui participent aux activités d'approvisionnement comprennent les développeurs de produits, les intégrateurs, les fabricants, les emballeurs, les assembleurs, les distributeurs, les fournisseurs et les revendeurs. Les incidents liés à la chaîne d'approvisionnement peuvent se produire n'importe où dans la chaîne d'approvisionnement et comprendre des compromissions ou des atteintes à la vie privée qui impliquent des fournisseurs principaux ou secondaires, des produits informatiques, des composants de systèmes, des processus de développement ou du personnel, et des processus de distribution ou des installations d'entreposage. Les organisations doivent inclure dans leur chaîne d'approvisionnement des ententes d'échange d'information pour la protection et l'échange d'information, et elles doivent tenir compte de leurs obligations quant au signalement des incidents fait aux organes d'examen du gouvernement.

IR-04(11) — Équipe intégrée d'intervention en cas d'incident (---)

Énoncés :

Établir et maintenir une équipe intégrée d'intervention en cas d'incident qui peut être déployée à tout endroit identifié par l'organisation dans [Affectation : délais définis par l'organisation].

Responsable : Aucun

Discussion :

Une équipe intégrée d'intervention en cas d'incident est une équipe d'expertes et experts qui évalue, documente et intervient en cas d'incidents de manière à ce que les systèmes organisationnels et les réseaux puissent récupérer rapidement et mettre en oeuvre les contrôles nécessaires pour éviter d'éventuels incidents. Le personnel de l'équipe d'intervention en cas d'incident comprend des analystes d'informatique judiciaire et de programmes malveillants, des développeuses et développeurs d'outils, les architectes ou ingénieures et ingénieurs de système, les praticiennes et praticiens de la protection de la vie privée et les membres du personnel affectés aux opérations en temps réel. La capacité de traitement des incidents comprend l'exécution rapide de la préservation de la preuve criminalistique et de l'analyse et de l'intervention face aux intrusions. Pour certaines organisations, l'équipe d'intervention en cas d'incident peut être une entité interorganisationnelle. Une équipe intégrée d'intervention en cas d'incident facilite l'échange d'information et permet au personnel de l'organisation (par exemple, les développeuses et développeurs, les personnes chargées de la mise en application et les opératrices et opérateurs) de tirer profit des connaissances de l'équipe concernant la menace afin de mettre en oeuvre des mesures de défense qui permettront aux organisations de décourager plus efficacement les intrusions. De plus, les équipes intégrées facilitent la détection rapide d'intrusions, l'élaboration de mesures d'atténuation appropriées et le déploiement de mesures de défense efficaces. Par exemple, dès qu'une intrusion est détectée, l'équipe intégrée peut rapidement développer des mesures que les opérateurs peuvent mettre en oeuvre, corréler le nouvel incident à l'information liée aux intrusions précédentes et élargir le développement du renseignement sur la cybersécurité en cours. Les équipes intégrées d'intervention en cas d'incident sont mieux en mesure d'identifier les tactiques, techniques et procédures liées aux opérations ou à des fonctions opérationnelles et de mission et définir les mesures d'intervention à prendre qui ne perturberont pas les fonctions liées à la mission et aux activités de l'organisation. Les équipes d'intervention en cas d'incident peuvent être réparties dans les organisations pour assurer une meilleure résilience.

IR-04(12) — Programme malveillant et analyse criminalistique (---)

Énoncés :

Analyser un programme malveillant ou d'autres artéfacts qui restent dans le système après l'incident.

Responsable : Aucun

Discussion :

Lorsqu'elle est effectuée avec soin dans un environnement isolé, l'analyse d'un programme malveillant et d'autres artéfacts résiduels d'un incident ou d'une brèche de sécurité peut procurer à l'organisation une connaissance approfondie sur les tactiques, les techniques et les procédures utilisées par les adversaires. Elle permet aussi d'indiquer l'identité ou certaines caractéristiques définies de l'adversaire. De plus, l'analyse des programmes malveillants peut aider l'organisation à élaborer des interventions en vue d'éventuels incidents.

IR-04(13) — Analyse comportementale (---)

Énoncés :

Analyser un comportement des adversaires anormal ou suspect en lien à des [Affectation : environnements ou ressources définis par l'organisation].

Responsable : Aucun

Discussion :

Si l'organisation maintient un environnement de déception, une analyse des comportements dans cet environnement précis, y compris des ressources ciblées par l'adversaire et du moment de l'incident ou de l'événement, peut fournir des renseignements à propos des tactiques, techniques et procédures des adversaires. À l'extérieur d'un environnement de déception, l'analyse d'un comportement anormal de la part des adversaires (par exemple, des changements concernant le rendement des systèmes ou les habitudes d'utilisation) ou un comportement suspect (par exemple, des changements dans les recherches d'emplacement de ressources spécifiques) peut donner à l'organisation une connaissance à ce sujet. Par moment, une analyse de l'information comportementale peut révéler de l'information sur une personne identifiable, et une autorité légitime ainsi que des mesures de protection liées aux renseignements personnels devraient être prises en considération.

IR-04(14) — Centre des opérations de sécurité (---)

Énoncés :

Établir et tenir à jour un centre des opérations de sécurité.

Responsable : Aucun

Discussion :

Un centre des opérations de sécurité (SOC pour Security Operations Centre) est le centre névralgique pour les opérations de sécurité et la défense des réseaux informatiques d'une organisation. L'objectif du centre des opérations de sécurité est de défendre et de surveiller en permanence les systèmes et les réseaux d'une organisation (c'est-à-dire la cyberinfrastructure). Le Centre des opérations de sécurité est aussi chargé de détecter, d'analyser et d'intervenir en temps opportun lors d'incidents de cybersécurité. L'organisation dote en personnel technique et opérationnel le centre des opérations de sécurité (par exemple, des analystes de la sécurité, du personnel chargé des interventions en cas d'incident, des ingénieures et ingénieurs en sécurité des systèmes) et met en oeuvre une série de contrôles techniques, procéduraux ou opérationnels (y compris ceux qui touchent la surveillance, l'analyse et les outils de criminalistique) pour surveiller, fusionner, mettre en correspondance, analyser et intervenir en fonction de données d'événements de menace et d'événements touchant la sécurité provenant de diverses sources. Ces sources comprennent les défenses du périmètre, les périphériques réseau (par exemple, routeurs et commutateurs) et des sources de données d'agents d'extrémité. Le centre des opérations de sécurité offre une capacité globale en matière de connaissance de la situation pour aider les organisations à déterminer la posture de sécurité du système et de l'organisation. Une capacité de centre des opérations de sécurité peut être obtenue de plusieurs façons. Les plus grandes organisations peuvent mettre en place un centre des opérations de sécurité dédié alors que des organisations plus petites peuvent faire appel à des organisations tierces pour fournir une telle capacité. Si un incident de sécurité venait à impliquer la compromission de renseignements personnels, le personnel du centre des opérations de sécurité devrait faire appel à des professionnelles et professionnels de la protection de la vie privée dans des organisations. En ce qui a trait aux organisations détenant un nombre important de renseignements personnels, il convient pour celles-ci d'avoir des représentantes et représentants dotés d'une expertise en matière de protection de la vie privée au sein de leur centre des opérations de sécurité parmi leur personnel technique et opérationnel.

IR-04(15) — Relations publiques, réparation de réputation et notification (---)

Énoncés :

a. Gérer les relations publiques associées à un incident
b. Employer des mesures visant à réparer la réputation d'une organisation
c. Le cas échéant, aviser les personnes dont les renseignements personnels ont été compromis

Responsable : Aucun

Discussion :

Il est important pour une organisation de mettre en place une stratégie pour aborder les incidents qui ont été portés à l'attention du grand public, qui ont donné une image négative de l'organisation, qui ont affecté les personnes liées à l'organisation (par exemple, les partenaires ou les clientes et clients) ou qui ont touché des personnes dont les renseignements personnels ont été compromis. Une telle publicité peut nuire grandement à l'organisation et affecter sa capacité à effectuer ses fonctions liées à la mission et aux activités. Prendre les mesures nécessaires pour réparer la réputation de l'organisation est un aspect essentiel qui permet de regagner la confiance de ses membres ainsi que des personnes liées à l'organisation. En notifiant les personnes concernées, cela leur permet de prendre les mesures nécessaires pour les empêcher de subir tout autre préjudice en raison de l'information compromise.

IR-05 — Surveillance des incidents (---)

Énoncés :

Faire le suivi et documenter les incidents.

Responsable : Aucun

Discussion :

La documentation des incidents comprend la tenue de dossiers au sujet de chaque incident, l'état de l'incident et toute autre information pertinente aux fins d'investigation informatique, ainsi que l'évaluation des détails, des tendances et du traitement des incidents. L'information relative à un incident peut provenir de diverses sources, y compris la surveillance réseau, les rapports d'incident, les équipes d'intervention en cas d'incident, les plaintes d'utilisatrices et utilisateurs, les partenaires de la chaîne d'approvisionnement, la surveillance des vérifications, la surveillance des accès physiques et les rapports d'utilisateur et d'administrateur. Le contrôle IR-04 fournit de l'information sur les types d'incidents qui sont appropriés pour la surveillance.

IR-05(01) — Suivi, collecte de données et analyses automatisés (---)

Énoncés :

Faire le suivi des incidents, recueillir et analyser l'information sur l'incident au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Parmi les mécanismes automatisés servant au suivi des incidents, à la collecte et à l'analyse d'information sur les incidents, il est possible de compter sur les centres d'intervention en cas d'incidents informatiques ou autres bases de données électroniques d'incidents et de dispositifs de surveillance de réseau. Si la collecte de données nécessite de recueillir ou de créer des renseignements personnels, l'organisation doit s'assurer de posséder l'autorité légitime pour cette collecte et elle devrait limiter les renseignements personnels uniquement aux renseignements requis pour réaliser une surveillance efficace.

IR-06 — Signalement des incidents (---)

Énoncés :

a. Exiger que les membres du personnel signalent les incidents suspects à l'équipe d'intervention en cas d'incident de l'organisation dans [Affectation : délais définis par l'organisation]
b. Donner de l'information sur l'incident à [Affectation : autorités désignées par l'organisation]

Responsable : Aucun

Discussion :

Les types d'incidents signalés, le contenu et la rapidité des signalements, ainsi que les autorités de signalement désignées doivent refléter les lois, les décrets, les directives, la réglementation, les politiques, les normes et les lignes directrices applicables. Les renseignements sur l'incident peuvent informer les évaluations des risques, les évaluations d'efficacité des contrôles, les exigences de sécurité pour l'acquisition et les critères de sélection pour les produits technologiques. Le partage et la divulgation de renseignements personnels devraient être limités, sauf s'ils sont exigés pour assurer un signalement efficace.

IR-06(01) — Signalement automatisé (---)

Énoncés :

Signaler les incidents au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Les destinataires des rapports d'incidents sont précisés dans la famille IR-06B. Les mécanismes de signalement automatisés comprennent les courriels, l'affichage sur des sites Web (avec des mises à jour automatisées) et des programmes et outils automatisés d'intervention en cas d'incident.

IR-06(02) — Vulnérabilités liées aux incidents (---)

Énoncés :

Signaler les vulnérabilités du système associées aux incidents signalés à [Affectation : personnel ou rôles définis par l'organisation].

Responsable : Aucun

Discussion :

Les incidents signalés qui permettent de découvrir des vulnérabilités du système sont analysés par le personnel de l'organisation, y compris les propriétaires de systèmes, les propriétaires de la mission et des activités, les cadres supérieures et supérieurs de la gouvernance en matière de sécurité du ministère, les hauts fonctionnaires ou cadres supérieures et supérieurs en matière de protection de la vie privée, les cadres supérieures et supérieurs désignés pour l'autorisation et la fonction de gestion des risques. L'analyse peut servir à accorder la priorité et à entamer des mesures d'atténuation pour aborder la question des vulnérabilités du système découvertes.

IR-06(03) — Coordination avec la chaîne d'approvisionnement (---)

Énoncés :

Fournir de l'information sur les incidents au fournisseur du produit ou du service et aux autres organisations impliquées dans la chaîne d'approvisionnement ou la gouvernance de celle-ci pour les systèmes ou les composants de systèmes liés à l'incident.

Responsable : Aucun

Discussion :

Les organisations qui participent aux activités d'approvisionnement comprennent les développeurs de produits, les intégrateurs, les fabricants, les emballeurs, les assembleurs, les distributeurs, les fournisseurs et les revendeurs. Parmi les entités qui assurent une gouvernance de la chaîne d'approvisionnement se trouve le ministère de la Cybersécurité et du Numérique (MCN). Les incidents liés à la chaîne d'approvisionnement comprennent les compromissions ou les violations qui impliquent des produits informatiques, des composants de systèmes, des processus de développement ou du personnel, des processus de distribution ou des installations d'entreposage. Les organisations devraient déterminer l'information utile à partager, et elles devraient tenir compte de la valeur ajoutée par le signalement aux organisations externes des incidents liés à la chaîne d'approvisionnement, notamment la capacité d'améliorer les processus ou de déterminer la cause fondamentale de l'incident.

IR-07 — Assistance en cas d’incident (---)

Énoncés :

Fournir une ressource de soutien qui fait partie intégrante de la capacité d’intervention en cas d’incident de l’organisation et qui offre conseils et assistance aux utilisatrices et utilisateurs du système pour ce qui touche le traitement et le signalement des incidents.

Responsable : Aucun

Discussion :

Les ressources de soutien fournies par les organisations pour l’intervention en cas d’incident comprennent les services de dépannage, les groupes d’assistance, les systèmes automatisés de demandes de service pour l’ouverture et le suivi des demandes d’intervention en cas d’incident, et l’accès aux services d’investigation informatique ou aux services de recours des consommatrices et consommateurs, au besoin.

IR-07(01) — Soutien automatisé concernant la disponibilité de l'information et du soutien (---)

Énoncés :

Accroître la disponibilité du soutien et de l'information sur les interventions en cas d'incident au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Les mécanismes automatisés peuvent offrir aux utilisatrices et utilisateurs une capacité d'assistance réactive ou proactive lors des interventions en cas d'incident. Par exemple, les utilisatrices et utilisateurs peuvent avoir accès à un site Web pour interroger la capacité d'assistance, ou la capacité peut transmettre de l'information sur les interventions en cas d'incident de manière proactive aux utilisatrices et utilisateurs (par diffusion générale ou ciblée) en vue d'accroître leurs connaissances concernant les capacités et le soutien actuels de l'organisation en matière d'intervention.

IR-07(02) — Coordination avec les fournisseurs externes (---)

Énoncés :

a. Établir une relation de coopération directe entre la capacité d'intervention en cas d'incident de l'organisation et la capacité de protection des systèmes de fournisseurs externes
b. Communiquer l'identité des membres de son équipe d'intervention en cas d'incident aux fournisseurs externes

Responsable : Aucun

Discussion :

Les fournisseurs externes d'une capacité de protection des systèmes comprennent les outils et services fournis par le Centre gouvernemental de cyberdéfense (CGCD). Les fournisseurs externes participent à la protection, la surveillance, l'analyse et la détection des activités illicites dans les systèmes d'information et les réseaux de l'organisation et interviennent, le cas échéant. Il peut être avantageux d'avoir en place des ententes avec des fournisseurs externes pour clarifier les rôles et responsabilités de chaque partie avant que ne se produise un incident.

IR-08 — Plan d'intervention en cas d'incident (---)

Énoncés :

a. Élaborer un plan d'intervention en cas d'incident qui :
- **1.** fournit à l'organisation une feuille de route pour la mise en oeuvre de ses capacités d'intervention en cas d'incident
- **2.** décrit la structure et l'organisation des capacités d'intervention en cas d'incident
- **3.** fournit une approche de haut niveau indiquant comment les capacités d'intervention en cas d'incident s'intègrent à l'organisation en général
- **4.** répond à ses exigences spécifiques concernant sa mission, sa taille, sa structure et ses fonctions
- **5.** définit les incidents devant être signalés
- **6.** définit les paramètres de mesure de sa capacité d'intervention en cas d'incident
- **7.** définit les ressources et le soutien de la direction nécessaires au maintien et à l'évolution de la capacité d'intervention en cas d'incident
- **8.** décrit les modalités d'échange d'information en cas d'incident
- **9.** est examiné et approuvé par [Affectation : personnel ou rôles définis par l'organisation] [Affectation : fréquence définie par l'organisation]
- **10.** élabore explicitement la responsabilité de l'intervention en cas d'incident à l'intention de [Affectation : entités, personnel ou rôles définis par l'organisation]

b. Distribuer des copies du plan d'intervention en cas d'incident [Affectation : employées et employés (par nom ou rôle) et éléments organisationnels responsables de l'intervention en cas d'incident définis par l'organisation]
c. Mettre à jour le plan d'intervention en cas d'incident afin de tenir compte des changements apportés aux systèmes et des changements organisationnels, ou encore des problèmes rencontrés durant la mise en oeuvre, l'exécution ou la mise à l'essai du plan d'intervention
d. Communiquer les changements apportés au plan d'intervention en cas d'incident [Affectation : employées et employés (par nom ou rôle) et éléments organisationnels responsables de l'intervention en cas d'incident définis par l'organisation]
e. Protéger le plan d'intervention en cas d'incident des divulgations et des modifications non autorisées

Responsable : Aucun

Discussion :

Il est important que les organisations élaborent et mettent en oeuvre une approche d'intervention coordonnée en cas d'incident. La mission et les activités organisationnelles déterminent la structure des capacités d'intervention en cas d'incident. Dans le cadre des capacités d'intervention en cas d'incident, les organisations doivent considérer la coordination et l'échange d'information avec des organisations externes, y compris des fournisseurs de services et d'autres organisations participant à la chaîne d'approvisionnement. Pour ce qui est des incidents qui impliquent des renseignements personnels (par exemple, des atteintes à la vie privée) il convient d'inclure un processus permettant de déterminer si la transmission d'un avis aux organisations de surveillance ou aux personnes touchées est pertinente et de fournir cet avis en conséquence.

IR-08(01) — Atteintes à la vie privée (---)

Énoncés :

Pour les atteintes à la vie privée touchant des renseignements personnels, il faut inclure ce qui suit dans le plan d'intervention en cas d'incident :
a. un processus permettant de déterminer s'il est nécessaire de faire un signalement à des personnes ou à d'autres organisations, y compris des organisations de surveillance
b. un processus d'évaluation pour déterminer l'étendue des dommages, de l'embarras, de l'injustice ou des désagréments aux personnes touchées et tout mécanisme pour atténuer des tels dommages
c. l'identification des exigences en matière de protection de la vie privée applicables

Responsable : Aucun

Discussion :

Les organisations pourraient être exigées par les lois, la réglementation ou les politiques à suivre des procédures spécifiques en lien aux violations, ce qui comprend : des notifications aux personnes, aux organisations touchées et aux organes d'examen; des normes relatives aux dommages; des mesures d'atténuation ou d'autres exigences spécifiques. Les organisations assujetties à la Loi sur la protection des renseignements personnels dans le secteur privé doivent signaler à la Commission d'accès à l'information du Québec (CAI) toute atteinte à la protection des renseignements personnels qui représente un risque de préjudice grave. Elles doivent également aviser les personnes de ces atteintes et conserver un dossier des atteintes à la protection des renseignements.

IR-09 — Intervention en cas de fuite d'information (---)

Énoncés :

Réagir aux fuites d'information en :
a. désignant [Affectation : personnel ou rôles définis par l'organisation] à titre de personnes responsables de l'intervention cas de fuite d'information
b. déterminant, de manière précise, quelle information a fait l'objet de la contamination du système
c. avertissant [Affectation : personnel ou rôles définis par l'organisation] de la fuite d'information au moyen d'un mode de communication n'étant pas lié à la fuite
d. isolant le système ou le composant du système contaminé
e. supprimant l'information du système ou le composant du système contaminé
f. déterminant si d'autres systèmes ou composants de systèmes avaient pu être contaminés subséquemment
g. effectuant les mesures supplémentaires suivantes : [Affectation : actions définies par l'organisation]

Responsable : Aucun

Discussion :

Les fuites d'information sont des situations où de l'information est transmise à des systèmes pour lesquels le traitement de ce type d'information n'a pas été autorisé. Les fuites d'information se produisent lorsqu'on croit faussement que la classification de l'information transmise à un système est moins élevée qu'elle ne l'est réellement et que cette correction est apportée après la transmission. À ce stade, il est nécessaire de mettre en place des mesures correctives. La nature de l'intervention est fondée sur la classification ou le niveau d'incidence de l'information faisant l'objet de la fuite, sur les capacités de sécurité du système, sur la nature précise du support de stockage contaminé et sur les autorisations d'accès des personnes autorisées à accéder au système contaminé. Les méthodes utilisées pour communiquer l'information relative à la fuite après le coup ne sont pas directement liées à la méthode de transmission de l'information faisant l'objet de la fuite de sorte à réduire le risque d'élargissement de la contamination avant que celle-ci ne soit isolée et l'information supprimée Si les fuites d'information touchent à des renseignements personnels, les responsables devraient passer en revue la situation pour évaluer si une atteinte à la vie privée s'est produite, et les protocoles sur les atteintes à la vie privée de l'organisation doivent être suivis, tel qu'il est précisé dans l'IR-08.

IR-09(01) — Personnel responsable (---)

Énoncés :

Annulé : Intégré au contrôle IR-09.

Responsable : Aucun

IR-09(02) — Formation (---)

Énoncés :

Offrir une formation sur l'intervention en cas de fuite d'information [Affectation : fréquence définie par l'organisation].

Responsable : Aucun

Discussion :

Les organisations établissent des exigences pour intervenir face aux incidents liés aux fuites d'information dans les plans d'intervention en cas d'incident. Une formation sur l'intervention en cas d'incident suivie sur une base régulière aide à s'assurer que les membres du personnel comprennent leurs responsabilités et les mesures précises à prendre lorsque surviennent des incidents liés aux fuites d'information.

IR-09(03) — Opérations à la suite d’une fuite (---)

Énoncés :

Mettre en oeuvre les procédures suivantes afin de veiller à ce que les membres du personnel de l’organisation touchés par les fuites d’information puissent continuer d’exécuter leurs fonctions même si les systèmes contaminés sont en cours d’assainissement : [Affectation : procédures définies par l’organisation].

Responsable : Aucun

Discussion :

Les mesures correctives appliquées aux systèmes contaminés par les fuites d’information peuvent exiger beaucoup de temps. Les membres du personnel peuvent ne pas avoir accès aux systèmes contaminés pendant que des mesures correctives sont prises, ce qui peut affecter leur capacité à mener les activités de l’organisation.

IR-09(04) — Exposition au personnel non autorisé (---)

Énoncés :

Employer les contrôles suivants pour les membres du personnel exposés à de l'information ne faisant pas partie des autorisations d'accès accordées : [Affectation : contrôles définis par l'organisation].

Responsable : Aucun

Discussion :

Les contrôles impliquent de s'assurer que les membres du personnel qui sont exposés à une fuite d'information soient mis au courant des lois, des décrets, des directives, de la réglementation, des politiques, des normes et des lignes directrices concernant l'information et les restrictions imposées en fonction de l'exposition à une telle information.

IR-10 — Équipe d'analyse de la sécurité de l'information intégrée (---)

Énoncés :

Annulé : Transféré sous le contrôle IR-04(11).

Responsable : Aucun

MA

Sécurité des opérations de maintenance

Maintenance

MA-01 — Politique et procédures de maintenance (---)

Énoncés :

a. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :
- **1.** une politique de maintenance [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables
- **2.** des procédures pour faciliter la mise en oeuvre de la politique de maintenance et des contrôles d'accès connexes

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à la maintenance

c. Passer en revue et mettre à jour, par rapport à la maintenance :
- **1.** la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]
- **2.** les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La politique et les procédures de maintenance abordent les contrôles de la famille MA qui ont été mis en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à l'élaboration de la politique et des procédures de maintenance. En règle générale, les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin pour des politiques et des procédures propres à la mission ou au système. La politique peut être intégrée à la politique générale de sécurité et de protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures de maintenance comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des chargements apportés aux lois, à la jurisprudence, aux décrets applicables, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.

MA-02 — Maintenance contrôlée (---)

Énoncés :

a. Planifier, exécuter, documenter et examiner les dossiers de maintenance, de réparation et de remplacement des composants de système conformément aux spécifications du fabricant ou du fournisseur ou à ses propres exigences
b. Approuver et surveiller toutes les activités de maintenance, qu'elles soient effectuées sur place ou à distance et que le système ou les composants des systèmes soient réparés sur les lieux ou dans un autre emplacement
c. Exiger que [Affectation : personnel ou rôles définis par l'organisation] approuve explicitement le retrait du système ou de ses composants, de ses installations aux fins de maintenance, de réparation ou de remplacement à l'extérieur de ses locaux
d. Nettoyer l'équipement afin de supprimer les données suivantes des supports connexes avant de l'expédier à l'extérieur aux fins de maintenance, de réparation ou de remplacement : [Affectation : information définie par l'organisation]
e. Vérifier tous les contrôles potentiellement concernés pour s'assurer qu'ils continuent de fonctionner adéquatement après les activités de maintenance, de réparation ou de remplacement
f. Inclure l'information suivante dans les enregistrements de maintenance organisationnels : [Affectation : information définie par l'organisation]

Responsable : Aucun

Discussion :

Le contrôle de la maintenance de système traite des aspects du programme de maintenance des systèmes liés à la sécurité de l'information et s'applique à tous les types de maintenance réalisée par des entités locales ou non locales dont fait l'objet les composants du système. La maintenance touche les périphériques comme les numériseurs, les photocopieurs et les imprimantes. L'information nécessaire à la création de dossiers de maintenance efficaces comprend la date et l'heure de la maintenance, une description de la maintenance effectuée, les noms des personnes responsables de la maintenance, le nom de l'escorte, et les composants des systèmes ou l'équipement retirés ou remplacés. Les organisations devraient tenir compte des risques liés à la chaîne d'approvisionnement qui concernent le remplacement des composants des systèmes.

MA-02(01) — Contenu des enregistrements (---)

Énoncés :

Annulé : Intégré au contrôle MA-02.

Responsable : Aucun

MA-02(02) — Activités de maintenance automatisées (---)

Énoncés :

a. Planifier, effectuer et documenter les interventions de maintenance, de réparation et de remplacement pour le système au moyen de [Affectation : mécanismes automatisés définis par l'organisation]
b. Tenir à jour des dossiers précis et complets de toutes les maintenances, réparations et de tous les remplacements exigés, planifiés, en cours et exécutés

Responsable : Aucun

Discussion :

Le recours à des mécanismes automatisés pour gérer et contrôler les programmes et les activités de maintenance de système permet d'assurer la production d'enregistrements de maintenance précise, ponctuelle, complète et conforme.

MA-03 — Outils de maintenance (---)

Énoncés :

a. Approuver, contrôler et surveiller l'utilisation des outils de maintenance des systèmes
b. Examiner les outils de maintenance précédemment approuvés [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

L'approbation, le contrôle, la surveillance et l'examen des outils de maintenance permettent de traiter les problèmes de sécurité en lien avec les outils de maintenance qui ne sont pas dans les limites d'autorisation et servent spécifiquement aux activités de diagnostic et de réparation sur le système. Les organisations ont une certaine souplesse quant à la détermination des rôles pour l'approbation des outils de maintenance et la manière dont l'approbation est documentée. Un examen périodique des outils de maintenance facilite le retrait de l'approbation d'outils désuets, non pris en charge, non pertinents ou inutilisés. Les outils de maintenance peuvent comprendre les éléments matériels, logiciels et micrologiciels et ils peuvent être préinstallés, transportés par le personnel de maintenance sur des supports, basés sur le nuage ou téléchargés à partir de sites Web. De tels outils peuvent servir au transport intentionnel ou non intentionnel de programmes malveillants à l'intérieur d'une installation et, subséquemment, dans les systèmes. Les outils de maintenance peuvent comprendre l'équipement de test et de diagnostic matériel ou logiciel, ainsi que les renifleurs de paquets. Les composants matériels ou logiciels qui servent à la maintenance du système et font partie de ce dernier (y compris le logiciel utilisé pour exécuter les fonctions comme ping, ls, ipconfig, ou matériel et logiciel mettant en oeuvre le port de surveillance d'un commutateur Ethernet), ne sont pas couverts par les outils de maintenance.

MA-03(01) — Inspection des outils (---)

Énoncés :

Inspecter les outils de maintenance utilisés par le personnel de maintenance pour repérer des modifications incorrectes ou non autorisées.

Responsable : Aucun

Discussion :

Le personnel de maintenance peut directement apporter les outils de maintenance dans une installation ou ces outils peuvent être téléchargés à partir d'un site Web de fournisseur. Lors de l'inspection, si l'organisation détermine que les outils de maintenance ont été modifiés de manière inappropriée, ou qu'ils contiennent un programme malveillant, elle gérera l'incident conformément à ses politiques et procédures organisationnelles en matière de traitement des incidents.

MA-03(02) — Inspection des supports (---)

Énoncés :

Vérifier les supports où sont stockés les programmes de diagnostic et de test afin de détecter la présence de code malveillant, avant d'utiliser les supports dans les systèmes.

Responsable : Aucun

Discussion :

Lors de l'inspection des supports contenant des programmes diagnostic et de test de la maintenance, si l'organisation détermine que les supports contiennent un programme malveillant, elle gérera l'incident conformément à ses politiques et procédures organisationnelles en matière de traitement des incidents.

MA-03(03) — Prévention des retraits non autorisés (---)

Énoncés :

Prévenir le retrait non autorisé d'équipements de maintenance contenant de l'information sur l'organisation ou des renseignements personnels en :
a. s'assurant qu'aucune information sur l'organisation ou aucun renseignement personnel ne se trouve dans l'équipement
b. nettoyant ou détruisant l'équipement
c. conservant l'équipement dans l'installation
d. obtenant une exemption de [Affectation : personnel ou rôles définis par l'organisation] autorisant explicitement le retrait de l'équipement de l'installation

Responsable : Aucun

Discussion :

L'information organisationnelle comprend toute information appartenant à l'organisation et celle fournie aux organisations qui gèrent l'information de cette dernière.

MA-03(04) — Utilisation restreinte des outils (---)

Énoncés :

Limiter l'utilisation d'outils de maintenance au personnel autorisé uniquement.

Responsable : Aucun

Discussion :

La limitation de l'utilisation d'outils de maintenance au personnel autorisé uniquement s'applique aux systèmes qui s'occupent généralement des fonctions de maintenance.

MA-03(05) — Exécution avec privilège (---)

Énoncés :

Surveiller l'emploi des outils de maintenance qui sont exécutés avec des privilèges accrus.

Responsable : Aucun

Discussion :

Les outils de maintenance qui sont exécutés avec des privilèges accrus peuvent mener à un accès non autorisé aux renseignements et aux biens de l'organisation qui seraient autrement inaccessibles.

MA-03(06) — Mises à jour logicielles et correctifs (---)

Énoncés :

Inspecter les outils de maintenance pour s'assurer que les plus récentes mises à jour et derniers correctifs ont été installés.

Responsable : Aucun

Discussion :

Les outils de maintenance qui font appel à des logiciels désuets et non corrigés peuvent fournir un vecteur de menace pour les adversaires et donner lieu à une vulnérabilité majeure pour les organisations.

MA-04 — Maintenance non locale (---)

Énoncés :

a. Approuver et surveiller les activités de maintenance et de diagnostic non locales
b. Permettre l'utilisation des outils de télémaintenance et de télédiagnostic seulement si elle est conforme à sa politique et documentée dans le plan de sécurité du système
c. Utiliser une authentification robuste lors de l'établissement des sessions de maintenance non locale
d. Tenir à jour des dossiers des activités de maintenance non locale et de télédiagnostic
e. Mettre fin aux sessions et aux connexions réseau lorsque la maintenance non locale est terminée

Responsable : Aucun

Discussion :

Les activités de maintenance et de diagnostic non locales sont menées par des personnes qui communiquent à partir de réseaux externes ou internes. Les activités de maintenance et de diagnostic locales sont menées par des personnes qui se trouvent physiquement à l'emplacement du système et qui ne communiquent pas au moyen d'une connexion réseau. Les techniques d'authentification utilisées pour établir des sessions de maintenance non locale et de télédiagnostic reflètent les exigences d'accès aux réseaux énoncées dans le contrôle IA-

02. Une authentification robuste exige des authentifiants résistant aux attaques par réinsertion et l'utilisation de l'AMF. Les authentifiants robustes comprennent l'ICP dont les certificats sont stockés dans un jeton protégé par mot de passe, une phrase passe ou des données biométriques. L'application des exigences énoncées dans le contrôle MA-04 est effectuée en partie par d'autres contrôles. Le Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information du Centre pour la cybersécurité (ITSP.30.03) donne des conseils supplémentaires sur une authentification et des authentifiants robustes.

MA-04(01) — Journalisation et examen (---)

Énoncés :

a. Journalisation [Affectation : événements vérifiables définis par l'organisation] pour des sessions de maintenance non locale et de télédiagnostic
b. Passer en revue les enregistrements de vérification des sessions de maintenance non locale et de télédiagnostic pour détecter un comportement anormal

Responsable : Aucun

Discussion :

La journalisation des données de vérification pour la maintenance non locale est appliquée par le contrôle AU-**02.** Les événements vérifiables sont définis dans le contrôle AU-02A.

MA-04(02) — Documenter la maintenance non locale (---)

Énoncés :

Annulé : Intégré aux contrôles MA-01 et MA-04.

Responsable : Aucun

MA-04(03) — Sécurité et nettoyage comparables (---)

Énoncés :

a. Exiger que les services de maintenance non locale et de télédiagnostic soient effectués à partir d'un système qui applique une capacité comparable à celle mise en oeuvre sur le système cible
b. Retirer le composant concerné du système avant l'exécution des activités de maintenance non locale et de télédiagnostic, le nettoyer (en supprimer toute information organisationnelle) et, une fois la réparation effectuée, l'inspecter et le nettoyer à nouveau (pour en éliminer tout logiciel malveillant) avant de le reconnecter au système

Responsable : Aucun

Discussion :

L'application d'une capacité de sécurité comparable sur les systèmes, les outils de diagnostic et l'équipement fournissant des services de maintenance signifie que les contrôles mis en oeuvre sur ces systèmes, outils et équipement sont aussi étendus que ceux sur le système cible.

MA-04(04) — Authentification et séparation des sessions de maintenance (---)

Énoncés :

Protéger les sessions de maintenance non locale en faisant ce qui suit :
a. employer [Affectation : authentifiants résistant aux attaques par réinsertion définis par l'organisation]
b. Séparer les sessions de maintenance des autres sessions avec le système en :
  1. séparant physiquement les chemins de communication
  2. séparant logiquement les chemins de communication

Responsable : Aucun

Discussion :

Les chemins de communication peuvent être séparés logiquement par chiffrement

MA-04(05) — Approbations et avis (---)

Énoncés :

a. Obtenir l'approbation de chaque session de maintenance non locale par [Affectation : personnel ou rôles définis par l'organisation]
b. Aviser le personnel ou les rôles suivants de la date et l'heure de la maintenance non locale planifiée : [Affectation : personnel ou rôles définis par l'organisation]

Responsable : Aucun

Discussion :

Le personnel de maintenance peut se charger des avis. L'approbation d'une session de maintenance non locale se fait par des membres du personnel ayant suffisamment de connaissances des systèmes de la sécurité de l'information pour déterminer la pertinence de la maintenance proposée.

MA-04(06) — Protection cryptographique (---)

Énoncés :

Mettre en oeuvre des mécanismes cryptographiques pour protéger l'intégrité et la confidentialité des communications liées à la maintenance non locale et au télédiagnostic : [Affectation : mécanismes cryptographiques définis par l'organisation].

Responsable : Aucun

Discussion :

L'incapacité de protéger des communications de maintenance non locale et de diagnostic risque de donner à des personnes non autorisées l'accès aux renseignements de l'organisation. Un accès non autorisé durant les sessions de maintenance à distance peut entraîner des actes hostiles, notamment l'insertion de code malveillant, des changements non autorisés aux paramètres système et une exfiltration des renseignements de l'organisation. De tels actes peuvent entraîner une perte ou une dégradation des capacités liées à la mission et aux activités.

MA-04(07) — Vérification de la déconnexion (---)

Énoncés :

Vérifier la fin de la connexion de la session et de la connexion réseau après avoir terminé les sessions de maintenance non locale et de diagnostic.

Responsable : Aucun

Discussion :

Vérifier la fin de la connexion une fois la maintenance terminée assure que les connexions établies durant les sessions de maintenance non locale et de diagnostic sessions ont été coupées et ne peuvent plus être utilisées.

MA-05 — Personnel de maintenance (---)

Énoncés :

a. Établir un processus d'autorisation du personnel de maintenance et tenir à jour une liste des organisations et du personnel autorisé à effectuer les activités de maintenance
b. Vérifier que le personnel non accompagné réalisant des activités de maintenance sur le système dispose des autorisations d'accès nécessaires
c. Désigner des membres du personnel de l'organisation qui possèdent les autorisations d'accès et les compétences techniques nécessaires pour superviser les activités de maintenance effectuées par le personnel qui ne possède pas les autorisations d'accès appropriées

Responsable : Aucun

Discussion :

Le personnel de maintenance fait référence aux personnes qui réalisent les activités de maintenance matérielle ou logicielle sur les systèmes de l'organisation, et le contrôle PE-02 traite de l'accès physique des personnes devant réaliser des activités de maintenance qui les placent dans le périmètre de protection matérielle des systèmes. Les compétences techniques des superviseurs sont liées à la maintenance effectuée sur les systèmes, tandis que la possession des autorisations d'accès appropriées est liée à la maintenance sur et près des systèmes. Les personnes non identifiées au préalable comme étant des membres du personnel autorisés, tels que les fabricants de technologies d'information, les fournisseurs, les intégrateurs de système et les experts-conseils, peuvent demander un accès privilégié aux systèmes organisationnels, comme pour mener des activités de maintenance avec court préavis ou sans préavis. Selon les évaluations organisationnelles des risques, les organisations peuvent octroyer des justificatifs d'identité temporaires à ces personnes. Ces justificatifs peuvent être octroyés pour un accès unique ou pour un délai très limité. L'information sur le personnel de maintenance peut comporter des renseignements personnels et devrait donc être protégée en conséquence.

MA-05(01) — Personnes ne détenant pas l'accès approprié (---)

Énoncés :

a. Mettre en oeuvre des procédures pour les membres du personnel de maintenance qui ne possèdent pas la cote de sécurité appropriée; ces procédures comprennent les exigences suivantes :

1. les membres du personnel de maintenance qui ne possèdent pas les autorisations d'accès, les cotes de sécurité ou les approbations formelles d'accès requises sont escortés et surveillés durant l'exécution des activités de maintenance et de diagnostic sur le système par des employés de l'organisation qui sont pleinement habilités, qui possèdent les autorisations d'accès appropriées et qui sont qualifiés sur le plan technique

2. avant que des membres du personnel qui ne possèdent pas les autorisations d'accès, les cotes de sécurité ou les approbations formelles d'accès requises puissent entreprendre les activités de maintenance ou de diagnostic, tous les composants de stockage d'information volatile du système sont nettoyés, et les supports d'information non volatile sont enlevés ou physiquement déconnectés du système puis rangés dans un endroit sûr

b. Élaborer et mettre en oeuvre [Affectation :contrôles de secours définis par l'organisation] dans l'éventualité où un composant de système ne pourrait pas être nettoyé, supprimé ou débranché du système

Responsable : Aucun

Discussion :

Les procédures à l'intention des personnes qui ne possèdent pas la cote de sécurité appropriée ont été conçues pour empêcher un accès visuel ou électronique à de l'information classifiée ou protégée contenue dans les systèmes organisationnels. Les procédures concernant le personnel de maintenance peuvent être consignées dans les plans de sécurité des systèmes.

MA-05(02) — Habilitations de sécurité pour les systèmes classifiés (---)

Énoncés :

Veiller à ce que les personnes qui effectuent des activités de maintenance et de diagnostic sur un système qui traite, stocke et transmet de l'information classifiée possèdent l'habilitation de sécurité et les approbations d'accès officiels au moins équivalant au niveau de sécurité le plus élevé de l'information contenue dans le système et équivalant aux compartiments de cette information.

Responsable : Aucun

Discussion :

Les membres du personnel qui effectuent la maintenance des systèmes organisationnels peuvent être exposés à de l'information classifiée dans le cadre de leurs activités de maintenance. Pour atténuer le risque inhérent à une telle exposition, les organisations font appel au personnel de maintenance ayant une habilité (c'est-à-dire le personnel qui possède une habilitation de sécurité) correspondant au niveau de classification de l'information stockée dans le système.

MA-05(03) — Exigences relatives à la citoyenneté pour les systèmes classifiés (---)

Énoncés :

Veiller à ce que les personnes qui effectuent des activités de maintenance et de diagnostic sur un système qui traite, stocke et transmet de l'information classifiée soient des citoyennes et citoyens canadiens.

Responsable : Aucun

Discussion :

Les membres du personnel qui effectuent la maintenance des systèmes organisationnels peuvent être exposés à de l'information classifiée dans le cadre de leurs activités de maintenance. Si l'accès à de l'information classifiée dans les systèmes organisationnels est limité aux citoyennes et citoyens canadiens, la même restriction s'applique aux membres du personnel effectuant la maintenance de ces systèmes.

MA-05(04) — Ressortissantes ou ressortissants étrangers (---)

Énoncés :

S'assurer que :
a. des ressortissantes ou ressortissants étrangers habilités ont l'habitude d'exécuter les activités de maintenance et de diagnostic sur des systèmes classifiés seulement lorsque ceux-ci sont possédés et exploités à la fois par le gouvernement canadien et des gouvernements étrangers alliés, ou uniquement par des gouvernements étrangers alliés
b. les approbations, les consentements et les modalités opérationnelles détaillées concernant l'emploi de ressortissantes et ressortissants étrangers pour mener des activités de maintenance et de diagnostic sur des systèmes classifiés sont bien documentés dans un protocole d'entente

Responsable : Aucun

Discussion :

Le personnel qui effectue des activités de maintenance et de diagnostic sur les systèmes organisationnels peut être exposé à de l'information classifiée. Si des citoyennes ou citoyens non canadiens sont autorisés à effectuer des activités de maintenance et de diagnostic sur des systèmes classifiés, alors des mesures de contrôles additionnelles sont nécessaires pour s'assurer que les ententes et les restrictions sont respectées.

MA-05(05) — Maintenance non liée aux systèmes (---)

Énoncés :

L'organisation s'assure que les personnes non accompagnées exécutant des activités de maintenance qui ne sont pas directement liées au système, mais qui sont réalisées à proximité du système, détiennent les autorisations d'accès appropriés.

Responsable : Aucun

Discussion :

Les personnes exécutant des activités de maintenance qui ne sont pas directement liées au système comprennent le personnel d'entretien des installations et le personnel de nettoyage.

MA-06 — Maintenance opportune (---)

Énoncés :

Obtenir des services de maintenance et/ou des pièces de rechange pour les [Affectation : composants de systèmes définis par l'organisation] dans les [Affectation : délais définis par l'organisation] qui suivent la panne.

Responsable : Aucun

Discussion :

Les organisations précisent les composants des systèmes qui représentent un risque accru pour les activités et les biens de l'organisation, les personnes, les autres organisations ou le Québec lorsque les fonctionnalités de ces composants ne sont pas opérationnelles. Les mesures que prend l'organisation pour obtenir des services de maintenance comprennent la mise en place de contrats appropriés.

MA-06(01) — Maintenance préventive (---)

Énoncés :

L'organisation effectue la maintenance préventive des [Affectation : composants de systèmes définis par l'organisation] tous les [Affectation : intervalles définis par l'organisation].

Responsable : Aucun

Discussion :

La maintenance préventive comprend l'entretien courant et la réparation des composants des systèmes pour assurer que l'équipement organisationnel et les installations fonctionnent de façon satisfaisante. Cette maintenance permet systématiquement d'inspecter, de tester, de mesurer et d'ajuster l'équipement, de remplacer des pièces ainsi que de détecter et de corriger les défaillances potentielles avant qu'elles se produisent ou avant qu'elles se transforment en problèmes majeurs. La maintenance préventive vise principalement à éviter ou à atténuer les conséquences des pannes d'équipement. Elle est conçue afin de préserver et de rétablir la fiabilité de l'équipement grâce au remplacement de vieux composants avant qu'ils cessent de fonctionner. Les méthodes à appliquer permettant de déterminer les politiques de gestion préventive des pannes (ou autre) comprennent les recommandations du constructeur, les enregistrements statistiques de panne, l'opinion d'une ou un spécialiste, la maintenance réalisée sur de l'équipement similaire, les exigences du code, les lois ou les règlements dans une juridiction, ou les valeurs mesurées et les indicateurs de rendement.

MA-06(02) — Maintenance prévisionnelle (---)

Énoncés :

Effectuer la maintenance prédictive des [Affectation : composants de systèmes définis par l'organisation] tous les [Affectation : intervalles définis par l'organisation].

Responsable : Aucun

Discussion :

La maintenance prédictive sert à évaluer l'état de l'équipement en surveillant l'état de façon périodique ou continue (en ligne). Elle vise à effectuer la maintenance au moment prévu où les activités de maintenance sont les plus efficaces et avant que le rendement de l'équipement diminue dans un seuil. La composante prévisionnelle découle de l'objectif selon lequel il faut prédire la tendance future en ce qui a trait à l'état de l'équipement. Cette approche utilise des principes de contrôle statistique du processus en vue de déterminer le moment où les activités de maintenance future seront appropriées. Les inspections de maintenance les plus prévisionnelles sont réalisées lorsque l'équipement est en service, ce qui réduit la perturbation des opérations normales du système. La maintenance prévisionnelle peut entraîner des économies considérables ainsi qu'une meilleure fiabilité système.

MA-06(03) — Soutien automatisé pour la maintenance prévisionnelle (---)

Énoncés :

Transférer les données de maintenance prédictive à un système de gestion de la maintenance au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Un système informatisé de gestion des activités de maintenance tient une base de données de l'information sur les activités de maintenance des organisations et automatise le traitement des données sur l'état de l'équipement afin de déclencher la planification, l'exécution et les rapports des activités de maintenance.

MA-07 — Maintenance sur site (---)

Énoncés :

Limiter ou interdire la maintenance sur site des [Affectation : systèmes ou composants de systèmes définis par l'organisation] dans les [Affectation : installations de maintenance de confiance définies par l'organisation].

Responsable : Aucun

Discussion :

La maintenance sur site est le type de maintenance effectuée sur un système ou un composant de système après que le système ou le composant ait été déployé dans un site particulier (c'est-à-dire un environnement opérationnel). Dans certains cas, la maintenance sur site (c'est-à-dire la maintenance locale qui se fait sur un site) peut ne pas être effectuée avec la même rigueur ou les mêmes vérifications de contrôle de la qualité que pour la maintenance au référentiel. Pour ce qui est des systèmes désignés comme étant essentiels par l'organisation, il peut s'avérer nécessaire de limiter ou d'interdire la maintenance sur site au site local, et une telle maintenance devrait être menée dans des installations de confiance avec des contrôles additionnels.

MP

Protection des supports d'information

Media Protection

MP-01 — Politique et procédures de protection des supports (---)

Énoncés :

a. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :

1. une politique de protection des supports [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables

2. des procédures pour faciliter la mise en oeuvre de la politique de protection des supports et des contrôles de protection des supports connexes

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à la protection des supports

c. Passer en revue et mettre à jour, par rapport à la protection des supports :

1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La politique et les procédures de protection des supports abordent les contrôles de la famille MP qui ont été mis en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à l'élaboration de la politique et des procédures de protection des supports. En règle générale, les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin pour des politiques et des procédures propres à la mission ou au système. La politique peut être intégrée à la politique générale de sécurité et de protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures de protection des supports comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.

MP-02 — Accès aux supports (---)

Énoncés :

Restreindre l'accès des [Affectation : types de support numérique et non numérique désignés par l'organisation] aux [Affectation : personnel ou rôles définis par l'organisation].

Responsable : Aucun

Discussion :

Les supports du système comprennent les supports numériques et non numériques. Les supports numériques incluent les disquettes, les disques à mémoire flash, les bandes magnétiques, les disques durs ou à entraînement magnétique externes ou amovibles, les disques compacts (CD) et les disques numériques polyvalents (DVD). Les supports non numériques incluent le papier et les microfilms. Un exemple de restriction des accès aux supports non numériques est de refuser l'accès aux dossiers médicaux des patientes et patients d'une communauté à des personnes autres que les professionnelles et professionnels de soins de santé autorisés à accéder à de tels dossiers. Un exemple de restriction des accès aux supports numériques est de limiter l'accès aux spécifications de conception stockées sur CD dans la bibliothèque des supports aux personnes faisant partie de l'équipe de développement de systèmes.

MP-02(01) — Accès limité automatisé (---)

Énoncés :

Annulé : Intégré au contrôle MP-04(02).

Responsable : Aucun

MP-02(02) — Protection cryptographique (---)

Énoncés :

Annulé : Intégré au contrôle SC-28(01).

Responsable : Aucun

MP-03 — Marquage des supports (---)

Énoncés :

a. Indiquer sur les supports du système d'information les limites de distribution, les mises en garde concernant la manutention et les mentions de sécurité (le cas échéant) de l'information
b. Exempter les [Affectation : types de supports du système définis par l'organisation] de tout marquage s'ils demeurent dans [Affectation : zones contrôlées définies par l'organisation]

Responsable : Aucun

Discussion :

Le « marquage de sécurité » désigne l'application ou l'utilisation d'attributs de sécurité lisibles par des humains. Les supports numériques comprennent des disquettes, des bandes magnétiques, des disques durs externes ou amovibles (par exemple, SSD et à entraînement magnétique), des disques à mémoire flash, des CD et des DVD. Les supports non numériques incluent le papier et les microfilms. L'information protégée est définie par le SCT. Les exigences de protection et de diffusion adéquates pour l'information protégée et classifiée sont définies par le Centre pour la cybersécurité et par le Programme de la sécurité des contrats de Services publics et Approvisionnement Canada (SPAC) à l'annexe C, chapitre 6 du Manuel de la sécurité des contrats. Les marquages de sécurité ne sont généralement pas requis dans le cas des supports qui contiennent de l'information qui, selon l'organisation, est du domaine public ou peut être diffusée publiquement. Certaines organisations peuvent exiger le marquage de l'information publique pour indiquer qu'elle peut être diffusée publiquement. Le marquage des supports du système est conforme aux lois, aux décrets, aux directives, aux politiques, à la réglementation, aux normes et aux lignes directrices applicables.

MP-04 — Entreposage des supports (---)

Énoncés :

a. Contrôler physiquement et entreposer de façon sécurisée les [Affectation : types de support numérique et non numérique définis par l'organisation] dans les [Affectation : zones contrôlées définies par l'organisation]
b. Protéger les types de supports du système définis dans MP-04A jusqu'à ce qu'ils soient détruits ou nettoyés avec de l'équipement, des techniques et des procédures approuvés

Responsable : Aucun

Discussion :

Les supports du système comprennent les supports numériques et non numériques. Les supports numériques comprennent des disques à mémoire flash, des disquettes, des bandes magnétiques, des disques durs externes ou amovibles (par exemple, SSD, à entraînement magnétique), des CD et des DVD. Les supports non numériques incluent le papier et les microfilms. Le contrôle physique des supports stockés comprend la conduite d'inventaires ainsi que de veiller à la mise en place de procédures afin de permettre aux personnes d'emprunter et de retourner des supports dans la bibliothèque et de préserver la responsabilisation des supports stockés. Le stockage sécurisé comprend les tiroirs, les armoires et les bureaux verrouillés ainsi que les bibliothèques de supports contrôlées. Le type d'entreposage de supports dépend de la catégorie de sécurité ou de la classification de l'information sur les supports. Les zones contrôlées sont des espaces qui fournissent des contrôles physiques et procéduraux afin de répondre aux exigences établies pour la protection de l'information et des systèmes. Moins de contrôles peuvent s'avérer nécessaires pour les supports qui contiennent de l'information qui devrait être du domaine public, être diffusée publiquement, ou avoir des incidences négatives limitées sur les organisations, les opérations ou les personnes si des personnes autres que celles autorisées ont accès à cette information. Dans de tels cas, les contrôles d'accès physique procurent une protection adéquate.

MP-04(01) — Protection cryptographique (---)

Énoncés :

Annulé : Intégré au contrôle SC-28(01).

Responsable : Aucun

MP-04(02) — Accès limité automatisé (---)

Énoncés :

Limiter l'accès aux zones de stockage des supports et journaliser les tentatives d'accès et l'accès octroyé au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Les mécanismes automatisés comprennent les pavés numériques, les lecteurs biométriques ou les lecteurs de cartes sur les entrées externes des zones d'entreposage des supports.

MP-05 — Transport des supports (---)

Énoncés :

a. Protéger et contrôler [Affectation : types de supports de système désignés par l'organisation] durant le transport à l'extérieur des zones contrôlées à l'aide de [Affectation : contrôles définis par l'organisation]
b. Demeurer responsable des supports du système durant leur transport hors des zones contrôlées
c. Documenter les activités associées au transport des supports du système
d. Réserver les activités associées au transport des supports au personnel autorisé

Responsable : Aucun

Discussion :

Les supports du système comprennent les supports numériques et non numériques. Les supports numériques comprennent des disques à mémoire flash, des disquettes, des bandes magnétiques, des disques durs externes ou amovibles (par exemple, SSD et à entraînement magnétique), des CD et des DVD. Les supports non numériques incluent le papier et les microfilms. Les zones contrôlées sont des espaces dans lesquels les organisations appliquent des contrôlesphysiques ou procéduraux afin de respecter les exigences établies pour la protection de l'information et des systèmes. Les contrôles visant à protéger les supports lors du transport comprennent la cryptographie et les contenants verrouillés. Certains mécanismes cryptographiques peuvent protéger la confidentialité et l'intégrité de l'information selon les mécanismes mis en oeuvre. Les activités associées au transport des supports comprennent la remise des supports aux fins de transport, la vérification que les supports suivent les processus de transport adéquats et le transport en tant que tel. Le personnel autorisé responsable du transport et de la messagerie peut inclure des personnes de l'extérieur de l'organisation. Préserver la responsabilisation des supports durant le transport comprend la restriction des activités de transport au personnel autorisé et le suivi ou l'obtention des enregistrements officiels des activités de transport, à mesure que les supports se déplacent dans le système de transport, afin de prévenir et de détecter les pertes, les destructions ou les modifications. Les organisations devraient établir les exigences de documentation des activités associées au transport des supports du système conformément aux évaluations organisationnelles des risques. Les organisations peuvent à leur guise définir leurs méthodes de tenue des dossiers pour les différents types de supports dans le contexte d'un système de dossiers afférents au transport.

MP-05(01) — Protection à l'extérieur des zones contrôlées (---)

Énoncés :

Annulé : Intégré au contrôle MP-05.

Responsable : Aucun

MP-05(02) — Documentation des activités (---)

Énoncés :

Annulé : Intégré au contrôle MP-05.

Responsable : Aucun

MP-05(03) — Gardiennes et gardiens (---)

Énoncés :

Faire appel à une gardienne ou un gardien désigné durant le transport des supports du système à l'extérieur des zones contrôlées.

Responsable : Aucun

Discussion :

Les gardiennes et gardiens désignés fournissent à l'organisation des points de contact durant le processus de transport des supports et facilitent la comptabilité individuelle. Les responsabilités qui incombent au gardien peuvent être transférées d'une personne à une autre s'il n'y a aucune ambiguïté quant à l'identité du gardien.

MP-05(04) — Protection cryptographique (---)

Énoncés :

Annulé : Intégré au contrôle SC-28(01).

Responsable : Aucun

MP-06 — Nettoyage des supports (---)

Énoncés :

a. Nettoyer les [Affectation : supports de système définis par l'organisation] avant leur élimination ou leur transfert hors du contrôle de l'organisation ou aux fins de réutilisation au moyen de [Affectation : techniques et procédures de nettoyage définies par l'organisation]
b. Utiliser des mécanismes de nettoyage dont la robustesse et l'intégrité correspondent à la catégorie de sécurité ou à la classification de l'information

Responsable : Aucun

Discussion :

Le nettoyage des supports s'applique à tous les supports de systèmes numériques et non numériques sujets à une élimination ou à une réutilisation, que les supports soient considérés comme amovibles ou non. Il peut s'agir, par exemple, de supports numériques qui se trouvent dans les numériseurs, les photocopieurs, les imprimantes, les ordinateurs blocs-notes, les postes de travail, les composants réseau, les appareils mobiles et les supports non numériques (par exemple, papier et microfilm). Le processus de nettoyage supprime l'information sur les supports de manière à ce qu'il soit impossible de la récupérer ou de la reconstituer. Les techniques de nettoyage, notamment l'effacement, l'épuration, l'effacement cryptographique, la dépersonnalisation des renseignements personnels et la destruction, empêchent la divulgation d'information à des personnes non autorisées lorsque les supports sont réutilisés ou transférés aux fins d'élimination. L'organisation détermine les méthodes de nettoyage appropriées tout en sachant qu'il est parfois nécessaire de détruire les supports si ces derniers ne peuvent être soumis à aucune autre méthode de nettoyage. L'organisation utilise à sa discrétion les techniques et procédures approuvées de nettoyage des supports qui contiennent de l'information du domaine public, ou qui peut être diffusée publiquement, ou dont le transfert à des fins de réutilisation ou d'élimination n'a pas d'incidence négative sur l'organisation ou les personnes. Le nettoyage des supports non numériques comprend la destruction ou la suppression d'une annexe classifiée dans un document autrement non classifié ou la rédaction de certaines sections ou de certains mots tirés d'un document en masquant les sections ou mots triturés aussi efficacement que s'ils avaient été supprimés du document.

MP-06(01) — Examen, approbation, suivi, documentation et vérification (---)

Énoncés :

Passer en revue, approuver, suivre, documenter et vérifier le nettoyage des supports et les activités d'élimination.

Responsable : Aucun

Discussion :

L'organisation examine et approuve les supports à nettoyer pour en assurer la conformité aux stratégies de conservation des dossiers. Les mesures de suivi et de documentation comprennent : dresser la liste du personnel ayant passé en revue et approuvé les activités de nettoyage et d'élimination, les types de supports nettoyés, les fichiers enregistrés sur le support, les méthodes de nettoyage employées, la date et l'heure des activités de nettoyage, le personnel ayant procédé au nettoyage, les activités de vérification qui ont été menées, le personnel ayant procédé à la vérification et les activités d'élimination qui ont été prises. Les organisations devraient s'assurer que le nettoyage des supports a bien été fait avant l'élimination.

MP-06(02) — Mise à l'essai du matériel (---)

Énoncés :

Tester les procédures et l'équipement de nettoyage [Affectation : fréquence définie par l'organisation] pour s'assurer que le nettoyage prévu a bien été réalisé.

Responsable : Aucun

Discussion :

La mise à l'essai de l'équipement et des procédures de nettoyage peut être réalisée par des entités externes qualifiées et autorisées, notamment des ministères ou organismes, ou fournisseurs de services externes).

MP-06(03) — Techniques non destructives (---)

Énoncés :

Appliquer un nettoyage des dispositifs de stockage portatifs au moyen de techniques de nettoyage non destructives avant de les connecter au système dans les situations suivantes : [Affectation : liste définie par l'organisation des circonstances où les dispositifs de stockage portatifs doivent être nettoyés].

Responsable : Aucun

Discussion :

Les dispositifs de stockage portatifs comprennent des disques durs externes ou amovibles (par exemple, SSD et à entraînement magnétique), des disques optiques, des bandes magnétiques ou optiques, des dispositifs à mémoire des cartes à mémoire flash et d'autres disques externes ou amovibles. Les dispositifs de stockage portatifs peuvent provenir de sources douteuses. Ils peuvent contenir du code malveillant susceptible d'être inséré ou transmis aux systèmes organisationnels par des ports USB ou d'autres portails d'entrée. Bien que l'analyse des dispositifs de stockage soit recommandée, le nettoyage offre une assurance additionnelle que ces dispositifs sont exempts de tout code malveillant. Les organisations devraient envisager de nettoyer les dispositifs de stockage portatifs de façon non destructrice au moment de l'achat chez un fabricant ou un fournisseur et avant leur utilisation, ou lorsque les organisations ne peuvent pas assurer la chaîne de possession.

MP-06(04) — Information protégée (---)

Énoncés :

Annulé : Intégré au contrôle MP-06.

Responsable : Aucun

MP-06(05) — Information classifiée (---)

Énoncés :

Annulé : Intégré au contrôle MP-06.

Responsable : Aucun

MP-06(06) — Destruction de supports (---)

Énoncés :

Annulé : Intégré au contrôle MP-06.

Responsable : Aucun

MP-06(07) — Double autorisation (---)

Énoncés :

Appliquer l'exigence de double autorisation pour le nettoyage des [Affectation : supports de système définis par l'organisation].

Responsable : Aucun

Discussion :

L'organisation fait appel à une double autorisation pour aider à assurer que le nettoyage des supports du système ne puisse être effectué que sous la supervision de deux personnes qualifiées sur le plan technique. Les personnes qui procèdent au nettoyage des supports du système possèdent les compétences et l'expertise suffisantes pour déterminer si le nettoyage proposé respecte les normes, les politiques et les procédures gouvernementales et de l'organisation. Une double autorisation permet également de s'assurer que le nettoyage s'effectue comme prévu, tout en évitant les erreurs et de fausses indications que des mesures de nettoyage ont été réalisées. La double autorisation est également appelée le contrôle par deux personnes. Pour réduire le risque de collusion, les organisations devraient considérer la rotation des tâches à double autorisation avec d'autres particuliers.

MP-06(08) — Purge ou nettoyage à distance de l'information (---)

Énoncés :

Fournir la capacité de purger ou de nettoyer l'information à partir de [Affectation : systèmes désignés par l'organisation] [Sélection (un choix) : à distance; selon les modalités suivantes : {Affectation : modalités définies par l'organisation}].

Responsable : Aucun

Discussion :

Une purge ou un nettoyage à distance d'information permet de protéger l'information sur les systèmes et composants des systèmes organisationnels si ceux-ci ont été obtenus par des personnes non autorisées. Les commandes de purge ou de nettoyage à distance exigent une authentification forte afin d'atténuer les risques que des personnes non autorisées procèdent à la purge ou au nettoyage du système, du composant ou du dispositif. La fonction de purge ou de nettoyage peut être mise en oeuvre de différentes façons, notamment en remplaçant les données ou l'information à plusieurs reprises ou en détruisant la clé nécessaire au déchiffrage des données chiffrées.

MP-07 — Utilisation des supports (---)

Énoncés :

a. [Sélection (un choix) : Limiter, interdire] l'utilisation de [Affectation : types de supports de système désignés par l'organisation] sur les [Affectation : systèmes ou composants de systèmes désignés par l'organisation] au moyen de [Affectation : contrôles définis par l'organisation]
b. Interdire dans ses systèmes l'utilisation de dispositifs de stockage portatifs dont la ou le propriétaire est inconnu

Responsable : Aucun

Discussion :

Les supports du système comprennent les supports numériques et non numériques. Les supports numériques comprennent des disquettes, des bandes magnétiques, des disques à mémoire flash, des CD, des DVD et des disques durs amovibles. Les supports non numériques incluent le papier et les microfilms. Les protections d'utilisation des supports s'appliquent également aux appareils mobiles ayant des capacités de stockage d'information. Contrairement au contrôle MP-02, qui restreint l'accès des utilisatrices et utilisateurs aux supports, le contrôle MP-07 limite l'utilisation de certains types de supports sur les systèmes comme, entre autres, restreindre ou interdire l'utilisation de clés USB ou de lecteurs de disques durs externes. Les organisations ont recours à des contrôles techniques et non techniques pour limiter l'utilisation de supports de systèmes. Elle peut restreindre l'utilisation de dispositifs de stockage portatifs en mettant notamment en place des cages sur les postes de travail pour interdire l'accès à certains ports externes ou en désactivant la fonction qui permet d'insérer, de lire ou d'écrire sur de tels dispositifs. Les organisations peuvent également limiter l'utilisation des dispositifs de stockage portatifs à ceux approuvés, y compris les dispositifs fournis par l'organisation, les dispositifs fournis par d'autres organisations approuvées et les dispositifs qui n'appartiennent pas aux personnes. Elle peut enfin restreindre l'utilisation de dispositifs de stockage portatifs en fonction du type de dispositif, notamment en interdisant l'utilisation de dispositifs de stockage portatifs inscriptibles et en désactivant la fonction qui permet d'écrire sur de tels dispositifs. Exiger des propriétaires identifiables pour les dispositifs de stockage permet de réduire le risque d'utilisation de tels dispositifs en laissant les organisations attribuer la responsabilité en cas de vulnérabilité connue dans les dispositifs.

MP-07(01) — Interdire l’utilisation sans propriétaire (---)

Énoncés :

Annulé : Intégré au contrôle MP-07.

Responsable : Aucun

MP-07(02) — Interdire l'utilisation de supports résistant au nettoyage (---)

Énoncés :

Interdire l'utilisation de supports résistant au nettoyage dans les systèmes organisationnels.

Responsable : Aucun

Discussion :

La résistance au nettoyage fait référence à la résistance des supports par rapport aux techniques de nettoyage non destructrices sur le plan de la capacité à purger l'information des supports. Certains types de supports ne prennent pas en charge les commandes de nettoyage ou, si c'est le cas, n'emploient pas d'interfaces communes à chacun. Les supports résistant au nettoyage comprennent les cartes flash compactes, les lecteurs flash intégrés aux cartes et aux dispositifs, les disques électroniques et les supports amovibles USB.

MP-08 — Déclassement des supports (---)

Énoncés :

a. Établir [Affectation : processus de déclassement des supports du système défini par l'organisation] qui comprend le recours à des mécanismes de déclassement dont la robustesse et l'intégrité correspondent à la catégorie de sécurité ou à la classification de l'information
b. Veiller à ce que le processus de déclassement des supports du système corresponde à la catégorie de sécurité et/ou au niveau de classification de l'information à supprimer et des autorisations d'accès des potentiels destinataires de l'information déclassée
c. Identifier les [Affectation : supports du système à déclasser définis par l'organisation]
d. Employer le processus établi pour déclasser les supports de système

Responsable : Aucun

Discussion :

Le déclassement des supports s'applique aux supports numériques et non numériques susceptibles d'être diffusés à l'extérieur de l'organisation, qu'ils soient amovibles ou non. Lorsqu'il est appliqué aux supports du système, le processus de déclassement supprime l'information des supports, généralement selon la catégorie de sécurité ou le niveau de classification, de manière à rendre l'information irrécupérable et impossible à reconstituer. Le déclassement des supports comprend la rédaction de l'information aux fins de divulgation et de distribution à un plus vaste public. Le déclassement s'assure que l'espace vide sur les supports est dépourvu d'information.

MP-08(01) — Documentation du processus (---)

Énoncés :

Documenter les mesures de déclassement des supports du système.

Responsable : Aucun

Discussion :

L'organisation peut documenter le processus de déclassement des supports en fournissant de l'information comme la technique de déclassement employée, le numéro d'identification des supports déclassés et l'identité des personnes qui ont autorisé et/ou effectué le déclassement.

MP-08(02) — Mise à l'essai du matériel (---)

Énoncés :

Tester les procédures et l'équipement de déclassement [Affectation : fréquence définie par l'organisation] pour s'assurer que les mesures de déclassement ont ben été réalisées.

Responsable : Aucun

MP-08(03) — Information protégée (---)

Énoncés :

Déclasser les supports du système comportant de l'information protégée avant toute diffusion publique.

Responsable : Aucun

MP-08(04) — Information classifiée (---)

Énoncés :

Déclasser les supports de système comportant de l'information classifiée avant de les rendre publics sans autorisation d'accès obligatoire.

Responsable : Aucun

PE

Sécurité physique des installations

Physical and Environmental Protection

PE-01 — Politique et procédures de protection physique et environnementale (---)

Énoncés :

a. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :

1. une stratégie de protection physique et environnementale [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables

2. des procédures pour faciliter la mise en oeuvre de la politique de protection physique et environnementale ainsi que des contrôles de protection physique et environnementale connexes

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures de protection physique et environnementale

c. Passer en revue et mettre à jour, par rapport à la protection physique et environnementale :

1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La politique et les procédures de protection physique et environnementale abordent les contrôles de la famille PE qui ont été mis en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à l'élaboration de la politique et des procédures de protection physique et environnementale. En règle générale, les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin pour des politiques et des procédures propres à la mission ou au système. La politique peut être intégrée à la politique générale de sécurité et de protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures de protection physique et environnementale comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.

PE-02 — Autorisations d’accès physique (---)

Énoncés :

a. Développer, approuver et tenir une liste des personnes disposant d’un accès autorisé à l’installation où se trouvent les systèmes
b. Émettre des justificatifs d’identité pour autoriser l’accès à l’installation
c. Passer en revue la liste d’accès qui fournit les détails quant aux personnes autorisées à accéder aux installations [Affectation : fréquence définie par l’organisation]
d. Retirer les personnes de la liste d’accès aux installations lorsqu’un tel accès n’est plus nécessaire

Responsable : Aucun

Discussion :

Les autorisations d’accès physique s’appliquent au personnel, aux visiteuses et aux visiteurs. Les personnes avec des justificatifs d’identité d’autorisation d’accès physique permanents ne sont pas considérées comme des visiteuses et visiteurs. Les justificatifs d’autorisation comprennent les laissez-passer, les cartes d’identité et les cartes à puce. Les organisations doivent déterminer la force des justificatifs d’autorisation nécessaires en fonction des lois, des décrets, des directives, de la réglementation, des politiques, des normes et des lignes directrices applicables. Il se peut que les autorisations d’accès physique ne soient pas nécessaires pour accéder à certaines zones dans les installations qui sont désignées comme zones d’accès public.

PE-02(01) — Accès par poste ou rôle (---)

Énoncés :

Autoriser l'accès physique à l'installation qui héberge le système selon le poste ou le rôle de l'employée ou employé.

Responsable : Aucun

Discussion :

L'accès à l'installation basé sur le rôle comprend l'accès au personnel permanent autorisé et de maintenance régulière/ systématique, aux agentes et agents de service, au personnel médical d'urgence.

PE-02(02) — Deux formes d’identification (---)

Énoncés :

Exiger deux formes d’identification à partir des documents d’identification suivants pour l’accès aux visiteuses et visiteurs dans l’édifice où se trouvent les systèmes : [Affectation : liste des formes acceptables d’identification définies par l’organisation].

Responsable : Aucun

Discussion :

Des exemples de formes acceptables d’identification comprennent les passeports, des cartes d’identité émises par le gouvernement fédéral, un gouvernement provincial ou territorial et des cartes d’identité de service militaire. Pour avoir accès à des installations au moyen de mécanismes automatisés, les organisations peuvent se servir de cartes d’entrée à identification par radiofréquence (RFID pour Radio Frequency Identification), de NIP et de biométrie. Les organisations doivent admettre que ces formes d’identification relèvent de renseignements personnels et ceux-ci doivent donc être protégés en conséquence.

PE-02(03) — Accès restreint sans escorte (---)

Énoncés :

Restreindre les accès sans escorte à l'installation qui héberge le système au personnel qui [Sélection (un choix ou plus) : possède les habilitations de sécurité pour toute l'information contenue dans le système; est formellement autorisé à accéder à toute l'information contenue dans le système; nécessite un accès à toute l'information contenue dans le système; {Affectation : autorisations d'accès physique définies par l'organisation}].

Responsable : Aucun

Discussion :

Les personnes qui ne possèdent pas l'habilitation de sécurité, les approbations d'accès nécessaires ou qui n'ont pas besoin de savoir, sont escortées par des membres du personnel qui possèdent les autorisations d'accès physique appropriées pour veiller à ce que l'information ne soit pas exposée ou compromise.

PE-02(400) — Exigences des cartes d’identité (---)

Énoncés :

S’assurer que les cartes d’identité respectent les exigences avant leur remise.

Responsable : Aucun

PE-03 — Contrôle d'accès physique (---)

Énoncés :

a. Appliquer les autorisations d'accès physique aux [Affectation : points d'entrée et de sortie définis par l'organisation de l'installation où se trouvent les systèmes] des façons suivantes :

1. vérification des autorisations d'accès avant d'accorder l'accès aux installations

2. en contrôlant l'entrée et la sortie de l'installation au moyen de [Sélection (un choix ou plus) : {Affectation : systèmes/dispositifs de contrôle d'accès physique désignés par l'organisation}; mécanismes de protection]

b. Tenir des journaux de vérification d'accès physique pour [Affectation : points d'entrée et de sortie définis par l'organisation]

c. Contrôler l'accès aux zones au sein de l'installation désignée comme étant accessible au public en mettant en oeuvre les contrôles suivants : [Affectation : contrôles d'accès physique définis par l'organisation]

d. Accompagner les visiteuses et visiteurs et contrôler leurs activités [Affectation : circonstances définies par l'organisation exigeant que les visiteuses et visiteurs soient accompagnés et qu'il y ait un contrôle de leurs activités]

e. Fournir des clés sécurisées, des cartes d'accès, des cadenas, des coffres-forts ou d'autres dispositifs d'accès physique

f. Inventaire [Affectation : dispositifs d'accès physique définis par l'organisation] tous les [Affectation : fréquence définie par l'organisation]

g. Modifier les combinaisons et les clés [Affectation : fréquence définie par l'organisation] lorsque des clés sont perdues, lorsque des combinaisons sont compromises ou lorsque des employées et employés en possession de clés ou de cadenas sont transférés ou quittent leur poste a

a. Retirer l'identifiant de la carte d'accès de la liste ou la base de données des accès [Affectation : fréquence définie par l'organisation] lorsque la carte d'accès est perdue, égarée ou volée, ou lorsque la personne en possession de la carte est transférée ou quitte son poste

Responsable : Aucun

Discussion :

Les contrôles d'accès physique s'appliquent au personnel, aux visiteuses et aux visiteurs. Les personnes avec des autorisations d'accès physique permanentes ne sont pas considérées comme des visiteuses et visiteurs. Les contrôles d'accès physiques pour les zones accessibles au public peuvent comprendre les journaux ou registres de contrôle d'accès physique, les mécanismes de protection ou les dispositifs ou barrières d'accès physique servant à prévenir les déplacements des zones accessibles au public aux zones non publiques. Les organisations doivent déterminer les types de mécanismes de protection nécessaires, y compris le personnel de sécurité professionnel, les utilisatrices et utilisateurs du système ou le personnel administratif. Les dispositifs de contrôle d'accès physique comprennent les clés, les verrous, les cadenas, les lecteurs biométriques et les lecteurs de cartes. Les systèmes de contrôle d'accès physique doivent être conformes aux lois, aux décrets, aux directives, aux politiques, à la réglementation, aux normes et aux lignes directrices applicables. Les organisations peuvent employer les types de journaux de vérification de leur choix. Les journaux de vérification peuvent être procéduraux, automatisés ou une combinaison des deux. Les points d'accès physique peuvent inclure les points d'accès à l'installation, les points d'accès intérieurs aux systèmes qui exigent des contrôles d'accès supplémentaires ou les deux. Les composants des systèmes peuvent se trouver dans des zones désignées comme étant accessibles au public auxquelles les organisations contrôlent l'accès.

PE-03(01) — Accès au système (---)

Énoncés :

Appliquer les autorisations d'accès physique au système en plus des contrôles d'accès physique à l'installation qui se trouve dans [Affectation : espaces physiques définis par l'organisation qui contiennent un ou plusieurs composants du système].

Responsable : Aucun

Discussion :

Le contrôle de l'accès physique au système procure une sécurité physique accrue dans les zones des installations où sont concentrés des composants de systèmes.

PE-03(02) — Installation et systèmes (---)

Énoncés :

Effectuer des vérifications de sécurité [Affectation : fréquence définie par l'organisation] au périmètre physique de l'installation ou du système pour détecter toute exfiltration d'information ou retrait de composants de systèmes.

Responsable : Aucun

Discussion :

L'organisation détermine la portée, la fréquence et/ou le caractère aléatoire des vérifications de sécurité pour atténuer de manière adéquate les risques associés aux exfiltrations.

PE-03(03) — Garde continue (---)

Énoncés :

Mettre en place des gardiennes et gardiens de sécurité pour contrôler en permanence [Affectation : points d'accès physique définis par l'organisation] de l'installation qui héberge le système.

Responsable : Aucun

Discussion :

Placer des gardiennes et des gardiens de sécurité aux points d'accès physique sélectionnés de l'installation permet de fournir aux organisations une capacité d'intervention plus rapide. Les gardiennes et gardiens de sécurité assurent également une surveillance humaine dans les zones de l'installation qui ne sont pas couvertes par la vidéo surveillance.

PE-03(04) — Contenants verrouillables (---)

Énoncés :

Utiliser des contenants verrouillables pour protéger [Affectation : composants de système définis par l'organisation] contre les accès physiques non autorisés.

Responsable : Aucun

Discussion :

Le plus grand risque lorsque des dispositifs portables sont utilisés, comme des téléphones intelligents, des tablettes et des ordinateurs blocs-notes, est le vol. Les organisations peuvent se servir de contenants verrouillables pour réduire ou éliminer le risque de vol d'équipement ou de trafiquage. Ces contenants peuvent être de tailles variées, allant d'unités qui protègent un seul ordinateur bloc-notes aux vastes enceintes pouvant protéger plusieurs serveurs, ordinateurs et périphériques. Les contenants verrouillables peuvent être utilisés avec des câbles de sécurité ou des plaques de protection pour empêcher le vol du contenant verrouillé renfermant l'équipement informatique.

PE-03(05) — Protection antitrafiquage (---)

Énoncés :

Employer des [Affectation : technologies antitrafiquage définies par l'organisation] pour [Sélection (un choix ou plus) : détecter; empêcher] le trafiquage physique ou la modification des [Affectation : composants matériels définis par l'organisation] du système.

Responsable : Aucun

Discussion :

L'organisation peut mettre en place des mesures de détection et de prévention du trafiquage sur les composants matériels sélectionnés, ou encore des mesures de détection sur certains et des mesures de prévention sur d'autres. Les activités de détection et de prévention peuvent utiliser plusieurs types de mécanismes d'inviolabilité, notamment des étiquettes et des revêtements d'inviolabilité. Les programmes antitrafiquage permettent de détecter les modifications apportées au matériel à la suite d'un acte de contrefaçon et d'autres risques liés à la chaîne d'approvisionnement.

PE-03(06) — Tests d’intrusion des installations (---)

Énoncés :

Annulé : Intégré au contrôle CA-08.

Responsable : Aucun

PE-03(07) — Barrières physiques (---)

Énoncés :

Restreindre l’accès au moyen de barrières physiques.

Responsable : Aucun

Discussion :

Les barrières physiques comprennent les bornes de protection, les dalles de protection, les barrières de Jersey et les barrières hydrauliques destinées aux véhicules.

PE-03(08) — Vestibules de contrôle d’accès (---)

Énoncés :

Employer des vestibules de contrôle d’accès dans [Affectation : emplacements dans l’installation définis par l‘organisation].

Responsable : Aucun

Discussion :

Un vestibule de contrôle d’accès fait partie d’un système de contrôle d’accès qui fournit en général un espace entre deux jeux de portes à verrouillage réciproque. Les vestibules sont conçus pour empêcher que des personnes non autorisées suivent des personnes autorisées dans des installations dotées d’un accès contrôlé. Cette activité, aussi appelée accès à califourchon ou talonnage, résulte d’un accès non autorisé à l’installation. Les contrôleurs de portes à verrouillage réciproque peuvent être utilisés pour limiter le nombre de personnes entrant dans les points d’accès contrôlé et pour assurer des zones de confinement pendant que l’autorisation de l’accès physique est vérifiée. Ces contrôleurs peuvent être entièrement automatisés (c’est-à-dire qu’ils peuvent contrôler l’ouverture et la fermeture des portes) ou partiellement automatisés (c’est-à-dire utiliser des mécanismes de protection pour contrôler le nombre de personnes qui entrent dans la zone de confinement).

PE-03(400) — Inspections de sécurité (---)

Énoncés :

Effectuer des inspections de sécurité dans les installations où de l'information ou des biens de nature délicate sont traités ou stockés, ou qui appuient des activités ou des services essentiels.

Responsable : Aucun

PE-04 — Contrôle d’accès pour la transmission (---)

Énoncés :

Contrôler l’accès physique aux [Affectation : lignes de distribution et de transmission du système définies par l’organisation] dans ses installations utilisant les [Affectation : contrôles de sécurité définis par l’organisation].

Responsable : Aucun

Discussion :

Les contrôles de sécurité appliqués aux lignes de distribution et de transmission des systèmes permettent de prévenir les dommages accidentels, les pannes et les modifications physiques. De tels contrôles peuvent également être nécessaires afin d’éviter l’écoute clandestine ou la modification des transmissions non chiffrées. Les contrôles de sécurité servant à contrôler l’accès physique aux lignes de distribution et de transmission des systèmes incluent la déconnexion ou le verrouillage des connecteurs non utilisés, le verrouillage des armoires de câblage, la protection du câblage par des conduits ou des chemins de câbles et l’écoute électronique des capteurs.

PE-05 — Contrôle d’accès aux dispositifs de sortie (---)

Énoncés :

Contrôler l’accès physique aux données transmises par les [Affectation : dispositifs de sortie définis par la ou le propriétaire du système] pour empêcher les personnes non autorisées d’obtenir les données de sortie.

Responsable : Aucun

Discussion :

Les contrôles de l’accès physique aux dispositifs de sortie incluent le rangement des dispositifs de sortie dans des pièces verrouillées ou d’autres zones sécurisées dotées d’un contrôle d’accès avec clavier numérique ou lecteur de cartes et auxquelles seules les personnes autorisées peuvent accéder, le rangement des dispositifs de sortie dans des emplacements pouvant être surveillés par le personnel, l’installation de filtres d’écran et l’utilisation de casques d’écoute. Les écrans, les imprimantes, les numériseurs, les dispositifs audio, les télécopieurs et les photocopieurs sont des exemples de dispositifs de sortie.

PE-05(01) — Accès à la sortie par personnes autorisées (---)

Énoncés :

Annulé : Intégré au contrôle PE-05.

Responsable : Aucun

PE-05(02) — Associer l’identité des individus (---)

Énoncés :

Associer l’identité des individus aux données transmises par le dispositif.

Responsable : Aucun

Discussion :

Les méthodes permettant d’associer l’identité des individus aux données transmises à partir des dispositifs de sortie comprennent l’installation de fonctionnalité de sécurité sur des télécopieurs, des copieurs et des imprimantes. Une telle fonctionnalité permet la mise en place de fonctions de sécurité sur les imprimantes, les photocopieurs et les télécopieurs permettant à l’organisation d’authentifier les utilisatrices et utilisateurs sur les dispositifs de sortie avant de leur transmettre les données de sortie.

PE-05(03) — Marquage des dispositifs de sortie (---)

Énoncés :

Annulé : Intégré au contrôle PE-22.

Responsable : Aucun

PE-06 — Surveillance de l’accès physique (---)

Énoncés :

a. Surveiller l’accès physique aux installations où se trouvent les systèmes afin de détecter et d’intervenir en cas d’incident de sécurité physique
b. Examiner les journaux d’accès physique tous les [Affectation : fréquence définie par l’organisation] et à la suite de [Affectation : événements ou indications potentielles d’événement définis par l’organisation]
c. Coordonner les résultats des examens et des enquêtes avec sa capacité d’intervention en cas d’incident

Responsable : Aucun

Discussion :

La surveillance de l’accès physique s’applique aux zones à accès public dans les installations de l’organisation. Elle peut être effectuée par des gardes de sécurité, de l’équipement de vidéosurveillance (c’est-à-dire les caméras) et des capteurs. L’examen des journaux d’accès physique peut aider à repérer les activités suspectes, les événements anormaux ou les menaces. Les examens peuvent être appuyés par les contrôles de journalisation des données de vérification, comme le contrôle AU-02, si les journaux d’accès font partie d’un système automatisé. Les capacités d’intervention en cas d’incident de l’organisation incluent les enquêtes associées aux incidents de sécurité physique et les interventions connexes. Les incidents comprennent les infractions de sécurité ou les activités d’accès physique suspectes. Les activités d’accès physique suspectes incluent les accès hors des heures normales de travail, les accès répétés aux zones auxquelles on n’accède pas normalement, les accès d’une durée anormalement longue et les accès ne respectant pas l’ordre établi.

PE-06(01) — Alarmes de détection d'intrusion et équipement de surveillance (---)

Énoncés :

Surveiller l'accès physique aux installations où se trouvent les systèmes au moyen d'alarmes de détection d'intrusion physique et d'équipement de surveillance.

Responsable : Aucun

Discussion :

Les alarmes de détection d'intrusion physique peuvent être utilisées pour alerter le personnel de sécurité lors d'une tentative d'accès non autorisé à l'installation. Les systèmes d'alarme fonctionnent de concert avec des barrières physiques, des systèmes de contrôle d'accès physique et des mécanismes de protection en déclenchant une intervention lorsque ces autres formes de sécurité ont été compromises ou ont fait l'objet d'une atteinte à la sécurité. Les alarmes de détection d'intrusion peuvent comprendre différents types de dispositifs de capteur, comme des détecteurs de mouvement, des capteurs à contact et des détecteurs de bris de verre. L'équipement de surveillance comprend les caméras installées à des endroits stratégiques dans l'ensemble de l'installation. Si des vidéos de surveillance sont enregistrées, cela peut constituer des renseignements personnels et ces renseignements devraient être protégés adéquatement.

PE-06(02) — Automatisation de la reconnaissance des intrusions et des interventions (---)

Énoncés :

Reconnaître [Affectation : classes ou types d'intrusions définis par l'organisation] et appliquer [Affectation : mesures d'intervention définies par l'organisation] au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Les mesures d'intervention peuvent comprendre l'envoi de notifications au personnel de l'organisation ou responsable de l'application de la loi sélectionné. Les mécanismes automatisés qui ont été mis en oeuvre pour appliquer des mesures d'intervention comprennent des notifications des alertes, des courriels et des messages texte, ainsi que l'activation de mécanismes de verrouillage des portes. La surveillance de l'accès physique peut être coordonnée avec les systèmes de détection des intrusions et les capacités de surveillance des systèmes pour fournir une couverture des menaces intégrée pour l'organisation. Des précautions doivent être prises pour s'assurer de recueillir et de communiquer une quantité minimale de renseignements personnels dans le cadre de la reconnaissance des intrusions et des interventions.

PE-06(03) — Surveillance vidéo (---)

Énoncés :

a. Employer la vidéo surveillance des [Affectation : secteurs opérationnels définis par l'organisation]
b. Examiner les enregistrements vidéo [Affectation : fréquence définie par l'organisation]
c. Conserver les enregistrements vidéo pendant [Affectation : délais définis par l'organisation]

Responsable : Aucun

Discussion :

La surveillance vidéo vise l'enregistrement de vidéos aux fins d'examen ultérieur, si les circonstances le justifient. Les enregistrements vidéo font en général l'objet d'un examen pour détecter des événements ou des incidents anormaux. Il n'est pas obligatoire de surveiller la vidéo de surveillance, même si l'organisation peut décider de le faire. Une évaluation des menaces et des risques (EMR) permettra de mieux déterminer les détails de la conservation, du stockage, de l'utilisation ou de la diffusion de la vidéo. Avant d'installer des systèmes de surveillance vidéo (CCTV), il est important de faire des recherches relatives aux lois et réglementations locales. Les enregistrements vidéo peuvent recueillir et stocker des renseignements personnels et devraient donc être protégés de façon appropriée.

PE-06(04) — Surveillance de l’accès physique aux systèmes (---)

Énoncés :

Surveiller l’accès physique au système en plus de l’accès physique à l’installation qui se trouve dans [Affectation : espaces physiques définis par l’organisation qui contiennent un ou plusieurs composants du système].

Responsable : Aucun

Discussion :

La surveillance de l’accès physique au système offre une plus grande surveillance des secteurs de l’installation où se retrouvent la plupart des composants du système, notamment les salles de serveurs, les aires d’entreposage des supports et les centres de communications. La surveillance de l’accès physique peut être coordonnée avec les systèmes de détection des intrusions et les capacités de surveillance des systèmes pour fournir une couverture des menaces approfondie et intégrée pour l’organisation.

PE-07 — Contrôle des visiteuses et visiteurs (---)

Énoncés :

Annulé : Intégré aux contrôles PE-02 et PE-03.

Responsable : Aucun

PE-08 — Registre des accès des visiteuses et visiteurs (---)

Énoncés :

a. Tenir un registre des accès des visiteuses et visiteurs à l'installation où se trouve le système pendant [Affectation : délais définis par l'organisation]
b. Examiner le registre des accès des visiteuses et visiteurs [Affectation : fréquence définie par l'organisation]
c. Signaler les anomalies dans le registre des accès des visiteuses et visiteurs à [Affectation : personnel défini par l'organisation]

Responsable : Aucun

Discussion :

Le registre des accès des visiteuses et visiteurs comprend le nom de la personne et son organisation, sa signature, les formes d'identification, la date de l'accès, les heures d'arrivée et de départ, le but de la visite, et le nom et l'organisation de la personne visitée. Les examens du registre des accès déterminent si les autorisations d'accès sont à jour et s'il est toujours nécessaire pour soutenir la mission et les activités d'organisation. Un tel registre n'est pas requis dans les lieux publics. Les signatures et l'identification des visiteuses et visiteurs, ainsi que (à l'occasion) l'objet de la visite, peuvent être considérées comme étant des renseignements personnels qu'il convient de protéger en conséquence. Les organisations devraient s'adresser à la ou au haut fonctionnaire ou cadre supérieur approprié en matière de protection de la vie privée pour obtenir de l'information.

PE-08(01) — Tenue et examen automatisés du registre (---)

Énoncés :

Tenir un registre des accès des visiteuses et visiteurs au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Les registres des accès des visiteuses et visiteurs peuvent être stockés et tenus dans une base de données accessible au personnel de l'organisation pour lequel le besoin de savoir a été consigné. L'accès automatisé à ces registres facilite les examens des registres sur une base régulière afin de déterminer si les autorisations d'accès sont à jour et si elles sont toujours nécessaires pour soutenir la mission et les activités d'organisation. Un examen de cette base de données doit être effectué périodiquement pour s'assurer de la conformité au calendrier de conservation approuvé par l'organisation.

PE-08(02) — Registre des accès physiques (---)

Énoncés :

Annulé : Intégré au contrôle PE-02.

Responsable : Aucun

PE-08(03) — Limitation des éléments liés aux renseignements personnels (---)

Énoncés :

Limiter les renseignements personnels contenus dans les registres d'accès des visiteuses et visiteurs aux éléments suivants identifiés dans l'évaluation des risques d'atteinte à la vie privée : [Affectation : éléments définis par l'organisation].

Responsable : Aucun

Discussion :

L'organisation peut avoir des exigences qui précisent le contenu des registres des accès des visiteuses et visiteurs. Des précautions doivent être prises pour s'assurer de recueillir et de stocker une quantité minimale de renseignements personnels pour les registres des accès des visiteuses et visiteurs lorsque ces renseignements ne sont pas nécessaires à des fins opérationnelles. Cela contribuera à réduire le niveau de risque d'atteinte à la vie privée créé par un tel système.

PE-09 — Équipement et câblage d’alimentation (---)

Énoncés :

Protéger l’équipement et le câblage d’alimentation du système contre les dommages et la destruction.

Responsable : Aucun

Discussion :

Les organisations déterminent les types de protection nécessaires à l’équipement et au câble d’alimentation dans différents emplacements internes et externes de l’installation et de l’environnement opérationnel de l’organisation. Les types d’équipement et de câblage d’alimentation comprennent le câblage interne et les sources d’alimentation sans coupure dans les bureaux ou les centres de données, les génératrices et le câblage d’alimentation à l’extérieur de l’édifice, et les sources d’alimentation provenant d’entités autonomes comme des satellites, des véhicules et d’autres systèmes déployables.

PE-09(01) — Câblage redondant (---)

Énoncés :

Employer des chemins de câblage d'alimentation redondant qui sont installés à une distance de [Affectation : distance définie par l'organisation].

Responsable : Aucun

Discussion :

Les câbles d'alimentation redondants et distants permettent d'assurer une alimentation continue si l'un des câbles est coupé ou endommagé.

PE-09(02) — Contrôles de tension automatisés (---)

Énoncés :

Utiliser des contrôles de tension automatisés pour [Affectation : composants essentiels du système définis par l'organisation].

Responsable : Aucun

Discussion :

Les contrôles de tension automatisés peuvent surveiller et contrôler la tension. De tels contrôles comprennent les régulateurs de tension, les conditionneurs de tension et les stabilisateurs de tension.

PE-10 — Arrêt d'urgence (---)

Énoncés :

a. Pouvoir, en situation d'urgence, couper l'alimentation de [Affectation : système; composants individuels de système désignés par l'organisation]
b. Placer des interrupteurs ou des dispositifs d'arrêt d'urgence dans [Affectation : liste définie par l'organisation des emplacements par système ou composant de système] pour faciliter l'accès au personnel
c. Protéger la capacité d'interruption d'urgence de l'alimentation contre toute activation non autorisée

Responsable : Aucun

Discussion :

L'interruption d'urgence de l'alimentation touche principalement les installations de l'organisation qui contiennent des concentrations de ressources système, comme des centres de données, des salles de serveurs et d'ordinateurs centraux et les zones où on retrouve des appareils contrôlés par ordinateur.

PE-10(01) — Activation accidentelle et non autorisée (---)

Énoncés :

Annulé : Intégré au contrôle PE-10.

Responsable : Aucun

PE-11 — Alimentation d’urgence (---)

Énoncés :

Prévoir un système d’alimentation sans coupure pour faciliter [Sélection (un choix ou plus) : l’arrêt ordonné du système; le réacheminement du système vers une source d’alimentation de secours à long terme] dans l’éventualité d’une perte de la source d’alimentation principale.

Responsable : Aucun

Discussion :

Un système d’alimentation sans coupure (UPS pour Uninterruptible Power Supply) est un système ou mécanisme électrique qui procure une alimentation d’urgence lors d’une panne de la source d’alimentation principale. On utilise habituellement les UPS pour protéger les ordinateurs, les centres de données, l’équipement de télécommunications ou d’autres équipements électriques lorsqu’une panne de courant imprévue risque de causer des blessures, des décès, d’importantes interruptions dans la mission ou les activités, ou une perte de données ou d’information. Un UPS est différent d’un système d’alimentation sans coupure ou d’une génératrice auxiliaire dans la mesure où il fournit une protection quasi instantanée contre les interruptions d’alimentation imprévues de la source principale en utilisant l’énergie stockée dans des piles, des supercondensateurs ou des volants d’inertie. La durée de la pile d’un UPS est relativement courte, mais elle offre suffisamment de temps pour passer à une source d’alimentation de secours, comme une génératrice auxiliaire, ou arrêter correctement le système.

PE-11(01) — Source d’alimentation de secours – Capacité opérationnelle minimale (---)

Énoncés :

Fournir une source d’alimentation de secours au système qui est activé [Sélection (un choix) : manuellement; automatiquement] et qui est capable de maintenir la capacité opérationnelle minimale requise dans l’éventualité d’une perte prolongée de la source d’alimentation principale.

Responsable : Aucun

Discussion :

Le provisionnement d’une source d’alimentation de secours avec une capacité opérationnelle minimale peut se faire en accédant à une source d’alimentation commerciale secondaire ou à une autre source d’alimentation externe.

PE-11(02) — Source d’alimentation de secours – Autonome (---)

Énoncés :

Fournir une source d’alimentation de secours au système qui est activé [Sélection (un choix) : manuellement; automatiquement] et qui est :
a. autonome
b. indépendante de toute source d’alimentation externe
c. capable de maintenir [Sélection(1) : la capacité opérationnelle minimale requise; une capacité opérationnelle totale] dans l’éventualité d’une perte prolongée de la source d’alimentation principale

Responsable : Aucun

Discussion :

Le provisionnement d’une source d’alimentation à long terme et autonome peut être réalisé en utilisant au moins une génératrice dotée d’une capacité suffisante pour répondre aux besoins de l’organisation.

PE-12 — Éclairage de sécurité (---)

Énoncés :

Utiliser et entretenir, pour le système, un système automatique d'éclairage de sécurité qui entre en fonction lorsqu'il y a coupure ou interruption de courant et qui éclaire les sorties d'urgence et les chemins d'évacuation dans l'installation.

Responsable : Aucun

Discussion :

Il importe principalement de fournir un éclairage de sécurité dans les installations de l'organisation qui contiennent une concentration de ressources système, comme les centres de données, les salles des serveurs et les salles d'ordinateurs centraux. L'éclairage de sécurité fourni au système est décrit dans le plan d'urgence de l'organisation. Si l'éclairage de sécurité du système ne s'active pas ou ne peut être fourni, l'organisation considère des sites de traitement de secours pour les éventualités liées à l'alimentation.

PE-12(01) — Fonctions opérationnelles et de mission essentielles (---)

Énoncés :

Prévoir l'éclairage de sécurité de toutes les zones de l'installation prenant en charge les fonctions opérationnelles et de mission essentielles.

Responsable : Aucun

Discussion :

Les organisations définissent leurs fonctions opérationnelles et de mission essentielles.

PE-13 — Protection contre les incendies (---)

Énoncés :

Utiliser et maintenir des dispositifs et systèmes de détection et d'extinction d'incendie alimentés par une source d'énergie indépendante.

Responsable : Aucun

Discussion :

Il importe principalement de fournir des systèmes de détection et d'extinction d'incendie dans les installations de l'organisation qui contiennent une concentration de ressources système, comme les centres de données, les salles des serveurs et les salles d'ordinateurs centraux. Les systèmes de détection et d'extinction d'incendie susceptibles d'exiger une source d'énergie indépendante comprennent les systèmes de gicleurs et les détecteurs de fumée. Une source d'énergie indépendante est une source d'énergie, comme un miniréseau, qui est séparé, ou pourrait être séparé, des sources d'énergie fournissant l'alimentation aux autres parties de l'installation.

PE-13(01) — Activation et avis automatiques (---)

Énoncés :

Utiliser, pour le système, des dispositifs ou systèmes de détection d'incendie qui s'activent automatiquement et informent [Affectation : personnel ou rôles définis par l'organisation] et [Affectation : intervenantes et intervenants d'urgence désignés par l'organisation] dans l'éventualité d'un incendie.

Responsable : Aucun

Discussion :

L'organisation peut préciser le personnel, les rôles et les intervenantes et intervenants d'urgence advenant le cas où les personnes se trouvant sur la liste de notification sont tenues d'avoir les autorisations d'accès et les habilitations de sécurité appropriées (par exemple, pour accéder aux installations où l'accès est limité en raison de la classification ou du niveau d'incidence de l'information dans l'installation). Les mécanismes de notification peuvent demander des sources d'énergie indépendantes pour assurer que la capacité de notification ne soit pas entravée par un incendie.

PE-13(02) — Systèmes d'extinction – Activation et avis automatiques (---)

Énoncés :

a. Utiliser, pour le système, des dispositifs ou systèmes d'extinction d'incendie qui s'activent automatiquement et informent [Affectation : personnel ou rôles définis par l'organisation] et [Affectation : intervenantes et intervenants d'urgence désignés par l'organisation]
b. Utiliser, pour le système, une capacité d'extinction automatique d'incendie lorsque l'installation n'a pas de personnel affecté de façon continue

Responsable : Aucun

Discussion :

L'organisation peut préciser le personnel, les rôles et les intervenantes et intervenants d'urgence advenant le cas où les personnes se trouvant sur la liste de notifications sont tenues d'avoir les autorisations d'accès appropriées et les habilitations de sécurité appropriées (par exemple, pour accéder aux installations où l'accès est limité en raison du niveau d'incidence ou de la classification de l'information dans l'installation). Les mécanismes de notification peuvent demander des sources d'énergie indépendantes pour assurer que la capacité de notification ne soit pas entravée par un incendie.

PE-13(03) — Extinction automatique d’incendie (---)

Énoncés :

Annulé : Intégré au contrôle PE-13(02).

Responsable : Aucun

PE-13(04) — Inspections (---)

Énoncés :

S'assurer que l'installation est [Affectation : fréquence définie par l'organisation] inspectée par des inspectrices et inspecteurs autorisés et qualifiés, et que les problèmes relevés sont corrigés dans les [Affectation : délais définis par l'organisation] suivants.

Responsable : Aucun

Discussion :

Le personnel autorisé et compétent dans la juridiction de l'organisation comprend les inspectrices et inspecteurs des incendies et les cheffes et chefs du service des incendies provinciaux et municipaux. L'organisation fournit des accompagnatrices et accompagnateurs durant les inspections lorsque les systèmes qui se trouvent dans les installations comportent de l'information sensible.

PE-13(400) — Services d’urgence (---)

Énoncés :

S’assurer de tenir compte de la capacité en eau nécessaire pour l’extinction d’incendie et d’avoir des délais de réponse efficaces pour les services d’urgence dans le cadre de l’élaboration des stratégies de protection.

Responsable : Aucun

Discussion :

La capacité en eau nécessaire pour l’extinction d’incendie et des délais de réponse efficaces de la part des services d’incendie et de police doit être prise en compte lors de l’élaboration de stratégies de protection, en fonction des principes de protection, de détection et d’intervention. Cela s’applique à la sélection du site, aux installations et aux biens. Si les délais de réponse en cas d’urgence sont inadéquats, des mesures de secours ou supplémentaires peuvent s’avérer nécessaires pour assurer la sécurité des individus et la protection des biens.

PE-14 — Contrôles environnementaux (---)

Énoncés :

a. Maintenir les niveaux [Sélection (un choix ou plus) : de température; d'humidité; de pression; de rayonnement; {Affectation : contrôle environnemental défini par l'organisation}] dans l'installation où se trouve le système à [Affectation : niveaux acceptables définis par l'organisation]
b. Surveiller les niveaux des contrôles environnementaux [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

Il importe principalement de fournir des contrôles environnementaux dans les installations de l'organisation qui contiennent une concentration de ressources système, comme les centres de données, les salles d'ordinateurs centraux et les salles des serveurs. Des contrôles environnementaux insuffisants, en particulier dans des environnements très difficiles, peuvent avoir des répercussions négatives importantes sur la disponibilité des systèmes et des composants du système nécessaires au soutien de la mission et des activités de l'organisation.

PE-14(01) — Contrôles automatisés (---)

Énoncés :

Employer les contrôles environnementaux automatisés dans l'installation pour empêcher des fluctuations du système pouvant être potentiellement préjudiciables : [Affectation : contrôles environnementaux automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

La mise en oeuvre de contrôles environnementaux automatisés fournit une réponse immédiate aux conditions environnementales qui peuvent endommager, dégrader ou détruire les systèmes de l'organisation ou les composants des systèmes.

PE-14(02) — Surveillance avec des alarmes et des notifications (---)

Énoncés :

Utiliser une surveillance des contrôles environnementaux qui fournit une alarme ou une notification des changements potentiellement préjudiciables pour le personnel ou l'équipement à [Affectation : personnel ou rôles définis par l'organisation].

Responsable : Aucun

Discussion :

L'alarme ou la notification peut prendre la forme d'une alarme audible ou d'un message visuel en temps réel adressé au personnel ou aux rôles définis par l'organisation. Ces alarmes et notifications peuvent aider à minimiser les préjudices que peuvent subir des individus et les dommages aux biens organisationnels en facilitant une intervention en cas d'urgence en temps opportun.

PE-15 — Protection contre les dégâts d’eau (---)

Énoncés :

Protéger le système contre tout dommage causé par une fuite d’eau en recourant à des robinets d’arrêt ou d’isolement accessibles qui fonctionnent adéquatement et dont le personnel concerné connaît l’emplacement.

Responsable : Aucun

Discussion :

Il importe principalement de fournir une protection contre les dégâts d’eau dans les installations de l’organisation qui contiennent une concentration de ressources système, comme les centres de données, les salles des serveurs et les salles d’ordinateurs centraux. Les robinets d’isolement peuvent être employés en plus ou à la place de robinets d’arrêt pour fermer l’approvisionnement en eau dans des zones données sans que toute l’organisation soit touchée.

PE-15(01) — Soutien automatisé (---)

Énoncés :

Détecter la présence d'eau près du système et alerter [Affectation : personnel ou rôles définis par l'organisation] au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Les mécanismes automatisés comprennent les systèmes de notification, les capteurs de détection d'eau et les alarmes.

PE-16 — Livraison et retrait (---)

Énoncés :

a. Autoriser et contrôler [Affectation : types de composants du système définis par l'organisation] entrant et sortant de l'installation
b. Tenir des registres des composants du système

Responsable : Aucun

Discussion :

Appliquer des autorisations d'entrée et de sortie des composants du système peut exiger une restriction de l'accès aux aires de livraison et leur isolation du système et des bibliothèques de supports.

PE-17 — Autres lieux de travail (---)

Énoncés :

a. Déterminer et documenter les [Affectation : autres lieux de travail définis par l'organisation] que peuvent utiliser les employées et employés
b. Employer les contrôles suivants dans d'autres lieux de travail : [Affectation : contrôles définis par l'organisation]
c. Évaluer l'efficacité des contrôles dans d'autres lieux de travail
d. Fournir aux employées et employés un moyen de communiquer avec le personnel responsable de la sécurité et de la protection de la vie privée de l'information en cas d'incidents

Responsable : Aucun

Discussion :

Parmi les autres lieux de travail, notons les installations du gouvernement ou les résidences privées des employées et employés. Bien qu'ils se distinguent des autres sites de traitement, les autres lieux de travail peuvent constituer des solutions de rechange facilement accessibles pendant des opérations d'urgence. L'organisation peut définir différents ensembles de contrôles pour des lieux de travail ou des types de sites précis selon les activités professionnelles qui y sont menées. Mettre en oeuvre et évaluer l'efficacité des contrôles définis par l'organisation et fournir un moyen de communication des incidents aux autres lieux de travail permettront d'appuyer les activités de planification d'urgence des organisations.

PE-18 — Emplacement des composants du système (---)

Énoncés :

Installer les composants du système de manière à réduire au minimum les dommages que pourraient causer [Affectation : risques physiques et environnementaux définis par l'organisation], de même que les possibilités d'accès non autorisé.

Responsable : Aucun

Discussion :

Les risques physiques et environnementaux comprennent les inondations, les tsunamis, les incendies, les tornades, les tremblements de terre, les ouragans, les actes terroristes, le vandalisme, les impulsions électromagnétiques, les interférences électriques et d'autres formes de rayonnements électromagnétiques. Les organisations choisissent l'emplacement des points d'entrée de manière à ce qu'une personne non autorisée, à qui l'accès est interdit, ne puisse s'approcher des systèmes. Une telle proximité peut accroître le risque d'un accès non autorisé aux communications de l'organisation au moyen de microphones de reniflage de paquets sans fil ou dans le cadre d'une divulgation non autorisée d'information.

PE-18(01) — Site de l’installation (---)

Énoncés :

Annulé : Transféré sous le contrôle PE-23.

Responsable : Aucun

PE-19 — Fuite d’information (---)

Énoncés :

Protéger le système contre les fuites d’information dues à l’émission de signaux électromagnétiques.

Responsable : Aucun

Discussion :

On entend par fuite d’information toute divulgation intentionnelle ou non intentionnelle d’information ou de données à un environnement non fiable résultant de l’émission de signaux électromagnétiques. La catégorisation ou la classification de sécurité des systèmes (en ce qui a trait à la confidentialité), les stratégies de sécurité et de confidentialité organisationnelles et la tolérance au risque permettent de sélectionner les contrôles employés pour protéger les systèmes contre les fuites d’information liées à l’émission de signaux électromagnétiques

PE-19(01) — Stratégies et procédures nationales en matière d'émission (---)

Énoncés :

Protéger les composants du système, les communications de données connexes ainsi que les réseaux conformément aux stratégies et procédures nationales en ce qui a trait aux émissions et à la norme TEMPEST.

Responsable : Aucun

Discussion :

Les stratégies d'émissions comprennent les anciennes stratégies en matière de norme TEMPEST.

PE-20 — Surveillance et suivi des biens (---)

Énoncés :

Utilise [Affectation : technologies associées à l'emplacement des biens définies par l'organisation] pour procéder au suivi et à la surveillance de l'emplacement et des déplacements des [Affectation : biens définis par l'organisation] dans [Affectation : zones contrôles définies par l'organisation].

Responsable : Aucun

Discussion :

Grâce aux technologies associées à l'emplacement des biens, les organisations peuvent veiller à ce que les biens essentiels, comme les véhicules, l'équipement et les composants du système, demeurent dans les emplacements autorisés. Les organisations consultent la haute ou le haut fonctionnaire ou cadre supérieure ou supérieur en matière de protection de la vie privée ou les services juridiques concernant la mise en oeuvre et l'utilisation de technologies associées à l'emplacement des biens pour aborder de possibles préoccupations en matière de protection de la vie privée.

PE-21 — Protection contre les impulsions électromagnétiques (---)

Énoncés :

Employer des [Affectation : mesures de protection définies par l'organisation] contre les dommages causés par des impulsions électromagnétiques (IEM) pour les [Affectation : systèmes et composants des systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Une IEM est un rayonnement d'énergie électromagnétique de forte intensité et de courte durée qui s'étend dans une gamme de fréquences. De tels rayonnements d'énergie peuvent être d'origine naturelle ou humaine. L'interférence par IEM peut provoquer des perturbations ou des dommages à l'équipement électronique. Les mesures de protection utilisées pour atténuer le risque d'IEM comprennent le recours au blindage, aux limiteurs de surtension, aux transformateurs ferrorésistants, et la mise à la terre. La protection contre les IEM peut être particulièrement importante pour les systèmes et applications qui font partie des infrastructures essentielles.

PE-22 — Marquage des composants (---)

Énoncés :

Marquer les [Affectation : composants matériels des systèmes définis par l'organisation] indiquant le niveau d'incidence ou de classification de l'information pouvant être traitée, stockée ou transmise par le composant matériel.

Responsable : Aucun

Discussion :

Les composants matériels pouvant nécessiter un marquage comprennent les dispositifs d'entrée et de sortie. Les ordinateurs de bureau et bloc-notes, les claviers, les tablettes et les téléphones intelligents sont des dispositifs d'entrée et de sortie. Les dispositifs de sortie comprennent les imprimantes, les moniteurs, les écrans vidéo, les télécopieurs, les numériseurs, les photocopieurs et les dispositifs audio. Les autorisations qui contrôlent les dispositifs d'entrée et de sortie sont abordées dans les contrôles AC-03 et AC-

04. Les composants sont marqués pour indiquer le niveau d'incidence ou de classification du système auxquels les dispositifs sont connectés, ou le niveau d'incidence ou de classification de l'information autorisée à sortir. Le « marquage de sécurité » désigne l'utilisation d'attributs de sécurité lisibles par des humains. L'« étiquetage de sécurité » désigne l'utilisation d'attributs de sécurité liés aux structures de données internes du système. Le marquage de sécurité n'est généralement pas requis dans le cas des composants matériels qui traitent, stockent ou transmettent de l'information qui, selon l'organisation, est du domaine public ou peut être diffusée publiquement. Toutefois, l'organisation peut exiger des marquages pour des composants matériels qui traitent, stockent ou transmettent de l'information du domaine public afin d'indiquer qu'une telle information peut être diffusée publiquement. Le marquage des composants matériels du système est conforme aux lois, aux décrets, aux directives, aux politiques, à la réglementation et aux normes applicables.

PE-23 — Emplacement de l’installation (---)

Énoncés :

a. Prévoir l’emplacement ou le site de l’installation où le système réside en tenant compte des risques physiques et environnementaux
b. Dans le cas d’installations existantes, tenir compte des risques physiques et environnementaux dans la stratégie de gestion des risques de l’organisation

Responsable : Aucun

Discussion :

Les risques physiques et environnementaux comprennent les inondations, les tsunamis, les incendies, les tornades, les tremblements de terre, les ouragans, les actes terroristes, le vandalisme, les impulsions électromagnétiques, les interférences électriques et d’autres formes de radiations électromagnétiques. Les études environnementales et des terrains peuvent aider à choisir le ou les emplacements optimaux pour les installations afin de réduire le plus grand nombre de menaces environnementales possible. S’il est impossible d’éviter de telles menaces, ces études indiqueront les facteurs d’atténuation à employer, le cas échéant, pour limiter les dommages causés aux biens et l’interruption des services. Le contrôle PE-18 porte sur l’emplacement des composants du système dans l’installation.

PE-400 — Environnements à distance et de télétravail (---)

Énoncés :

a. Évaluer la sécurité physique des environnements à distance et de télétravail
b. Appliquer des exigences appropriées en matière de protection et de stockage pour l'information et les biens
c. Utiliser un équipement de sécurité et des dispositifs électroniques approuvés conformément à la catégorisation du matériel

Responsable : Aucun

PE-400(01) — Rangement physique d’information et de biens (---)

Énoncés :

Conserver l’information physique et les biens conformément aux conseils de la GRC et des pratiques de sécurité établies par le ministère.

Responsable : Aucun

PE-400(02) — Travail à distance et télétravail à l'étranger (---)

Énoncés :

Autoriser les demandes de travail à distance ou de télétravail à partir d'emplacements à l'étranger que dans des circonstances exceptionnelles.

Responsable : Aucun

PE-401 — Centre des opérations de sécurité (---)

Énoncés :

Établir et tenir à jour un centre des opérations de sécurité (COS) pour protéger le personnel, la propriété, les biens et l'information de l'organisation par une surveillance et un suivi physiques et techniques.

Responsable : Aucun

Discussion :

Un COS regroupe les gens, les processus et la technologie pour fournir des services opérationnels et d'autres services de sécurité aux organisations, notamment la protection des personnes, de la propriété, des biens et de l'information. Le COS fournit habituellement les installations pour soutenir le personnel de sécurité dans le cadre du suivi, de la surveillance, de la présentation, du contrôle et de la gestion d'événement en lien avec la sécurité, y compris les menaces internes. Le COS permet aux exploitants de système de recueillir de l'information en lien à un environnement physique ou à un cyberenvironnement pour l'analyser, pour détecter et évaluer les notifications d'alertes, et pour effectuer la répartition du personnel nécessaire pour intervenir adéquatement face aux événements. Un COS permet d'accroître la connaissance de la situation en ce qui a trait à l'environnement de l'organisation, en favorisant une prise de décisions et une intervention efficaces pendant un événement. Le COS peut aider les équipes multidisciplinaires, notamment celles de la sécurité physique, des TI et de la sécurité des technologies opérationnelles (TO), les analystes, les ingénieures/ingénieurs, les architectes et autres fournisseurs de services. D'ailleurs, la convergence des TI et de la TO instaure de nouvelles exigences visant à évaluer le risque que posent l'information et la sécurité physique. Par exemple, le bon fonctionnement des systèmes de contrôle, comme ceux utilisés pour élaborer l'automatisation qui contrôle la température, les éclairs, les accès, etc., risquerait d'être touché si le logiciel ou l'application venait à être compromis. Le contrôle IR-04(14) fournit de l'information sur un COS censé protéger l'infrastructure technique d'une organisation, qui comporte des systèmes et des réseaux.

PL

Planification de la cybersécurité

Planning

PL-01 — Politique et procédures de planification (---)

Énoncés :

a. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :
- **1.** une politique de planification [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables
- **2.** des procédures pour faciliter la mise en oeuvre de la politique de planification et des contrôles connexes

c. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à la planification

c. Passer en revue et mettre à jour, par rapport à la planification :
- **1.** la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]
- **2.** les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation].

Responsable : Aucun

Discussion :

La politique et les procédures de planification pour les contrôles de la famille PL sont mises en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et procédures de planification contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à leur élaboration. Les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin pour des politiques et des procédures propres à la mission ou au système. La politique peut être intégrée à la politique générale de sécurité et de protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures comprennent, sans s'y limiter, les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, à la jurisprudence, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.

PL-02 — Plans de sécurité et de protection de la vie privée des systèmes (---)

Énoncés :

a. Élaborer des plans de sécurité et de protection de la vie privée pour le système qui :
- **1.** sont conformes à l'architecture d'entreprise de l'organisation
- **2.** définissent explicitement les composants constitutifs du système
- **3.** décrivent le contexte opérationnel du système sur le plan des processus liés à la mission et aux activités
- **4.** identifient les personnes qui assument des responsabilités et des rôles liés au système
- **5.** identifient les types d'informations traitées, stockées et transmises par le système
- **6.** définissent la catégorisation de sécurité du système, y compris la justification à l'appui
- **7.** décrivent les menaces particulières pour le système qui sont préoccupantes pour l'organisation
- **8.** fournissent les résultats de l'évaluation des risques d'atteinte à la vie privée pour les systèmes qui traitent les renseignements personnels
- **9.** décrivent l'environnement opérationnel du système ainsi que les dépendances ou les connexions à d'autres systèmes ou à d'autres composants du système
- **10.** donnent un aperçu des exigences en matière de contrôle de la sécurité et de la protection de la vie privée du système
- **11.** déterminent les bases de référence ou les profils des contrôles pertinents, le cas échéant
- **12.** décrivent les contrôles en place ou prévus pour satisfaire aux exigences de sécurité et de protection de la vie privée, y compris la justification des décisions concernant l'adaptation des contrôles
- **13.** incluent les déterminations des risques découlant des décisions liées à la conception et à l'architecture de sécurité et de protection de la vie privée
- **14.** comprennent des activités liées à la sécurité et à la protection de la vie privée visant le système dont la planification et la coordination doivent être assurées avec [Affectation : personnes ou groupes désignés par l'organisation]
- **15.** sont examinés et approuvés par l'autorité responsable ou une représentante ou un représentant désigné avant leur mise en oeuvre
- **400.** documentent les objectifs organisationnels pour le traitement des renseignements personnels
- **401.** définissent les normes de conservation et d'élimination des documents pour les renseignements personnels stockés dans le système

b. Distribuer des copies des plans et communiquer les changements qui y sont apportés par la suite aux [Affectation : personnel ou rôles définis par l'organisation]
c. Examiner les plans [Affectation : fréquence définie par l'organisation]
d. Mettre à jour les plans pour tenir compte des changements apportés au système et à l'environnement d'exploitation, ou des problèmes soulevés lors de la mise en oeuvre des plans ou des évaluations des contrôles
e. Protéger les plans contre les divulgations ou les modifications non autorisées

Responsable : Aucun

Discussion :

Les plans de sécurité et de protection de la vie privée du système sont adaptés au système et aux composants du système dans la limite d'autorisation définie et contiennent une vue d'ensemble des exigences de sécurité et de protection de la vie privée pour le système et les contrôles sélectionnés pour satisfaire aux exigences. Les plans décrivent l'application prévue de chaque contrôle sélectionné dans le contexte du système avec un niveau suffisant de détail pour mettre en oeuvre correctement le contrôle et en évaluer l'efficacité par la suite. La documentation des contrôles décrit la façon dont les contrôles hybrides et propres au système sont mis en oeuvre, ainsi que les plans et les attentes concernant la fonctionnalité du système. Les plans de sécurité et de protection de la vie privée du système peuvent également être utilisés dans la conception et le développement des systèmes pour appuyer les processus d'ingénierie de la sécurité et de la protection de la vie privée basés sur le cycle de vie. Les plans de sécurité et de protection de la vie privée du système sont des documents évolutifs qui sont mis à jour et adaptés tout au long du cycle de développement du système (par exemple, lors de la détermination des capacités, l'analyse des solutions de rechange, les demandes de propositions et les examens de la conception). La section 2.1 décrit les différents types d'exigences qui touchent les organisations durant le cycle de développement du système et la relation entre les exigences et les contrôles. Les organisations peuvent élaborer un seul plan intégré de sécurité et de protection de la vie privée ou tenir à jour plusieurs plans distincts. Les plans de sécurité et de protection de la vie privée associent les exigences en matière de sécurité et de protection de la vie privée à un ensemble de contrôles et d'améliorations de contrôle. Les plans décrivent également en quoi les contrôles et les améliorations de contrôle satisfont aux exigences en matière de sécurité et de protection de la vie privée, sans pour autant fournir des descriptions détaillées et techniques de la conception ou de la mise en oeuvre de ces contrôles ou de ces améliorations de contrôle. Les plans de sécurité et de protection de la vie privée contiennent suffisamment d'information (y compris des spécifications explicites ou par référence des paramètres d'affectation et de sélection) pour permettre une conception et une mise en oeuvre clairement conformes à ses objectifs et la détermination subséquente des risques qu'ils

représentent, s'ils sont appliqués, pour les activités et les biens de l'organisation, les individus, les autres organisations et le gouvernement. Les plans de sécurité et de protection de la vie privée n'ont pas à être des documents uniques. Ils peuvent être un ensemble de documents, y compris des documents qui existent déjà. Des plans de sécurité et de protection de la vie privée efficaces renvoient largement aux stratégies, aux procédures et à des documents additionnels, comme les spécifications liées à la conception et à la mise en oeuvre, dans lesquels il est possible d'obtenir de plus amples détails. L'utilisation de ces références permet de réduire la documentation associée aux programmes de sécurité et de protection de la vie privée, de même que de conserver l'information relative à la sécurité et à la protection de la vie privée dans d'autres secteurs opérationnels ou de gestion établis, notamment l'architecture d'entreprise, le cycle de développement des systèmes, l'ingénierie des systèmes et l'acquisition. Par exemple, les plans de sécurité n'ont pas à faire mention des plans de secours, des plans d'intervention en cas d'incident ou des processus à suivre advenant une atteinte à la vie privée. Ils peuvent plutôt fournir suffisamment d'information (explicitement et en référence) pour établir quels objectifs ces plans visent à atteindre. Les activités liées à la sécurité et à la protection de la vie privée susceptibles d'exiger de la coordination et de la planification avec d'autres personnes ou groupes au sein de l'organisation comprennent les évaluations, les vérifications, les inspections, la maintenance du matériel et des logiciels, la gestion des acquisitions et des risques liés à la chaîne d'approvisionnement, la gestion des correctifs et la mise à l'essai des plans d'urgence. La planification et la coordination englobent les situations urgentes et celles qui ne le sont pas (c'est-à-dire, planifiées ou non urgentes et non planifiées). Le processus défini par l'organisation pour planifier et coordonner les activités liées à la sécurité et à la protection de la vie privée peut également être inclus dans d'autres documents, le cas échéant.

PL-02(01) — Concept d’opérations (---)

Énoncés :

Annulé : Intégré au contrôle PL-07.

Responsable : Aucun

PL-02(02) — Architecture fonctionnelle (---)

Énoncés :

Annulé : Intégré au contrôle PL-08.

Responsable : Aucun

PL-02(03) — Planifier et coordonner avec d’autres entités organisationnelles (---)

Énoncés :

Annulé : Intégré au contrôle PL-02.

Responsable : Aucun

PL-03 — Mise à jour du plan de sécurité des systèmes (---)

Énoncés :

Annulé : Intégré au contrôle PL-02.

Responsable : Aucun

PL-04 — Règles de conduite (Nc--)

Énoncés :

a. Établir et communiquer les règles qui décrivent les responsabilités et le comportement attendu des personnes qui doivent accéder au système en ce qui concerne l'utilisation, la sécurité et la protection de la vie privée de l'information et du système
b. Obtenir des personnes devant accéder au système une attestation documentée selon laquelle elles ont lu et compris le document et acceptent de respecter les règles de conduite avant d'obtenir l'accès autorisé à l'information et au système
c. Passer en revue et mettre à jour les règles de conduite tous les [Affectation : fréquence définie par l'organisation]
d. Exiger que les personnes qui ont accepté de se conformer à une version antérieure des règles de conduite les lisent et les acceptent de nouveau [Sélection (un choix ou plus) : {Affectation : fréquence définie par l'organisation}; lorsque les règles sont révisées ou mises à jour]

Responsable : Aucun

Discussion :

Les règles de conduite représentent un type d'entente d'accès pour les utilisatrices et utilisateurs de l'organisation. D'autres types d'ententes d'accès comprennent les ententes régissant les conflits d'intérêts et les ententes d'utilisation acceptable (voir le contrôle PS-06). Les organisations devraient prévoir les règles de conduite selon les rôles et les responsabilités des utilisatrices et utilisateurs et faire une distinction entre les règles appliquées aux utilisatrices et utilisateurs privilégiés et celles appliquées aux utilisatrices et utilisateurs généraux. Il est souvent difficile d'établir des règles de conduite pour certains types d'utilisateurs non organisationnels, notamment des personnes qui reçoivent des renseignements de systèmes gouvernementaux, étant donné le grand nombre de ces utilisatrices et utilisateurs et la nature limitée de leurs interactions sur les systèmes. Les règles de conduite des utilisatrices et utilisateurs organisationnels et non organisationnels peuvent également être établies sous le contrôle AC-

08. La section des contrôles et des activités connexes fournit une liste des contrôles qui sont pertinents aux règles de conduite de l'organisation. Pour satisfaire le contrôle PL-04B (l'attestation documentée de ce contrôle), l'organisation peut offrir de la formation et de la sensibilisation en matière de sécurité, ainsi que des programmes de formation axés sur les rôles, si de telles formations traitent des règles de conduite. Les attestations documentées des règles de conduite comprennent le recours à des signatures électroniques ou physiques et l'utilisation de cases d'option pour l'acceptation électronique.

PL-04(01) — Restriction d'utilisation des médias sociaux et des sites et applications externes (---)

Énoncés :

Tenir compte des restrictions que les règles de conduite imposent sur ce qui suit :
a. la publication d'information organisationnelle sur des sites Web publics par l'entremise de médias sociaux, de réseaux sociaux et de sites et applications externes
b. l'utilisation d'identifiants fournis par l'organisation (par exemple, des adresses courriel) et de secrets d'authentification (par exemple, des mots de passe) pour la création de comptes sur des sites et applications externes

Responsable : Aucun

Discussion :

Les restrictions imposées à l'utilisation des médias sociaux, des réseaux sociaux et des sites et applications externes tiennent compte des règles de conduite liées à une telle utilisation lorsque le personnel de l'organisation utilise de tels sites dans l'exercice de ses fonctions officielles ou dans le cadre de ses activités officielles, lorsque l'information organisationnelle fait partie d'une interaction sur des médias ou réseaux sociaux et lorsque le personnel utilise des systèmes de l'organisation pour accéder aux sites de médias et réseaux sociaux. Les organisations devraient également prévoir des règles particulières pour empêcher que des entités non autorisées utilisent les sites de médias et réseaux sociaux pour obtenir de l'information non publique sur l'organisation, que ce soit directement ou de façon indirecte. L'information non publique comprend les renseignements personnels et l'information sur les comptes des systèmes.

PL-05 — Évaluation des facteurs relatifs à la vie privée (---)

Énoncés :

Annulé : Intégré au contrôle RA-08.

Responsable : Aucun

PL-06 — Planification des activités relatives à la sécurité (---)

Énoncés :

Annulé : Intégré au contrôle PL-02.

Responsable : Aucun

PL-07 — Concepts d'opérations (---)

Énoncés :

a. Élaborer un concept d'opérations (CONOPS) pour le système qui définit comment l'organisation prévoit exploiter le système du point de vue de la sécurité et de la protection de la vie privée de l'information
b. Passer en revue et mettre à jour le CONOPS [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

Le CONOPS peut faire partie des plans de sécurité et de protection de la vie privée du système ou des autres documents liés au cycle de développement des systèmes. Le CONOPS est un document évolutif qui exige des mises à jour tout au long du cycle de développement des systèmes. Par exemple, au cours de la revue de conception des systèmes, le CONOPS est vérifié pour veiller à ce qu'il soit uniforme avec la conception des contrôles, de l'architecture des systèmes et des procédures opérationnelles. Les changements apportés au CONOPS se reflètent en permanence dans les mises à jour des plans de sécurité et de protection de la vie privée, les architectures de sécurité et de protection de la vie privée et d'autres documents organisationnels, comme les spécifications relatives à l'approvisionnement, les documents relatifs au cycle de développement des systèmes et les documents liés à l'ingénierie des systèmes.

PL-08 — Architecture de sécurité et de protection de la vie privée (---)

Énoncés :

a. Élaborer des architectures de sécurité et de protection de la vie privée pour le système qui décrit :
- **1.** les exigences et l'approche à adopter pour protéger la confidentialité, l'intégrité et la disponibilité de l'information de l'organisation
- **2.** les exigences et l'approche à adopter pour traiter les renseignements personnels de manière à limiter les risques d'atteinte à la vie privée des personnes
- **3.** la façon dont les architectures sont intégrées à l'architecture d'entreprise et prises en charge par cette dernière
- **4.** toutes les hypothèses en lien avec les services et systèmes externes et les interdépendances

b. Passer en revue et mettre à jour les architectures [Affectation : fréquence définie par l'organisation] de manière à tenir compte des changements apportés à l'architecture d'entreprise
c. Refléter les changements prévus à l'architecture dans les plans de sécurité et de protection de la vie privée, le CONOPS, l'analyse de criticité, les procédures organisationnelles, de même que l'approvisionnement et les acquisitions

Responsable : Aucun

Discussion :

Les architectures de sécurité et de protection de la vie privée au niveau du système sont conformes aux architectures de sécurité et de protection de la vie privée de l'organisation décrites dans le contrôle PM-
07. Elles en font partie intégrante et sont développées dans le cadre de l'architecture d'entreprise. Les architectures comprennent une description de l'architecture, l'affectation des fonctions de sécurité (dont les contrôles), l'information relative à la sécurité et à la protection de la vie privée des interfaces externes, l'information échangée entre les interfaces, le flux de données des renseignements personnels et les mécanismes de protection associés à chacune des interfaces. Les architectures peuvent également comprendre d'autres renseignements, comme les rôles des utilisateurs et les privilèges d'accès associés à chacun de ces rôles; les exigences propres à la sécurité et à la protection de la vie privée; les types de renseignements traités, stockés et transmis par les systèmes; les exigences relatives à la gestion des risques liés à la chaîne d'approvisionnement; les priorités de restauration de l'information et des services des systèmes, ainsi que tout autre besoin de protection. Il est important de respecter l'orientation pertinente sur l'utilisation des architectures de sécurité dans le cadre du processus du cycle de développement des systèmes. Le Centre pour la cybersécurité recommande d'adopter les concepts d'ingénierie de la sécurité des systèmes décrits dans le document Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes (ITSP.10.037). Les architectures de sécurité et de protection de la vie privée sont examinées et mises à jour tout au long du cycle de développement des systèmes, de l'analyse des alternatives à l'examen de l'architecture proposée dans les propositions de marché et aux revues de conception réalisées avant et durant la mise en oeuvre (par exemple, durant les revues de conception préliminaires et de conception critiques). Dans les architectures informatiques modernes, de moins en moins d'organisations contrôlent l'ensemble des ressources d'information. Les organisations pourraient dépendre fortement des services d'information externes et des fournisseurs de services. Il est nécessaire de décrire ces dépendances dans l'architecture de sécurité et de protection de la vie privée pour mettre en place une stratégie de protection exhaustive de la mission et des activités. La mise en oeuvre et le maintien d'architectures efficaces passent essentiellement par l'élaboration, le développement, la documentation et le maintien d'une configuration de base pour les systèmes de l'organisation dans le cadre du contrôle des configurations. Le développement des architectures est coordonné avec le bureau de la ou du CSIO de l'organisme, la ou le haut fonctionnaire chargé de la gouvernance de sécurité du ministère, ainsi que la ou le cadre supérieur en matière de protection de la vie privée pour veiller à ce que les contrôles nécessaires pour soutenir les exigences propres à la sécurité et à la protection de la vie privée soient établies et mises en oeuvre efficacement. Dans plusieurs cas, il pourrait n'y avoir aucune distinction entre les architectures de sécurité et de protection de la vie privée d'un système. Dans d'autres cas, il est possible d'atteindre adéquatement les objectifs liés à la sécurité, alors que ceux liés à la protection de la vie privée ne sont que partiellement satisfaits par les exigences relatives à la sécurité. Dans de tels scénarios, le fait d'avoir à considérer l'imposition d'exigences en matière de protection de la vie privée pour atteindre les objectifs donnera lieu à la mise en oeuvre d'une architecture de protection de la vie privée distincte. La documentation pourrait toutefois ne faire mention que des architectures combinées. Le contrôle PL-08 concerne principalement les organisations. Il vise à s'assurer que ces dernières mettent en place des architectures pour le système, et que ces architectures s'intègrent à l'architecture d'entreprise ou y soient étroitement liées. Par opposition, le contrôle SA-17 concerne principalement les développeuses, les développeurs, les intégratrices et les intégrateurs de produits et de systèmes de TI externes. Les organisations sélectionnent le contrôle SA-17, qui est complémentaire au contrôle PL-08, lorsqu'elles externalisent le développement des systèmes ou des composants connexes à des entités externes et dans la mesure où il est nécessaire d'assurer l'uniformité avec l'architecture d'entreprise et les architectures de sécurité et de protection de la vie privée de l'organisation.

PL-08(01) — Défense en profondeur (---)

Énoncés :

Concevoir les architectures de sécurité et de protection de la vie privée pour le système en adoptant une approche de défense en profondeur qui :
a. affecte [Affectation : contrôles définis par l'organisation] aux [Affectation : emplacements et couches d'architecture désignés par l'organisation]
b. s'assure que les contrôles affectés fonctionnent de façon coordonnée et se renforcent mutuellement

Responsable : Aucun

Discussion :

L'organisation affecte stratégiquement les contrôles de sécurité et de protection de la vie privée dans les architectures de sécurité et de protection de la vie privée de manière à ce que les adversaires ne puissent atteindre leur objectif sans être confrontés à plusieurs contrôles. Forcer les adversaires à mettre en échec plusieurs contrôles les empêche d'attaquer trop facilement les ressources d'information en leur compliquant la tâche. Cela augmente également les chances que leurs activités soient détectées. Il est essentiel de bien coordonner les contrôles affectés de manière à éviter qu'une attaque visant l'un de ces contrôles n'ait des conséquences néfastes imprévues et aille à l'encontre d'autres contrôles. Les conséquences imprévues peuvent comprendre le verrouillage des systèmes et des alertes successives. La mise en place des contrôles dans les systèmes et les organisations est une activité importante qui exige une analyse minutieuse. Il est important de tenir compte de la valeur des biens de l'organisation au moment de procéder à une structuration en couches plus poussée. Les approches à l'architecture de défense en profondeur comprennent la modularité et la structuration en couches (voir le contrôle SA-08(03)), la séparation des fonctionnalités des utilisateurs et du système (voir le contrôle SC-02) et l'isolation des fonctions de sécurité (voir le contrôle SC-03).

PL-08(02) — Diversité des fournisseurs (---)

Énoncés :

Exiger que les [Affectation : mécanismes de sécurité définis par l'organisation] affectés aux [Affectation : emplacements et couches d'architecture désignés par l'organisation] soient obtenus de différents fournisseurs

Responsable : Aucun

Discussion :

Les produits informatiques présentent diverses forces et faiblesses. C'est en combinant un large éventail de produits qu'il est possible de renforcer chacune des solutions. Par exemple, les fournisseurs de mécanismes de protection contre les programmes malveillants mettent généralement à jour leurs produits à différents moments et développent souvent des solutions aux virus, aux chevaux de Troie ou aux vers connus en fonction de leurs priorités et de leurs calendriers de développement. Déployer différents produits dans divers emplacements permet d'augmenter les chances que le programme malveillant soit détecté par l'un ou l'autre de ces composants. En ce qui concerne la protection de la vie privée, les fournisseurs peuvent offrir des produits qui font le suivi des renseignements personnels dans les systèmes. Les produits peuvent utiliser différentes méthodes de suivi. Le recours à de multiples produits peut accroître l'assurance que les renseignements personnels seront répertoriés.

PL-09 — Gestion centrale (Nc--)

Énoncés :

Centraliser la gestion des [Affectation : contrôles et processus connexes définis par l'organisation].

Responsable : Aucun

Discussion :

La gestion centrale renvoie à la gestion et à la mise en oeuvre des contrôles et des processus sélectionnés à l'échelle de l'organisation. Elle comprend la planification, la mise en oeuvre, l'évaluation, l'autorisation et la surveillance des contrôles et des processus définis par l'organisation et gérés de façon centralisée. Comme la gestion centrale des contrôles est généralement associée au concept de contrôles courants (hérités), une telle gestion favorise et facilite la normalisation de la mise en oeuvre des contrôles, de leur gestion, et d'une utilisation judicieuse des ressources de l'organisation. Des contrôles et des processus gérés de façon centralisée peuvent également répondre aux exigences d'autonomie associées aux évaluations qui visent à appuyer les autorisations initiales et permanentes d'exploiter dans le cadre de la surveillance continue de l'organisation. Des outils automatisés (par exemple, les outils de gestion des informations et des événements de sécurité ou les outils de gestion et de surveillance de la sécurité d'entreprise) peuvent accroître l'exactitude, l'uniformité et la disponibilité de l'information associée aux contrôles et aux processus gérés de façon centralisée. L'automatisation peut aussi fournir des capacités en matière d'agrégation et de corrélation de données, des mécanismes d'alerte et des tableaux de bord pour soutenir la prise de décisions fondée sur le risque au sein de l'organisation. Certains outils de surveillance de la sécurité d'entreprise ou gérés de façon centralisée peuvent collecter et créer de l'information sur les comportements des utilisatrices et utilisateurs des systèmes. Cette information devrait être protégée en tant que renseignements personnels. Pour mieux comprendre, l'organisation s'adresser à la ou au haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée approprié pour obtenir des conseils et de l'orientation. Conformément au processus de sélection des contrôles, les organisations déterminent quels seront les contrôles susceptibles d'être gérés de façon centralisée en tenant compte des ressources et des capacités. Il n'est pas toujours possible de gérer de façon centralisée chacun des aspects d'un contrôle de sécurité. Dans de tels cas, ce dernier est traité comme un contrôle hybride : il est géré et mis en oeuvre de façon centralisée ou au niveau du système. Les contrôles et les améliorations de contrôle qui se prêtent à une gestion centrale complète ou partielle comprennent, sans s'y limiter : AC-02(01), AC-02(02), AC-02(03), AC-02(04), AC-04(all), AC-17(01), AC-17(02), AC-17(03), AC-17(09), AC-18(01), AC-18(03), AC-18(04), AC-18(05), AC-19(04), AC-22, AC-23, AT-02(01), AT-02(02), AT-03(01), AT-03(02), AT-03(03), AT-04, AU-03, AU-06(01), AU-06(03), AU-06(05), AU-06(06), AU-06(09), AU-07(01), AU-07(02), AU-11, AU-13, AU-16, CA-02(01), CA-02(02), CA-02(03), CA-03(01), CA-03(02), CA-03(03), CA-07(01), CA-09, CM-02(02), CM-03(01), CM-03(04), CM-04, CM-06, CM-06(01), CM-07(02), CM-07(04), CM-07(05), CM-08(all), CM-09(01), CM-10, CM-11, CP-07(tous), CP-08(tous), SC-43, SI-02, SI-03, SI-04(tous), SI-07 et SI-08.

PL-10 — Sélection de la base de référence (---)

Énoncés :

Sélectionner la base de référence des contrôles d'un système.

Responsable : Aucun

Discussion :

Les bases de référence des contrôles sont des ensembles prédéfinis de contrôles rassemblés pour satisfaire explicitement aux besoins de protection d'un groupe, d'une organisation ou d'une communauté d'intérêts. Les contrôles sont sélectionnés aux fins des bases de référence de manière à respecter les mandats imposés en vertu des lois, des décrets, des directives, des politiques, de la réglementation, des normes et des lignes directrices applicables ou à atténuer les menaces courantes qui pèsent sur l'ensemble des utilisatrices et utilisateurs de la base de référence selon les hypothèses soulevées par cette dernière. Les bases de référence représentent un point de départ pour la protection de la vie privée des utilisatrices et utilisateurs, de l'information et des systèmes d'information et sont suivies de mesures d'adaptation visant à gérer le risque conformément aux contraintes imposées par la mission, les activités ou de toute autre nature (voir le contrôle PL-11). La sélection de la base de référence d'un contrôle est déterminée par les besoins des parties prenantes. Les parties prenantes doivent tenir compte des exigences liées à la mission ou aux activités de l'organisation, ainsi qu'aux mandats imposés en vertu des lois, des décrets, des directives, des politiques, de la réglementation, des normes et des lignes directrices applicables. Pour répondre aux exigences, on recommande aux organisations de sélectionner l'une des bases de référence des contrôles après avoir passé en revue les types d'information et les renseignements qui sont traités, stockés et transmis sur le système; avoir analysé les incidences négatives potentielles découlant de la perte ou de la compromission de l'information ou du système sur les activités et les biens organisationnels, les individus, les autres organisations ou le gouvernement; et avoir pris en considération les résultats des évaluations des risques touchant les systèmes et l'organisation.

PL-11 — Adaptation de la base de référence (---)

Énoncés :

Adapter la base de référence du contrôle sélectionné en appliquant les mesures d'adaptation indiquées.

Responsable : Aucun

Discussion :

Le concept d'adaptation permet à l'organisation de spécialiser ou de personnaliser un ensemble de contrôles de référence en appliquant un ensemble défini de mesures d'adaptation. Les mesures d'adaptation facilitent cette spécialisation et personnalisation, puisqu'elle permet à l'organisation d'élaborer des plans de sécurité et de protection de la vie privée qui reflètent des fonctions liées à sa mission et à ses activités, les environnements où s'exécutent les systèmes, les menaces et vulnérabilités qui touchent ses systèmes et toute autre condition ou situation susceptible d'avoir une incidence sur la réussite de sa mission ou de ses activités. Des conseils sur mesure sont fournis dans le document La gestion des risques liés à la cybersécurité et à la vie privée : Une méthode axée sur le cycle de vie. L'adaptation de la base de référence d'un contrôle passe par l'identification et la désignation des contrôles communs, l'application des considérations en matière d'établissement de la portée, la sélection des contrôles compensatoires, l'attribution de valeurs aux paramètres des contrôles, l'ajout des contrôles additionnels nécessaires à la base de référence du contrôle et la diffusion d'information sur la mise en oeuvre du contrôle. Les mesures générales d'adaptation fournies dans la Série sur la gestion des risques liés à la cybersécurité et des risques d'atteinte à la vie privée : Une méthode axée sur le cycle de vie peuvent être complétées par des mesures additionnelles selon les besoins de l'organisation.

PM

Gestion de programme à l'échelle organisationnelle

Program Management

PM-01 — Plan du programme de sécurité de l'information (---)

Énoncés :

a. Élaborer et diffuser le plan d'un programme de sécurité de l'information panorganisationnel qui :
- **1.** donne une vue d'ensemble des exigences liées au programme de sécurité et une description des contrôles de gestion du programme de sécurité et des contrôles communs qui ont été mis en place ou que l'on envisage de mettre en place en vue de satisfaire ces exigences
- **2.** comprend l'identification et la répartition des rôles, les responsabilités, l'engagement de la direction, la coordination au sein des entités organisationnelles et la conformité
- **3.** tient compte de la coordination parmi les entités responsables de la sécurité de l'information dans l'organisation
- **4.** est approuvé par une ou un cadre supérieur ayant les responsabilités et la reddition de comptes nécessaires pour le risque qui pèse sur les activités organisationnelles (ce qui comprend la mission, les fonctions, l'image et la réputation), les biens organisationnels, les individus, les autres organisations et le gouvernement

b. Passer en revue et mettre à jour le plan du programme de sécurité de l'information panorganisationnel [Affectation : fréquence définie par l'organisation] et à la suite de [Affectation : événements définis par l'organisation]
c. Protéger le plan du programme de sécurité de l'information contre les divulgations ou les modifications non autorisées

Responsable : Aucun

Discussion :

Le plan du programme de sécurité de l'information est un document officiel qui donne une vue d'ensemble des exigences de sécurité du programme de sécurité de l'information panorganisationnel et décrit les contrôles de gestion du programme et les contrôles communs qui ont été mis en oeuvre ou que l'on envisage de mettre en oeuvre pour satisfaire ces exigences. Le plan d'un programme de sécurité de l'information peut être représenté dans un seul document ou un ensemble de documents. Les plans du programme de protection de la vie privée et les plans de gestion des risques liés à la chaîne d'approvisionnement sont abordés séparément dans les contrôles PM-18 et SR-02 respectivement. Le plan d'un programme de sécurité de l'information documente les détails de la mise en oeuvre de la gestion du programme et des contrôles communs. Le plan fournit de l'information sur les contrôles (y compris la spécification explicite ou par référence des paramètres d'affectation et de sélection) pour permettre une mise en oeuvre clairement conforme à ses objectifs et la détermination des risques qu'il représente s'il est appliqué comme prévu. Les mises à jour apportées aux plans des programmes de sécurité de l'information comprennent des changements organisationnels et les problèmes relevés durant la mise en oeuvre du plan ou les évaluations de contrôles. Les contrôles de gestion des programmes peuvent être mis en oeuvre au niveau de l'organisation, de la mission ou du processus opérationnel, et sont essentiels à la gestion du programme de sécurité de l'information de l'organisation. Les contrôles de gestion des programmes se distinguent des contrôles hybrides, courants et propres aux systèmes, puisqu'ils sont indépendants de tout système particulier. Ensemble, les plans de sécurité de l'information individuels et le plan du programme de sécurité de l'information panorganisationnel fournissent une couverture complète des contrôles de sécurité employés dans l'organisation. Les contrôles communs dont les systèmes organisationnels peuvent hériter sont documentés dans une annexe du plan du programme de sécurité de l'information de l'organisation, à moins qu'ils ne soient compris dans le plan de sécurité distinct d'un système. Le plan du programme de sécurité de l'information panorganisationnel précise quels plans de sécurité distincts contiennent les descriptions des contrôles communs. Les événements qui peuvent précipiter une mise à jour du plan du programme de sécurité de l'information comprennent, sans s'y limiter, les conclusions d'une évaluation ou d'une vérification pangouvernementale, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices.

PM-02 — Rôle de leadership du programme de sécurité de l'information (---)

Énoncés :

Nommer une ou un haut fonctionnaire de la gouvernance en matière de sécurité du ministère avec la mission et les ressources nécessaires pour coordonner, développer, mettre en œuvre et tenir à jour un programme de sécurité de l'information panorganisationnel.

Responsable : Aucun

Discussion :

La ou le haut fonctionnaire de la gouvernance en matière de sécurité du ministère est une ou un agent responsable de l'organisation. Dans le cas des ministères et organismes (tels que décrits par les lois, les décrets, la réglementation, les directives, les politiques et les normes applicables), on entend, par haut fonctionnaire, l'agente supérieure ou agent supérieur de la sécurité de l'information. Dans les organisations, on entend, par cadre supérieure ou supérieur, l'agente supérieure ou agent supérieur de la sécurité de l'information ou la dirigeante principale ou le dirigeant principal de la sécurité de l'information.

PM-03 — Ressources de sécurité et de protection de la vie privée de l'information (---)

Énoncés :

a. Inclure les ressources nécessaires pour mettre en œuvre les programmes de sécurité et de protection de la vie privée de l'information dans les demandes de planification des immobilisations et des investissements et documenter toutes les exceptions à cette exigence
b. Préparer la documentation nécessaire pour tenir compte des programmes de sécurité et de protection de la vie privée de l'information dans les demandes de planification des immobilisations et des investissements conformément aux lois, aux décrets, aux directives, aux politiques, à la réglementation et aux normes applicables
c. Veiller à ce que les ressources liées à la sécurité et à la protection de la vie privée de l'information soient disponibles pour la dépense comme prévu

Responsable : Aucun

Discussion :

L'organisation considère d'identifier des championnes et champions en sécurité et en protection de la vie privée de l'information et de mettre en place l'expertise et les ressources spécialisées nécessaires dans le cadre du processus d'affectation des ressources, le cas échéant. L'organisation peut désigner et habiliter un groupe pour gérer les aspects de la sécurité et de la protection de la vie privée de l'information dans le cadre du processus de planification des immobilisations et de contrôle des investissements.

PM-04 — Processus du plan d’action et des jalons (---)

Énoncés :

a. Mettre en œuvre un processus visant à s’assurer que les plans d’action et les jalons associés au programme de sécurité et de protection de la vie privée de l’information, au programme de gestion des risques liés à la chaîne d’approvisionnement et aux systèmes organisationnels connexes :

1. sont élaborés et tenus à jour

2. est approuvé par une ou un cadre supérieur ayant les responsabilités et la reddition de comptes nécessaires pour le risque qui pèse sur les activités organisationnelles (ce qui comprend la mission, les fonctions, l’image et la réputation), les biens organisationnels, les individus, les autres organisations et le gouvernement

3. sont mentionnés conformément aux exigences liées à la production de rapports qui ont été établies

b. Passer en revue les plans d’action et les jalons pour veiller à ce qu’ils soient uniformes avec la stratégie de gestion des risques de l’organisation et les priorités panorganisationnelles en ce qui a trait aux mesures d’intervention liées aux risques

Responsable : Aucun

Discussion :

Les organisations élaborent des plans d’action et des jalons avec une perspective panorganisationnelle, priorisant les mesures d’intervention liées aux risques et s’assurant qu’ils sont conformes avec leurs buts et leurs objectifs. Les mises à jour des plans d’action et des jalons sont basées sur les constatations des évaluations de contrôles et des activités de surveillance continue. Plusieurs plans d’action et jalons peuvent être mis en place au niveau du système d’information, au niveau de la mission ou du processus opérationnel et au niveau de l’organisation ou de la gouvernance. Bien que les plans d’action et les jalons soient obligatoires pour les organismes, d’autres types d’organisations peuvent réduire les risques en documentant les mesures d’atténuation prévues et en assurant le suivi. Le contrôle CA-05 fournit des conseils propres aux plans d’action et aux jalons au niveau du système.

PM-05 — Inventaire des systèmes et des programmes (Nc--)

Énoncés :

Élaborer et tenir à jour [Affectation : fréquence définie par l'organisation] un inventaire des systèmes et des programmes organisationnels.

Responsable : Aucun

Discussion :

Par inventaire des systèmes, on entend l'inventaire des systèmes dans l'ensemble de l'organisation, et non les composants de systèmes décrits au contrôle CM-08.

PM-05(01) — Inventaire des renseignements personnels (---)

Énoncés :

Réaliser, tenir et mettre à jour [Affectation : fréquence définie par l'organisation] un inventaire de tous les systèmes, programmes, applications et projets qui traitent des renseignements personnels.

Responsable : Aucun

Discussion :

L'inventaire des systèmes, des programmes, des applications et des projets traitant des renseignements personnels soutient la mise en correspondance des actions de données. Il exige la confirmation de l'autorité légitime pour collecter et tenir à jour des renseignements personnels précis et pour limiter le traitement des renseignements personnels à moins qu'ils ne soient directement liés à un programme opérationnel ou à une activité de l'organisation. L'organisation peut utiliser cet inventaire pour s'assurer que les systèmes n'utilisent que les renseignements personnels nécessaires aux programmes et services opérationnels d'une institution, conformément aux normes approuvées de conservation de documents.

PM-06 — Mesures du rendement (---)

Énoncés :

Développer et surveiller les résultats des mesures du rendement de la sécurité et en faire rapport.

Responsable : Aucun

Discussion :

Les mesures du rendement sont des mesures basées sur les résultats que l'organisation emploie pour mesurer l'efficacité ou l'efficience des programmes de sécurité et de protection de la vie privée de l'information et des contrôles utilisés pour soutenir le programme. Pour faciliter la gestion des risques liés à la sécurité et à la protection de la vie privée, l'organisation considère d'aligner les mesures du rendement sur sa tolérance au risque, comme il est indiqué dans la stratégie sur la gestion des risques. Les mesures du rendement de la cybersécurité pourraient tenir compte du nombre de violations de la sécurité, de la réalisation des objectifs relatifs à l'état de préparation en matière de cybersécurité (OEPC), de la robustesse, de la mise en œuvre de changements après incident et des investissements en sécurité par rapport au budget associé aux poursuites judiciaires, aux recours collectifs, aux relations publiques et à la reprise après incident. Parmi les facteurs à considérer au moment d'évaluer les mesures du rendement de la protection de la vie privée, on retrouve le nombre de violations, les mesures liées aux plaintes fondées déposées à la Commission d'accès à l'information du Québec (CAI) et l'achèvement des outils d'évaluation du respect de la vie privée pour les programmes et les services organisationnels.

PM-07 — Architecture d'entreprise (---)

Énoncés :

Développer une architecture d'entreprise en tenant compte de la sécurité et de la protection de la vie privée de l'information et du risque qui en résulte sur les activités et les biens organisationnels, les individus, les autres organisations et le gouvernement.

Responsable : Aucun

Discussion :

L'intégration des exigences et des contrôles de sécurité et de protection de la vie privée à l'architecture d'entreprise permet de s'assurer que les facteurs à considérer en matière de sécurité et de protection de la vie privée sont pris en compte tout au long du cycle de vie des systèmes et qu'ils sont explicitement liés aux processus liés à la mission et aux activités de l'organisation. Le processus d'intégration des exigences de sécurité et de protection de la vie privée vise également l'architecture d'entreprise et les architectures de sécurité et de protection de la vie privée de l'organisation qui sont conformes à la stratégie organisationnelle de gestion des risques. Pour le contrôle PM-07, les architectures de sécurité et de protection de la vie privée sont développées au niveau du système des systèmes, représentant ainsi tous les systèmes de l'organisation. Pour le contrôle PL-08, les architectures de sécurité et de protection de la vie privée sont développées à un niveau qui représente un système en particulier. Les architectures au niveau d'un système sont conformes aux architectures de sécurité et de protection de la vie privée définies pour l'organisation. Les exigences de sécurité et de protection de la vie privée et l'intégration des contrôles sont réalisées plus efficacement si on met rigoureusement en pratique les normes et les lignes directrices de la Série sur la gestion des risques liés à la cybersécurité et des risques d'atteinte à la vie privée : Une méthode axée sur le cycle de vie, ainsi que les normes et lignes directrices de sécurité connexes.

PM-07(01) — Déchargement (---)

Énoncés :

Décharger les [Affectation : fonctions ou services définis par l'organisation] sur d'autres systèmes, des composants de systèmes ou un fournisseur externe.

Responsable : Aucun

Discussion :

Les fonctions ou les services fournis par un système ne sont pas tous essentiels aux fonctions liées à la mission ou aux activités de l'organisation. L'impression et la copie sont des exemples d'un service de soutien non essentiel pour une organisation. Dans la mesure du possible, de tels services ou fonctions de soutien non essentiels ne cohabitent pas avec les services et fonctions qui prennent en charge les fonctions liées à la mission ou aux activités de l'organisation. Maintenir de telles fonctions sur le même système ou un composant de système augmente la surface d'attaque des fonctions ou des services organisationnels essentiels à la mission. Déplacer des fonctions de soutien non essentielles vers un système non essentiel, un composant de système ou un fournisseur externe peut accroître l'efficacité en faisant en sorte que les fonctions et services en question se trouvent maintenant sous le contrôle de personnes ou de fournisseurs qui sont des spécialistes en la matière (EM) relativement à ces fonctions ou à ces services. Si un fournisseur externe a accès aux renseignements personnels, il est important de s'assurer que les contrôles de protection de la vie privée et les activités sont pris en compte dans les mécanismes de passation de marchés connexes.

PM-08 — Plan des infrastructures essentielles (---)

Énoncés :

Aborder les problèmes liés à la sécurité et à la protection de la vie privée de l'information qui touchent le développement, la documentation et la mise à jour d'un plan de protection visant les infrastructures essentielles et des ressources clés.

Responsable : Aucun

Discussion :

Les stratégies de protection sont basées sur la hiérarchisation des biens et des ressources indispensables. L'obligation et l'orientation nécessaires pour définir les infrastructures essentielles et les principales ressources et pour préparer un plan de protection des infrastructures essentielles connexes sont mentionnées dans les lois, la jurisprudence, les décrets, les directives, les politiques, la réglementation, les normes et les lignes directrices applicables.

PM-09 — Stratégie de gestion des risques (---)

Énoncés :

a. Élaborer une stratégie complète de gestion :
- **1.** des risques pour les activités et les biens organisationnels, les individus, les autres organisations et le gouvernement associés à l'exploitation et à l'utilisation des systèmes de l'organisation
- **2.** des risques d'atteinte à la vie privée qui pèsent sur les personnes dans le cadre du traitement autorisé des renseignements personnels

b. Mettre en place la stratégie de gestion des risques uniformément dans l'ensemble de l'organisation
c. Passer en revue et mettre à jour la stratégie de gestion des risques [Affectation : fréquence définie par l'organisation] ou au besoin pour tenir compte des changements organisationnels

Responsable : Aucun

Discussion :

Une stratégie de gestion des risques panorganisationnelle comprend une expression de la tolérance de l'organisation aux risques liés à la sécurité et à la protection de la vie privée, les stratégies d'atténuation des risques liés à la sécurité et à la protection de la vie privée, les méthodes d'évaluation des risques acceptables, un processus pour l'évaluation des risques liés à la sécurité et à la protection de la vie privée dans l'organisation en ce qui a trait à sa tolérance aux risques et les approches à adopter pour surveiller le risque au fil du temps. La ou le cadre supérieur responsable de la gestion des risques (chef du ministère ou haut responsable) s'assure que les processus de gestion de la sécurité de l'information s'alignent avec les processus de planification stratégique, opérationnelle et budgétaire. La fonction de gestion des risques exercée par la ou le cadre supérieur responsable de la gestion des risques peut faciliter une application uniforme de la stratégie de gestion des risques dans l'ensemble de l'organisation. La stratégie de gestion des risques peut reposer sur des intrants liés à la sécurité et à la protection de la vie privée qui sont tirés d'autres sources internes et externes à l'organisation et permettent d'assurer une portée générale et complète de la stratégie. La stratégie de gestion des risques liés à la chaîne d'approvisionnement décrite au contrôle PM-30 peut également fournir de l'information utile sur la stratégie de gestion des risques panorganisationnelle.

PM-10 — Processus d’autorisation (---)

Énoncés :

a. Gérer l’état de sécurité et de protection de la vie privée des systèmes organisationnels et des environnements dans lesquels ces systèmes s’exécutent dans le cadre des processus d’autorisation
b. Désigner les personnes qui assumeront des rôles et des responsabilités, en particulier dans le processus de gestion des risques de l’organisation
c. Intégrer les processus d’autorisation au programme panorganisationnel de gestion des risques

Responsable : Aucun

Discussion :

Les processus d’autorisation des systèmes organisationnels et des environnements d’exploitation exigent la mise en œuvre d’un processus de gestion des risques panorganisationnel, ainsi que des normes et des lignes directrices connexes en matière de sécurité et de protection de la vie privée. Parmi les rôles propres aux processus de gestion des risques, on retrouve une fonction de gestion des risques et des cadres supérieures et supérieurs désignés pour l’autorisation de chaque système organisationnel et d’un fournisseur de contrôles communs. Les processus d’autorisation de l’organisation sont intégrés à des processus de surveillance continue pour faciliter la compréhension et l’acceptation des risques liés à la sécurité et à la protection de la vie privée qui pèsent sur les activités, les individus et les biens liés à l’organisation, ainsi que les autres organisations et le gouvernement.

PM-11 — Définition des processus liés à la mission et aux activités (---)

Énoncés :

a. Développer des processus liés à la mission et aux activités de l'organisation en tenant compte de la sécurité et de la protection de la vie privée de l'information et du risque qui en résulte sur les activités et les biens organisationnels, les individus, les autres organisations et le gouvernement
b. Déterminer les besoins en matière de protection de l'information et de traitement des renseignements personnels qui découlent des processus liés à la mission et aux activités qui ont été définis
c. Examiner et revoir les processus liés à la mission et aux activités [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

Les besoins en matière de protection sont des capacités indépendantes de la technologie qui permettent de contrer les menaces qui ciblent les organisations, les individus, les systèmes et le gouvernement et d'éviter la compromission de l'information (c'est-à-dire, une atteinte à la protection de la vie privée, à l'intégrité, à la disponibilité ou à la vie privée). Les besoins en matière de protection de l'information et de traitement des renseignements personnels sont dérivés des besoins liés à la mission et aux activités qui ont été définis par les parties prenantes de l'organisation, les processus liés à la mission et aux activités mis en place pour répondre à ces besoins et la stratégie de gestion des risques de l'organisation. Les besoins en matière de protection de l'information et de traitement des renseignements personnels déterminent les contrôles nécessaires à l'organisation et aux systèmes. Pour définir les besoins en matière de protection de l'information et de traitement des renseignements personnels, il est essentiel de comprendre les répercussions négatives qui pourraient découler d'une compromission ou d'une fuite d'information. On fait appel à ce processus de catégorisation pour déterminer les répercussions potentielles. Les risques d'atteinte à la vie privée des individus peuvent être le résultat de la compromission de renseignements personnels, mais ils peuvent également survenir comme conséquences imprévues ou indirectes du traitement de renseignements personnels à n'importe quelle phase du cycle de vie de l'information. On utilise les EFVP pour relever les préjudices potentiels que pourrait causer le traitement des renseignements personnels. Ces évaluations des répercussions permettent de sélectionner les contrôles requis. Les définitions des processus liés à la mission et aux activités et les exigences connexes en matière de protection sont documentées conformément aux politiques et aux procédures de l'organisation.

PM-12 — Programme de protection contre la menace interne (---)

Énoncés :

Mettre en place un programme de protection contre la menace interne qui comprend une équipe multidisciplinaire de traitement des incidents liés à la menace interne.

Responsable : Aucun

Discussion :

Les programmes d'atténuation des menaces internes peuvent tirer parti de l'existence d'équipes de traitement des incidents mises en place par l'organisation, comme les équipes d'intervention en cas d'incident lié à la sécurité informatique. Les dossiers de ressources humaines sont particulièrement importants à cet égard, car des preuves convaincantes démontrent que certains types de crimes commis à l'interne sont souvent précédés de comportements atypiques en milieu de travail, comme la manifestation continue de signes de mécontentement et des conflits avec des collègues de travail et d'autres collègues. Ces signes précurseurs peuvent guider les responsables de l'organisme dans des efforts de surveillance plus ciblés. Cela dit, l'utilisation des dossiers des ressources humaines pourrait soulever des préoccupations importantes en matière de protection de la vie privée et de conformité à la Charte des droits et libertés de la personne. La participation d'une équipe juridique, y compris la consultation avec la ou le haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée approprié, permet de s'assurer que les activités de surveillance sont menées conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables.

PM-13 — Personnel affecté à la sécurité et à la protection de la vie privée (---)

Énoncés :

Élaborer un programme de développement et de perfectionnement du personnel affecté à la sécurité et à la protection de la vie privée.

Responsable : Aucun

Discussion :

Les programmes de développement et de perfectionnement du personnel affecté à la sécurité et à la protection de la vie privée visent à définir les connaissances, les compétences et les aptitudes nécessaires pour accomplir les tâches et les fonctions liées à la sécurité et à la protection de la vie privée, à développer des programmes de formation basés sur les rôles pour les personnes à qui on a confié des responsabilités et des rôles liés à la sécurité et à la protection de la vie privée, et à fournir les normes et les lignes directrices pour la mesure et l'élaboration des compétences attendues des titulaires de postes liés à la sécurité et à la protection de la vie privée et des candidates et candidats voulant occuper de tels postes. De tels programmes de développement et de perfectionnement du personnel peuvent également comprendre des parcours de carrière en sécurité et en protection de la vie privée pour encourager les professionnelles et professionnels de la sécurité et de la protection de la vie privée à se perfectionner dans le domaine et à occuper des postes exigeant de plus grandes responsabilités. Les programmes incitent les organisations à pourvoir les postes liés à la sécurité et à la protection de la vie privée par du personnel qualifié. Les programmes de développement et de perfectionnement du personnel affecté à la sécurité et à la protection de la vie privée sont complémentaires aux programmes organisationnels de formation et de sensibilisation à la sécurité et mettent l'accent sur le développement et l'institutionnalisation des principales capacités du personnel en matière de sécurité et de protection de la vie privée qui sont nécessaires pour protéger les activités, les biens et le personnel de l'organisation. Une main-d'œuvre qualifiée mise sur des employées et employés qui ont les ressources, les outils, les relations, la formation, la sensibilisation et la supervision nécessaires pour leur permettre de mettre en pratique leurs connaissances et leurs compétences dans le cadre de leurs tâches quotidiennes.

PM-14 — Tests, formation et surveillance (---)

Énoncés :

a. Mettre en place un processus visant à s'assurer que les plans organisationnels liés à la conduite des activités de mise à l'essai, de formation et de surveillance en matière de sécurité qui sont associées aux systèmes organisationnels :

1. sont élaborés et tenus à jour
2. continuent d'être exécutés

b. Passer en revue les plans de mise à l'essai, de formation et de surveillance pour veiller à ce qu'ils soient uniformes avec la stratégie organisationnelle de gestion des risques en matière de sécurité et de protection de la vie privée, et les priorités panorganisationnelles en ce qui a trait aux mesures d'intervention liées aux risques

Responsable : Aucun

Discussion :

La mise en place d'un processus panorganisationnel pour les tests, la formation et la surveillance en matière de sécurité et de protection de la vie privée permet de s'assurer que l'organisation supervise et coordonne les activités de tests, de formation et de surveillance. Étant donné l'importance grandissante des programmes de surveillance continue, la mise en œuvre de la sécurité et de la protection de la vie privée de l'information à chacun des trois niveaux hiérarchiques de la gestion des risques et l'utilisation à grande échelle de contrôles communs, les organisations coordonnent et regroupent les activités de tests et de surveillance qui sont menées de façon régulière dans le cadre d'évaluations continues visant à soutenir une gamme de contrôles. Bien qu'elles mettent l'accent sur des systèmes et des rôles en particulier, les activités de formation en sécurité et en protection de la vie privée doivent être coordonnées pour tous les éléments de l'organisation. Les plans et les activités de tests, de formation et de surveillance reposent sur les évaluations des menaces et des vulnérabilités actuelles.

PM-15 — Groupes et associations de sécurité et de protection de la vie privée (---)

Énoncés :

Déterminer et institutionnaliser les contacts avec certains groupes et certaines associations de la collectivité de la sécurité pour :
a. faciliter la formation continue de son personnel en matière de sécurité et de protection de la vie privée
b. se tenir au fait des pratiques, des techniques et des technologies recommandées en matière de sécurité et de protection de la vie privée
c. échanger de l'information à jour sur la sécurité et la protection de la vie privée, notamment sur les menaces, les vulnérabilités et les incidents

Responsable : Aucun

Discussion :

Il est important de maintenir un contact continu avec les groupes et associations de sécurité et de protection de la vie privée dans un environnement où les technologies et les menaces évoluent rapidement. Par groupes et associations, on entend les groupes d'intérêts spéciaux, les associations professionnelles, les forums spécialisés, les groupes de nouvelles, les groupes d'utilisatrices et utilisateurs et les groupes de pairs professionnels de la sécurité et de la protection de la vie privée dans des organisations similaires. L'organisation sélectionne les groupes et les associations de sécurité et de protection de la vie privée selon les fonctions liées à sa mission et à ses activités. L'organisation échange de l'information sur les menaces, les vulnérabilités et les incidents, ainsi que du contexte, des techniques de conformité et des problèmes liés à la protection de la vie privée conformément aux lois, aux décrets, aux directives, aux politiques, à la réglementation, aux normes et aux lignes directrices applicables.

PM-16 — Programme de sensibilisation aux menaces (---)

Énoncés :

Mettre en œuvre un programme de sensibilisation aux menaces qui comprend une capacité d'échange d'information interorganisationnelle pour le renseignement sur les menaces.

Responsable : Aucun

Discussion :

Comme les adversaires démontrent un degré de sophistication de plus en plus grand et en constant changement, en particulier pour ce qui a trait aux menaces persistantes avancées (MPA), il peut être plus probable que les adversaires arrivent à s'introduire dans les systèmes d'une organisation et à les compromettre. Une des meilleures techniques pour aborder cette préoccupation passe par l'échange de renseignement sur les menaces entre les organisations, notamment les événements de menace (par exemple, des tactiques, techniques et procédures) que les organisations ont rencontrés, les mesures d'atténuation prises par les organisations qui se sont avérées efficaces contre certains types de menaces et le renseignement sur les menaces (par exemple, la présence d'indices et d'avertissements concernant les menaces). L'échange de renseignement sur les menaces peut être bilatéral ou multilatéral. L'échange bilatéral de renseignement sur les menaces comprend les coopérations entre le gouvernement et le secteur privé et les coopérations intergouvernementales. L'échange multilatéral s'effectue quant à lui entre des organisations qui font partie d'un consortium sur l'échange de renseignement sur les menaces. Le renseignement sur les menaces exige des ententes et des mesures de protection spéciales, ou peut être échangé librement.

PM-16(01) — Moyens automatisés pour l'échange de renseignement sur les menaces (---)

Énoncés :

Avoir recours à des mécanismes automatisés pour maximiser l'efficacité de l'échange de renseignement sur les menaces.

Responsable : Aucun

Discussion :

Pour optimiser l'efficacité de la surveillance, il est important de savoir quelles données observables et quels indicateurs les capteurs devront rechercher. En utilisant des cadres d'applications, des services et des outils automatisés bien définis, les organisations sont mieux outillées pour échanger rapidement les signatures de détection des menaces pertinentes et de les intégrer aux outils de surveillance.

PM-17 — Protection de l'information contrôlée sur les systèmes externalisés (---)

Énoncés :

a. Établir la stratégie et les procédures nécessaires pour veiller à ce que les exigences relatives à la protection de l'information contrôlée qui est traitée, stockée ou transmise sur des systèmes externes, soient mises en œuvre conformément aux lois, aux décrets, aux directives, aux politiques, à la réglementation et aux normes applicables
b. Passer en revue et mettre à jour la stratégie et les procédures tous les [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

PM-18 — Plan du programme de protection de la vie privée (---)

Énoncés :

a. Élaborer et diffuser le plan du programme de protection de la vie privée panorganisationnel, qui offre une vue d'ensemble du programme de protection de la vie privée de l'organisation et :

1. comprend une description de la structure du programme de prestation des services en matière de protection de la vie privée et des ressources consacrées au programme de protection de la vie privée

2. donne une vue d'ensemble des exigences liées au programme de protection de la vie privée et une description des contrôles de gestion du programme de protection de la vie privée et des contrôles communs qui ont été mis en place ou que l'on envisage de mettre en place en vue de satisfaire ces exigences

3. comprend le rôle de la ou du haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée approprié, décrit la délégation officielle des pouvoirs de l'administratrice générale ou de l'administrateur général, et établit et affecte les rôles et responsabilités des autres cadres supérieures et supérieurs en matière de protection de la vie privée et de leur personnel

4. décrit l'engagement de la direction, les exigences relatives à la conformité, ainsi que les buts et les objectifs du programme de protection de la vie privée

5. tient compte de la coordination parmi les entités organisationnelles responsables des différents aspects de la protection de la vie privée

6. est approuvé par une ou un cadre supérieur ayant les responsabilités et la reddition de comptes nécessaires pour le risque qui pèse sur la protection de la vie privée des opérations organisationnelles (ce qui comprend la mission, les fonctions, l'image et la réputation), les biens organisationnels, les individus, les autres organisations et le gouvernement

b. Mettre à jour le plan [Affectation : fréquence définie par l'organisation] et tenir compte des changements apportés à l'application des lois en matière de respect de la vie privée en fonction de la jurisprudence, des changements stratégiques et organisationnels et des problèmes relevés au cours de la mise en œuvre du plan ou des évaluations de contrôle de la protection de la vie privée a

a. S'assurer que le plan du programme de protection de la vie privée est communiqué et transmis au personnel responsable de sa mise en œuvre

Responsable : Aucun

Discussion :

Le plan du programme de protection de la vie privée est un document formel qui offre une vue d'ensemble du programme de protection de la vie privée d'une organisation, notamment une description de la structure du programme de protection de la vie privée, les ressources consacrées au programme de protection de la vie privée, le rôle de la ou du haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée approprié, les buts et objectifs stratégiques du programme de protection de la vie privée, de même que les contrôles de gestion des programmes et les contrôles communs qui ont été mis en place ou que l'on envisage de mettre en place pour répondre aux exigences de protection de la vie privée applicables et gérer les risques d'atteinte à la vie privée. Le plan des programmes de protection de la vie privée peut être représenté dans un seul document ou un ensemble de documents. Il incombe à la ou au haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée d'établir les contrôles de protection de la vie privée qui seront traités par l'organisation comme des contrôles courants, hybrides, de gestion des programmes et propres aux systèmes. Les plans des programmes de protection de la vie privée fournissent suffisamment d'information sur les contrôles communs et de gestion des programmes de protection de la vie privée (y compris la spécification explicite ou par référence des paramètres d'affectation et de sélection) pour permettre une mise en œuvre clairement conforme à leurs objectifs et la détermination des risques qu'ils représentent, s'ils sont appliqués comme prévu. Les contrôles de gestion des problèmes sont généralement mis en œuvre au niveau de l'organisation et sont essentiels à la gestion du programme de protection de la vie privée de l'organisation. Les contrôles de gestion des programmes se distinguent des contrôles hybrides, courants et propres aux systèmes, puisqu'ils sont indépendants de tout système d'information. Ensemble, les plans de protection de la vie privée individuels et le plan du programme de protection de la vie privée panorganisationnel fournissent une couverture complète des contrôles de protection de la vie privée employés dans l'organisation. Les contrôles communs sont documentés dans une annexe du plan du programme de protection de la vie privée de l'organisation, à moins qu'ils ne soient compris dans le plan de protection de la vie privée distinct d'un système. Le plan du programme de protection de la vie privée panorganisationnel précise quels plans de protection de la vie privée distincts contiennent les descriptions des contrôles de protection de la vie privée.

PM-19 — Rôle de leadership du programme de protection de la vie privée (---)

Énoncés :

Désigner une ou un haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée et lui conférer les pouvoirs, la mission, les responsabilités et les ressources nécessaires pour coordonner, élaborer et mettre en place les exigences de protection de la vie privée applicables et pour gérer les risques d'atteinte à la vie privée dans le cadre du programme de protection de la vie privée panorganisationnel.

Responsable : Aucun

Discussion :

L'agente ou agent à la protection des renseignements personnels est une ou un cadre supérieur de l'organisation.

PM-20 — Communication des principaux services de protection de la vie privée (---)

Énoncés :

Tenir à jour une page Web centrale des ressources sur le site Web principal public de l'organisation, qui sert de source centralisée d'information sur les services de protection de la vie privée de l'organisation et :
a. permet de s'assurer que le public a accès à une liste des programmes et des services qui collectent et utilisent des renseignements personnels
b. veille à ce que les stratégies, les pratiques et les ressources organisationnelles en matière de protection de la vie privée soient publiées
c. rend public des adresses courriel et des numéros de téléphone afin que le public puisse fournir une rétroaction et poser des questions aux bureaux de la protection des renseignements personnels concernant les pratiques en matière de respect de la vie privée a
a. comprend les résumés des évaluations des facteurs relatifs à la vie privée qui ont été réalisées bb. fournit de l'orientation pour aider les personnes à soumettre une demande d'accès à leurs renseignements personnels, à soumettre une demande de correction officielle de leur dossier ou à déposer une plainte officielle si elles décident de le faire

Responsable : Aucun

PM-20(01) — Politiques de protection de la vie privée pour les sites Web, les applications et les services numériques (---)

Énoncés :

Élaborer et diffuser les politiques de protection de la vie privée sur tous les sites Web externes, les applications mobiles et les autres services numériques si la vie privée des personnes qui visitent les sites Web est à risque. S'assurer que les politiques :
a. sont rédigées dans un langage clair et organisées de manière à faciliter leur compréhension et leur consultation
b. fournissent l'information dont le public a besoin pour prendre une décision éclairée sur la pertinence et la façon d'interagir avec l'organisation
c. sont mises à jour chaque fois que l'organisation apporte des changements importants aux pratiques qu'elles visent à décrire et incluent l'estampille temporelle pour informer le public de la date des plus récents changements

Responsable : Aucun

Discussion :

Les organisations élaborent et publient les politiques de protection de la vie privée sur tous les sites Web externes, les applications mobiles et les autres services numériques si la vie privée des personnes qui visitent les sites Web est à risque. Les organisations publient un lien vers la politique de protection de la vie privée pertinente sur tous les points d'entrée majeurs connus qui mènent au site Web, à une application ou à un service numérique. Les organisations peuvent être sujettes aux lois, aux directives, à la réglementation ou aux politiques applicables en vertu desquelles il convient de fournir des renseignements particuliers au public. Le personnel de l'organisation consulte la ou le haut fonctionnaire ou cadre supérieur et la conseillère ou le conseiller juridique en matière de protection de la vie privée concernant de telles exigences.

PM-21 — Maintien d’un registre des divulgations (---)

Énoncés :

a. Mettre en place les procédures relatives à la divulgation des renseignements personnels et au maintien d’un registre des divulgations, notamment :

1. la date et les détails de la divulgation

2. le poste et l’adresse (ou autres coordonnées) de la personne ou de l’organisation à qui l’information a été divulguée

b. Conserver un registre des divulgations pour la période durant laquelle les renseignements personnels sont conservés ou conformément aux normes de gestion de l’information de l’organisation

c. Faire en sorte que le registre des divulgations soit accessible sur demande aux personnes à qui se rapportent les renseignements personnels dans la mesure où la divulgation respecte les exceptions citées dans la Loi sur l’accès aux documents des organismes publics et sur la protection des renseignements personnels a

a. Conclure un contrat, un accord d’échange de renseignements ou une entente d’échange de renseignements pour documenter les mesures de protection appropriées avant toute divulgation de renseignements personnels à un autre programme gouvernemental ou à une autre entité du secteur public ou privé

Responsable : Aucun

Discussion :

L’objectif du registre des divulgations est de permettre aux personnes de savoir à qui leurs renseignements personnels ont été divulgués, de fournir une base pour aviser les autres destinataires des renseignements personnels corrigés ou annotés et d’offrir une piste de vérification pour les examens subséquents de la conformité de l’organisation aux conditions applicables aux divulgations. La Loi sur la protection des renseignements personnels dans le secteur privé exige généralement que l’organisation obtienne le consentement des individus avant de divulguer leurs renseignements personnels. L’organisation peut utiliser n’importe quel système pour maintenir un registre des divulgations. Si elle peut bâtir un tel système, il conviendra d’utiliser un document dressant la liste de toutes les divulgations et d’y consigner toute l’information requise. Des mécanismes automatisés peuvent être utilisés par les organisations pour déterminer le moment où les renseignements personnels seront divulgués, y compris des services commerciaux qui fournissent des notifications et des alertes. On peut également avoir recours à des registres des divulgations pour aider les organisations à vérifier la conformité aux lois applicables sur la protection de la vie privée et aux politiques qui régissent la divulgation ou l’élimination de l’information, ainsi que les restrictions en matière d’élimination.

PM-22 — Gestion de la qualité des renseignements personnels (---)

Énoncés :

Élaborer et documenter les stratégies et les procédures panorganisationnelles pour :
a. assurer l'exactitude, la pertinence, la rapidité et l'exhaustivité des renseignements personnels tout au long du cycle de vie de l'information
b. mettre en place un processus de correction des registres qui facilite la correction ou la suppression de renseignements personnels inexacts ou obsolètes
c. mettre en place un processus de correction des registres qui facilite la diffusion des avis de renseignements personnels corrigés lorsque de l'information erronée a été divulguée précédemment a
a. s'assurer que les procédures de collecte respectent les exigences imposées par les lois applicables bb. documenter toute modification ou tout changement apporté aux renseignements, y compris la date et les sources du changement d'information

Responsable : Aucun

Discussion :

La gestion de la qualité des renseignements personnels comprend les étapes prises par l'organisation pour confirmer l'exactitude et la pertinence des renseignements personnels tout au long du cycle de vie de l'information. Le cycle de vie des renseignements personnels comprend la création, la collecte, l'utilisation, la correction, la conservation, la divulgation et l'élimination des renseignements personnels. Les stratégies et procédures organisationnelles relatives à la gestion des renseignements personnels sont importantes, puisque le maintien de renseignements personnels inexacts ou obsolètes par les organisations pourrait causer des problèmes aux personnes à qui appartiennent ces renseignements. L'organisation considère la qualité des renseignements personnels pris en compte dans les fonctions liées aux activités dans la mesure où l'inexactitude de tels renseignements pourrait donner lieu à des décisions défavorables ou à un refus des avantages et des services, ou lorsque la divulgation de tels renseignements pourrait mener à de la stigmatisation. Dans certaines circonstances, des renseignements personnels erronés peuvent causer des problèmes aux individus qui surpassent les avantages que les organisations pourraient tirer du maintien de tels renseignements. Les organisations devraient envisager de mettre en place des stratégies et des procédures pour le retrait de ces renseignements personnels. La ou le haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée approprié s'assure que des moyens et des mécanismes pratiques ont été mis en place et qu'ils sont accessibles aux personnes qui veulent corriger des renseignements personnels ou les supprimer, ainsi qu'à leurs représentantes et représentants autorisés. Les processus de correction ou de suppression des données sont clairement définis et accessibles au public. Les organisations exercent un pouvoir discrétionnaire au moment de déterminer s'il convient de corriger ou de supprimer les données selon l'ampleur des demandes, les changements à apporter et l'incidence des changements. De plus, les processus doivent faire en sorte de fournir des réponses aux personnes appelées à décider s'il convient ou non de refuser les demandes de correction ou de suppression. Les réponses devraient comprendre les raisons des décisions, un moyen de consigner chacune des objections aux décisions, ainsi qu'un moyen de déposer une plainte auprès de la Commission d'accès à l'information du Québec (CAI) si la personne veut pousser la question plus loin. Les organisations informent les personnes, ou les représentantes ou représentants qu'elles ont désignés, une fois que les renseignements personnels sont corrigés ou supprimés pour offrir plus de transparence et confirmer que l'action a été effectuée. Étant donné la complexité des flux de données et du stockage, d'autres entités pourraient devoir être informées de la correction ou de la suppression. Les avis appuient une correction et une suppression uniformes des renseignements personnels dans tout l'écosystème des données.

PM-23 — Comité de gouvernance des données (---)

Énoncés :

Mettre en place un comité de gouvernance des données composé de [Affectation : rôles définis par l'organisation] avec [Affectation : responsabilités définies par l'organisation].

Responsable : Aucun

Discussion :

Un comité de gouvernance des données peut aider à s'assurer que l'organisation dispose de stratégies cohérentes et est en mesure de trouver un équilibre entre l'utilité des données et les exigences de sécurité et de protection de la vie privée. Le comité de gouvernance des données met en place les stratégies, les procédures et les normes qui facilitent la gouvernance des données de manière à ce que ces données, dont les renseignements personnels, soient gérées et tenues à jour efficacement, conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Les responsabilités peuvent comprendre l'élaboration et la mise en œuvre des lignes directrices qui soutiennent les besoins pour des renseignements personnels en ce qui concerne la modélisation, la qualité, l'intégrité et la dépersonnalisation des données tout au long du cycle de vie de l'information. Le comité de gouvernance des données peut superviser l'examen et l'approbation des applications pour la diffusion de données à l'extérieur de l'organisation, l'archivage des applications et les données diffusées, ainsi que la surveillance postdiffusion afin d'assurer la validité des hypothèses émises lors de la diffusion des données. Le comité de gouvernance des données peut également superviser l'utilisation des données, dont les renseignements personnels, dans les technologies comme l'analytique de pointe, l'automatisation et l'intelligence artificielle; procéder à des analyses statistiques pour relever et atténuer les biais systématiques dans les systèmes et les données des institutions; analyser les techniques de dépersonnalisation pour garantir une efficacité continue; et veiller à ce que les mécanismes de responsabilisation appropriés soient mis en place, mis à jour, compris et respectés. Les membres comprennent généralement la ou le DPI, la ou le DPS et la ou le haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée, comme une ou un chef de la protection des renseignements personnels (CPRP).

PM-24 — Comité de l’intégrité des données (---)

Énoncés :

Mettre en place un comité de l’intégrité des données pour :
a. examiner les propositions visant à organiser un programme d’appariement statistique ou à y participer
b. procéder à un examen annuel de tous les programmes d’appariement statistique auxquels l’organisation a pris part

Responsable : Aucun

PM-25 — Réduction des renseignements personnels utilisés aux fins de tests, de formation et de recherche (---)

Énoncés :

a. Élaborer, documenter et mettre en place des stratégies et des procédures qui abordent l'utilisation de renseignements personnels aux fins de test, de formation et de recherche
b. Limiter ou réduire la quantité de renseignements personnels utilisés aux fins de test, de formation et de recherche
c. Autoriser l'utilisation de renseignements personnels aux fins de tests, de formation et de recherche internes lorsque le résultat requis ne peut être obtenu sans le recours aux renseignements personnels
d. Passer en revue et mettre à jour les stratégies et les procédures [Affectation : fréquence définie par l'organisation] a
a. Limiter la divulgation des jeux de données contenant des renseignements personnels aux entrepreneures et entrepreneurs externes, dans la mesure du possible

Responsable : Aucun

Discussion :

L'utilisation de renseignements personnels aux fins de test, de formation et de recherche augmente le risque d'utilisation et de divulgation non autorisées de tels renseignements. L'organisation consulte la ou le haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée désigné et/ou la conseillère ou le conseiller juridique pour veiller à ce que l'utilisation de renseignements personnels aux fins de test, de formation et de recherche respecte la raison pour laquelle ceux-ci ont été recueillis initialement. Dans la mesure du possible, l'organisation utilise des données fictives (dépersonnalisées ou anonymisées) pour éviter d'exposer les renseignements personnels au moment d'effectuer des tests, d'offrir des formations et de mener des recherches. Si on ne peut éviter d'utiliser des renseignements personnels dans ces environnements, les environnements de test, de formation et de recherche deviennent alors sujets aux mêmes exigences en matière de contrôles que l'environnement initial.

PM-26 — Gestion des plaintes (---)

Énoncés :

Mettre en place un processus pour la réception et le traitement des plaintes, des préoccupations ou des questions des individus concernant les pratiques de l'organisation en matière de sécurité et de protection de la vie privée, ce qui comprend :
a. des mécanismes simples à utiliser et facilement accessibles au public
b. toute l'information nécessaire pour déposer une plainte
c. les mécanismes de suivi nécessaires pour veiller à ce que toutes les plaintes reçues soient examinées et traitées dans les [Affectation : délais définis par l'organisation]
d. accuser réception des plaintes, des préoccupations ou des questions des individus dans les [Affectation : délais définis par l'organisation]
e. répondre avec discrétion aux plaintes, aux préoccupations ou aux questions des individus dans les [Affectation : délais définis par l'organisation]

Responsable : Aucun

Discussion :

Les plaintes, les préoccupations et les questions des individus peuvent être une source précieuse d'information pour les organisations et permettre ultimement d'améliorer les modèles opérationnels, l'utilisation de la technologie, les pratiques en matière de collecte de données et les contrôles. Parmi les mécanismes qui peuvent être utilisés par le public, on retrouve le service d'aide téléphonique, les courriels et les formulaires en ligne. L'information nécessaire pour déposer les plaintes comprend les coordonnées de la ou du haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée désigné ou de toute ou tout autre responsable désigné pour recevoir les plaintes. Les plaintes concernant la protection de la vie privée peuvent également comprendre des renseignements personnels qui sont traités conformément aux stratégies et aux processus pertinents. Dans certaines circonstances, la Commission d'accès à l'information du Québec (CAI) peut lancer sa propre enquête ou déposer une plainte.

PM-27 — Génération de rapports concernant la protection de la vie privée (---)

Énoncés :

a. Élaborer [Affectation : rapports concernant la protection de la vie privée désignés par l'organisation] et les diffuser :
- **1.** aux [Affectation : organes d'examen désignés par l'organisation] pour démontrer la responsabilité quant aux mandats de réglementation, ainsi que les mandats conférés par la loi et relatifs aux politiques de protection de la vie privée
- **2.** aux [Affectation : responsables désignées ou désignés par l'organisation] et aux autres membres du personnel responsables de surveiller la conformité au programme de protection de la vie privée

b. Passer en revue et mettre à jour les rapports [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

PM-28 — Cadrage des risques (---)

Énoncés :

a. Établir et documenter :
- **1.** les hypothèses relatives à l'évaluation des risques, aux mesures d'atténuation des risques et à la surveillance des risques
- **2.** les contraintes relatives à l'évaluation des risques, aux mesures d'atténuation des risques et à la surveillance des risques
- **3.** les priorités et les compromis envisagés par l'organisation pour gérer le risque
- **4.** la tolérance au risque de l'organisation

b. Distribuer les résultats des activités de cadrage des risques à [Affectation : personnel désigné par l'organisation]
c. Passer en revue et mettre à jour les facteurs à considérer sur le plan du cadrage des risques [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

Le cadrage des risques est plus efficace lorsqu'on l'exécute au niveau de l'organisation et en consultation avec des parties prenantes de toute l'organisation, y compris les propriétaires de la mission, des activités et des systèmes. Les hypothèses, les contraintes, la tolérance au risque, les priorités et les compromis relevés dans le cadre du processus de cadrage des risques éclairent la stratégie de gestion des risques, qui éclaire ensuite l'évaluation des risques, les mesures d'atténuation des risques et les activités de surveillance des risques. Les résultats du cadrage des risques sont communiqués au personnel de l'organisation, y compris les propriétaires de la mission et des activités, les propriétaires, gardiennes et gardiens d'information, les propriétaires de système, les cadres supérieures et supérieurs désignés responsables de l'autorisation, les agentes ou agents supérieurs de la sécurité de l'information de l'organisme, la ou le haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée, et la ou le cadre supérieur responsable de la gestion des risques.

PM-29 — Rôles de leadership pour le programme de gestion des risques (---)

Énoncés :

a. Nommer une ou un cadre supérieur responsable de la gestion des risques pour veiller à ce que les processus organisationnels de gestion de la sécurité et de la protection de la vie privée de l'information soient conformes aux processus de planification stratégique, opérationnelle et budgétaire
b. Mettre en place une fonction de gestion des risques pour considérer et analyser le risque d'un point de vue panorganisationnel et s'assurer que la gestion des risques est uniforme à travers l'organisation

Responsable : Aucun

Discussion :

La ou le cadre supérieur responsable de la gestion des risques dirige la fonction de gestion des risques lors des activités panorganisationnelles de gestion des risques.

PM-30 — Stratégie de gestion des risques liés à la chaîne d'approvisionnement (---)

Énoncés :

a. Élaborer une stratégie panorganisationnelle pour gérer les risques liés à la chaîne d'approvisionnement associés au développement, à l'acquisition, à la maintenance et à la disposition des systèmes, des composants de systèmes et des services qui s'y rapportent
b. Mettre en place la stratégie de gestion des risques liés à la chaîne d'approvisionnement uniformément dans l'ensemble de l'organisation
c. Passer en revue et mettre à jour la stratégie de gestion des risques liés à la chaîne d'approvisionnement [Affectation : fréquence définie par l'organisation] ou au besoin pour tenir compte des changements organisationnels

Responsable : Aucun

Discussion :

La stratégie panorganisationnelle de gestion des risques liés à la chaîne d'approvisionnement comprend une expression claire de la propension et de la tolérance aux risques liés à la chaîne d'approvisionnement de l'organisation, des stratégies ou contrôles d'atténuation des risques acceptables liés à la chaîne d'approvisionnement, un processus visant à évaluer et à surveiller continuellement les risques liés à la chaîne d'approvisionnement, des approches à adopter pour la mise en œuvre et la communication de la stratégie de gestion des risques liés à la chaîne d'approvisionnement, et les rôles et responsabilités connexes. La gestion des risques liés à la chaîne d'approvisionnement comprend les facteurs à considérer concernant les risques liés à la sécurité et à la protection de la vie privée associés au développement, à l'acquisition, à la maintenance et à la disposition des systèmes, des composants de systèmes et des services qui s'y rapportent. La stratégie de gestion des risques liés à la chaîne d'approvisionnement peut être intégrée à la stratégie globale de gestion des risques de l'organisation et peut guider et orienter les stratégies liées à la chaîne d'approvisionnement et les plans de gestion des risques liés à la chaîne d'approvisionnement au niveau des systèmes. De plus, le recours à une fonction de gestion des risques peut faciliter une application uniforme de la stratégie de gestion des risques liés à la chaîne d'approvisionnement dans toute l'organisation. La stratégie de gestion des risques liés à la chaîne d'approvisionnement est mise en place au niveau de l'organisation, de la mission et des activités, tandis que le plan de gestion des risques liés à la chaîne d'approvisionnement (voir le contrôle SR-02) est mis en œuvre au niveau du système.

PM-30(01) — Fournisseurs d’articles critiques ou essentiels à la mission (---)

Énoncés :

Identifier, prioriser et évaluer les fournisseurs de technologies, de produits et de services critiques ou essentiels à la mission.

Responsable : Aucun

Discussion :

Le succès de la mission et des activités des organisations repose sur l’identification et la priorisation des fournisseurs de technologies, de produits et de services critiques ou essentiels à la mission. L’évaluation des fournisseurs est réalisée à partir des examens des fournisseurs (voir le contrôle SR-06) et des processus de gestion des risques liés à la chaîne d’approvisionnement (voir le contrôle RA-03(01)). Une analyse des risques liés à la chaîne d’approvisionnement peut aider une organisation à identifier les systèmes ou les composants pour lesquels il est nécessaire de prendre de plus amples mesures d’atténuation de tels risques.

PM-31 — Stratégie de surveillance continue (---)

Énoncés :

Élaborer une stratégie de surveillance continue panorganisationnelle et mettre en place des programmes de surveillance continue qui tiennent compte de :
a. l'établissement des mesures panorganisationnelles suivantes qu'il convient de surveiller [Affectation : mesures définies par l'organisation]
b. la mise en place de [Affectation : fréquences de surveillance définies par l'organisation] et de [Affectation : fréquences d'évaluation définies par l'organisation] pour l'efficacité des contrôles
c. la surveillance en permanence des mesures définies par l'organisation, conformément à la stratégie de surveillance continue définie par l'organisation
d. la corrélation et l'analyse de l'information générée par les évaluations de contrôle et la surveillance
e. les mesures d'intervention concernant les résultats qui découlent de l'analyse de l'information
f. le signalement de l'état de la sécurité et de la protection de la vie privée du système à [Affectation : personnel ou rôles définis par l'organisation] [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

La surveillance continue au niveau de l'organisation facilite une sensibilisation permanente de la posture de sécurité et de protection de la vie privée dans l'ensemble de l'organisation afin d'appuyer les décisions relatives à la gestion des risques organisationnels. Les termes « continu » et « permanent » signifient que les organisations évaluent et surveillent leurs contrôles et leurs risques à une fréquence suffisante pour appuyer les décisions en fonction des risques. Différents types de contrôles peuvent nécessiter différentes fréquences de surveillance. Les résultats associés à une surveillance continue orientent et éclairent les mesures d'intervention liées aux risques que mettent en œuvre les organisations. Grâce aux programmes de surveillance continue, les organisations peuvent maintenir en permanence les autorisations des systèmes de même que les contrôles communs dans un environnement d'exploitation très dynamique où les menaces, les vulnérabilités, les technologies et les besoins liés à la mission et aux activités sont en constante évolution. L'accès constant à l'information sur la sécurité et la protection de la vie privée dans les rapports ou les tableaux de bord permet aux responsables des organisations de prendre des décisions éclairées sur la gestion des risques de façon efficace et opportune, comme des décisions sur les autorisations permanentes. Pour faciliter la gestion des risques liés à la sécurité et à la protection de la vie privée, l'organisation considère d'aligner les mesures de la surveillance définies par l'organisation sur sa tolérance au risque, comme il est indiqué dans la stratégie sur la gestion des risques. Les exigences en matière de surveillance du système, y compris la nécessité d'avoir recours à la surveillance, peuvent se trouver dans d'autres exigences, comme AC-02G, AC-02(07), AC-02(12)a, AC-02(07)b, AC-02(07)c, AC-17(01), AT-04A, AU-13, AU-13(01), AU-13(02), CA-07, CM-03F, CM-06D, CM-11C, IR-05, MA-02B, MA-03A, MA-04A, PE-03D, PE-06, PE-14B, PE-16, PE-20, PM-06, PM-23, PS-07E, SA-09C, SC-05(03)b, SC-07A, SC-07(24)b, SC-18B, SC-43B et SI-04.

PM-32 — Établissement des objectifs (---)

Énoncés :

Analyser les [Affectation : systèmes ou composants de systèmes désignés par l'organisation] qui prennent en charge les fonctions ou les services essentiels à la mission pour s'assurer que les ressources d'information sont utilisées aux fins prévues.

Responsable : Aucun

Discussion :

Les systèmes sont conçus pour soutenir une fonction liée à la mission ou aux activités. Au fil du temps, les systèmes et les composants des systèmes peuvent être utilisés pour soutenir des fonctions et des services qui ne relèvent pas de la portée des fonctions liées à la mission ou aux activités qui ont été prévues. Cela pourrait donner lieu à l'exposition des ressources d'information dans des environnements non prévus et à une utilisation susceptible d'accroître considérablement l'exposition aux menaces. Les systèmes sont ainsi plus vulnérables à la compromission, ce qui peut ultimement avoir une incidence sur les services et les fonctions pour lesquels ils sont prévus. C'est particulièrement le cas pour les fonctions et les services essentiels à la mission. L'analyse des ressources permet aux organisations de cerner les expositions potentielles.

PS

Sécurité du personnel (vérifications, accès, etc.)

Personnel Security

PS-01 — Politique et procédures de sécurité du personnel (---)

Énoncés :

a. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :

1. une politique de sécurité du personnel [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables

2. des procédures facilitant la mise en oeuvre des politiques de sécurité du personnel et des contrôles de sécurité du personnel connexes

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à la sécurité du personnel

c. Passer en revue et mettre à jour, par rapport à la sécurité du personnel :

1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La politique et les procédures de sécurité du personnel abordent les contrôles de la famille PS qui ont été mis en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à leur élaboration. En règle générale, les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin pour des politiques et des procédures propres à la mission ou au système. La politique peut être intégrée à la politique générale sur la sécurité et la protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures de sécurité du personnel comprennent, sans s'y limiter, les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.

PS-02 — Analyse de sécurité des postes (---)

Énoncés :

a. Déterminer les exigences en matière de filtrage de sécurité pour tous les postes de l'organisation
b. Établir les critères de sélection des personnes occupant ces postes
c. Passer en revue et mettre à jour l'exigence en matière de filtrage de sécurité [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

Le niveau du filtrage de sécurité et les autorisations d'accès sont déterminés par les fonctions à effectuer, la sensibilité de l'information, des installations et des biens auxquels il sera possible d'accéder, au niveau d'autorité ou de contrôle exercé par la ou le titulaire du poste, et au degré de préjudice qui pourrait résulter de la compromission de l'information sensible, des installations ou des biens auxquels il sera possible d'accéder. Les résultats de l'analyse de sécurité des postes déterminent le niveau de la demande, les vérifications requises et les évaluations à effectuer pour un poste.

PS-03 — Filtrage de sécurité du personnel (---)

Énoncés :

a. Procéder au filtrage de sécurité des personnes avant de leur accorder l'accès au système
b. Effectuer une nouvelle enquête de sécurité lorsque [Affectation : liste définie par l'organisation des conditions qui exigent un nouveau filtrage de sécurité et de la fréquence de ce filtrage, le cas échéant]

Responsable : Aucun

Discussion :

Les activités liées aux deux types de filtrage reflètent les lois, les décrets, les directives, la réglementation, les politiques, les normes et les lignes directrices applicables, ainsi que les critères établis pour la désignation des risques associés au poste concerné. Les exemples de filtrage de sécurité du personnel comprennent les enquêtes sur les antécédents et la vérification des antécédents effectuée par des tiers. L'organisation peut définir différentes conditions et fréquences pour un nouveau filtrage du personnel qui accède aux systèmes selon le type d'information traitée, stockée ou transmise.

PS-03(01) — Information classifiée (---)

Énoncés :

S'assurer que chaque utilisatrice ou utilisateur d'un système qui traite, stocke ou transmet de l'information classifiée a une habilitation et un endoctrinement au plus haut niveau de classification de l'information à laquelle il a accès dans le système.

Responsable : Aucun

PS-03(02) — Endoctrinement officiel (---)

Énoncés :

S’assurer que chaque utilisatrice ou utilisateur d’un système qui traite, stocke ou transmet des types d’information classifiée pour lesquels il faut suivre une séance d’endoctrinement officielle est officiellement endoctriné pour tous les types d’information pertinents auxquels il a accès sur le système.

Responsable : Aucun

PS-03(03) — Information exigeant des mesures de protection spéciales (---)

Énoncés :

Vérifier si les personnes qui accèdent à un système qui traite, stocke ou transmet de l'information exigeant une protection spéciale :
a. possèdent une autorisation d'accès valide attestée par les fonctions gouvernementales officielles qui leur ont été assignées
b. satisfont aux [Affectation : critères additionnels de filtrage de sécurité du personnel définis par l'organisation]

Responsable : Aucun

PS-03(04) — Exigences relatives à la citoyenneté (---)

Énoncés :

Vérifier si les personnes qui accèdent à un système qui traite, stocke ou transmet [Affectation : types d'information définis par l'organisation] satisfont aux [Affectation : exigences relatives à la citoyenneté définies par l'organisation].

Responsable : Aucun

PS-04 — Cessation d'emploi du personnel (---)

Énoncés :

Lors de la cessation d'emploi d'une employée ou un employé :
a. désactiver l'accès au système dans une période de [Affectation : période définie par l'organisation]
b. mettre fin ou révoquer tous les authentifiants et les justificatifs d'identité associés à la personne
c. effectuer une entrevue de fin d'emploi et mener une discussion sur [Affectation : sujets liés à la sécurité de l'information définis par l'organisation]
d. récupérer toutes les propriétés liées à la sécurité et à un système organisationnel
e. conserver l'accès à l'information et aux systèmes précédemment contrôlés par la personne concernée

Responsable : Aucun

Discussion :

Les propriétés système comprennent les jetons d'authentification matériels, les manuels techniques d'administration de système, les clés, les cartes d'identité et les laissez-passer de l'édifice. Les entrevues de fin d'emploi permettent de s'assurer que les personnes concernées comprennent les contraintes de sécurité auxquelles elles doivent se soumettre à titre d'anciennes employées et anciens employés et leurs responsabilités à l'égard des biens associés au système. Lors des entrevues de fin d'emploi, l'équipe de la Sécurité veille à rappeler aux employées et employés leur acceptation des ententes de non-divulgation et les éventuelles limitations professionnelles dont ils pourraient faire l'objet. Il se peut qu'il soit impossible de procéder aux entrevues de départ pour certaines employées et certains employés, y compris dans les cas de non-disponibilité des superviseures et superviseurs, de maladie ou d'abandon de poste. Une exécution rapide des mesures de cessation d'emploi est essentielle dans les cas de congédiement pour motif valable. Dans certaines situations, l'organisation devrait envisager de désactiver les comptes de système des employées et employés ayant été congédiés avant même qu'ils ne soient informés.

PS-04(01) — Exigences régissant l'après-mandat (---)

Énoncés :

a. Informer les personnes ayant quitté leur emploi des exigences applicables régissant l'après-mandat auxquelles elles sont tenues par la loi de se conformer pour protéger l'information de l'organisation
b. Exiger que les personnes ayant quitté leur emploi signent un avis de reconnaissance des exigences régissant l'après-mandat dans le cadre du processus organisationnel de cessation d'emploi

Responsable : Aucun

PS-04(02) — Opérations automatisées (---)

Énoncés :

Utiliser des [Affectation : mécanismes automatisés définis par l'organisation] pour [Sélection (un choix ou plus) : informer [Affectation : personnel ou rôles définis par l'organisation] des mesures de cessation d'emploi; désactiver l'accès aux ressources des systèmes].

Responsable : Aucun

Discussion :

Dans les organisations qui comptent un grand nombre d'employées et employés, le personnel qui doit être mis au courant des mesures associées à la cessation d'emploi d'une ou un employé ne reçoit pas toujours les notifications appropriées ou ne les reçoit pas dans des délais opportuns. Des mécanismes automatisés peuvent être utilisés pour envoyer des alertes ou des notifications automatiques au personnel ou aux rôles de l'organisation lorsque des personnes font l'objet d'une cessation d'emploi. Ces alertes ou notifications peuvent être acheminées de différentes façons, que ce soit par téléphone, par courriel, par message texte ou par l'entremise d'un site Web. Des mécanismes automatisés peuvent également être employés pour désactiver rapidement et entièrement l'accès aux ressources des systèmes lors de la cessation d'emploi d'une ou un employé.

PS-04(400) — Astreint au secret à perpétuité (---)

Énoncés :

Transmettre les données sur le formulaire Registre d'une personne d'un ministère ou organisme mentionné à l'annexe en application de la Loi sur la protection de l'information (LPI) au Service canadien du renseignement de sécurité (SCRS).

Responsable : Aucun

PS-05 — Transfert du personnel (---)

Énoncés :

a. Examiner et confirmer les exigences opérationnelles liées aux autorisations d'accès physique et logique existantes aux systèmes et aux installations lorsque des employées et employés sont réaffectés ou transférés à d'autres postes au sein de l'organisation
b. Amorcer [Affectation : mesures de transfert ou de réaffectation définies par l'organisation] dans les [Affectation : délais définis par l'organisation suivant la prise de mesures de transfert officielles]
c. Modifier au besoin les autorisations d'accès afin de tenir compte de toute modification apportée aux exigences opérationnelles en raison d'une réaffectation ou d'un transfert
d. Informer [Affectation : personnel ou rôles définis par l'organisation] dans les [Affectation : délais définis par l'organisation]

Responsable : Aucun

Discussion :

Le transfert de personnel s'applique dans les cas où la réaffectation ou le transfert d'une ou un employé est permanent ou d'une durée qui justifie les mesures requises. De plus, l'organisation définit les mesures appropriées pour le type de réaffectation ou de transfert, qu'il soit permanent ou prolongé. Ces mesures comprennent le retour et le remplacement des anciens laissez-passer, cartes d'identité et clés, la fermeture des comptes de système et l'établissement de nouveaux, la modification des autorisations d'accès aux systèmes (c'est-à-dire, les privilèges) et l'octroi des accès aux dossiers officiels auxquels l'employée ou employé avait accès dans les lieux de travail précédents et au moyen des comptes de système précédents.

PS-05(400) — Autorisation de sécurité (---)

Énoncés :

a. Accepter la cote de fiabilité ou l'habilitation de la personne lorsque le niveau de celle qui est exigée est équivalent ou inférieur au niveau précédemment accordé
b. Refaire le processus de filtrage de sécurité lorsque :
- **1.** les résultats remontent à plus de cinq ans
- **2.** la preuve indique que le filtrage de sécurité n'a pas été fait précédemment
- **3.** une dispense de sécurité est jointe à la cote ou à l'autorisation
- **4.** les résultats des enquêtes sur l'exécution de la loi et des évaluations de sécurité ont été retirés du dossier de la personne concernée
- **5.** des renseignements défavorables figurant au dossier pourraient poser un risque de sécurité pour le ministère ou l'organisme d'arrivée

Responsable : Aucun

PS-06 — Ententes d'accès (---)

Énoncés :

a. Élaborer et documenter les ententes d'accès aux systèmes organisationnels
b. Passer en revue et mettre à jour les ententes d'accès [Affectation : fréquence définie par l'organisation]
c. S'assurer que les personnes qui ont besoin d'accéder à l'information et aux systèmes de l'organisation :
  1. signent les ententes d'accès appropriées avant qu'on leur accorde l'accès
  2. signent de nouveau les ententes d'accès pour conserver l'accès aux systèmes de l'organisation lorsque les ententes d'accès sont mises à jour ou [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

Les ententes d'accès comprennent les accords de non-divulgation, les ententes d'utilisation acceptable, les règles de conduite et les accords régissant les conflits d'intérêts. Une entente d'accès signée comprend une attestation que la personne a lu et compris les contraintes associées aux systèmes organisationnels auxquels on lui a accordé l'accès et qu'elle accepte de s'y conformer. Les signatures électroniques sont admises pour l'acceptation d'ententes d'accès, à moins d'être expressément interdites par les politiques de l'organisation.

PS-06(01) — Information exigeant une protection spéciale (---)

Énoncés :

Annulé : intégré au contrôle PS-03.

Responsable : Aucun

PS-06(02) — Information classifiée exigeant une protection spéciale (---)

Énoncés :

S'assurer que l'accès à l'information classifiée exigeant une protection spéciale est accordée uniquement aux personnes qui :
a. possèdent une autorisation d'accès valide attestée par les responsabilités gouvernementales officielles qui leur ont été conférées
b. satisfont aux critères connexes de sécurité du personnel
c. ont lu, compris et signé une entente de non-divulgation

Responsable : Aucun

PS-06(03) — Exigences régissant l'après-mandat (---)

Énoncés :

a. Informer les employées et employés des exigences applicables régissant l'après-mandat auxquelles elles sont tenues par la loi de se conformer pour protéger l'information de l'organisation
b. Exiger que les employées et employés attestent par écrit de ces exigences, le cas échéant, au moment d'accorder l'accès à l'information concernée

Responsable : Aucun

Discussion :

Les organisations se conforment aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables pour ce qui est des exigences régissant l'après-mandat des personnes ayant quitté leur emploi.

PS-07 — Sécurité du personnel externe (---)

Énoncés :

a. Définir les exigences liées à la sécurité du personnel, y compris les rôles et responsabilités des fournisseurs externes
b. Exiger que les fournisseurs externes se conforment aux stratégies et aux procédures en matière de sécurité du personnel mises en place par l'organisation
c. Documenter les exigences en matière de sécurité du personnel
d. Exiger que les fournisseurs externes informent [Affectation : personnel ou rôles définis par l'organisation] du transfert ou de la cessation d'emploi de toute employée ou tout employé de tierces parties qui possède des justificatifs d'identité et/ou des laissez-passer de l'organisation, ou dispose de privilèges d'accès au système dans les [Affectation : délais définis par l'organisation]
e. Surveiller la conformité des fournisseurs aux exigences en matière de sécurité du personnel
f. S'assurer que les organisations et les personnes du secteur privé qui ont accès à l'information, aux installations et aux biens protégés et classifiés font l'objet d'un filtrage de sécurité
g. Définir explicitement la surveillance gouvernementale et les rôles et responsabilités d'utilisatrice finale ou utilisateur final relativement aux services fournis par des tiers

Responsable : Aucun

Discussion :

Par fournisseurs externes, on entend les organisations autres que celle qui exploite ou acquiert le système. Les fournisseurs externes comprennent les bureaux de service, les entrepreneures et entrepreneurs, et les autres organisations qui assurent le développement des systèmes ou fournissent des services de TI, de test ou d'évaluation, ainsi que les applications externalisées et la gestion du réseau ou de la sécurité. Les organisations incluent explicitement les exigences en matière de sécurité du personnel dans les documents d'approvisionnement. Le personnel des fournisseurs externes peut travailler dans les installations de l'organisation si cette dernière lui remet des justificatifs d'identité, des laissez-passer ou des privilèges d'accès aux systèmes. Les avis envoyés advenant des changements au niveau du personnel externe permettent d'assurer l'annulation opportune des privilèges d'accès et des justificatifs d'identité. Les organisations déterminent quels seront les transferts et les cessations d'emploi à signaler en fonction de caractéristiques de sécurité comme les fonctions, les rôles et la nature des justificatifs d'identité et des privilèges associés aux personnes qui font l'objet du transfert ou de la cessation d'emploi.

PS-08 — Sanctions imposées au personnel (---)

Énoncés :

a. Utiliser un processus formel de sanctions pour le personnel qui ne se conforme pas aux stratégies et aux procédures de sécurité et de protection de la vie privée de l'information qui ont été établies
b. Informer [Affectation : personnel ou rôles définis par l'organisation] dans les [Affectation : délais définis par l'organisation] lorsque le processus formel de sanctions est amorcé et indique qui est l'employée ou employé sanctionné et les motifs de la sanction

Responsable : Aucun

PS-09 — Descriptions de poste (---)

Énoncés :

Intégrer les rôles et les responsabilités en matière de sécurité et de protection de la vie privée aux descriptions de postes de l'organisation.

Responsable : Aucun

Discussion :

Préciser les rôles liés à la sécurité et à la protection de la vie privée dans les descriptions de postes du personnel de l'organisation aide à clarifier les responsabilités associées aux rôles à ce sujet, ainsi que les exigences en matière de formation sur la sécurité et la protection de la vie privée basées sur les rôles.

PT

Traitement des renseignements personnels identifiables et transparence

Personally Identifiable Information Processing and Transparency

PT-01 — Politique et procédures de traitement des renseignements personnels et de transparence (---)

Énoncés :

a. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :

1. une politique de protection de la vie privée et des procédures de traitement des renseignements personnels [Sélection (un choix ou plus) : au niveau de l'organisation; au niveau des processus de la mission et des activités; au niveau du système] qui : (a) définissent les objectifs, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et les obligations en matière de conformité (b) sont conformes aux lois, à la jurisprudence, aux directives, à la réglementation, aux politiques, aux directives, aux normes et aux lignes directrices applicables

2. les procédures visant à faciliter la mise en oeuvre de la politique de protection de la vie privée et des procédures de traitement des renseignements personnels, ainsi que les contrôles de traitement des renseignements personnels et de transparence connexes

b. Déléguer la responsabilité à [Affectation : responsable désignée ou désigné par l'organisation] pour élaborer, documenter et communiquer la politique et les procédures de traitement de renseignements personnels et de transparence

c. Passer en revue et mettre à jour, par rapport au traitement des renseignements personnels et de la transparence :

1. la politique actuelle [Affectation : fréquence définie par l'organisation] et à la suite de [Affectation : événements définis par l'organisation]

2. les procédures de traitement des renseignements personnels, dont les exigences en matière de transparence, [Affectation : fréquence définie par l'organisation] et à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

Les politiques de protection de la vie privée et les procédures de traitement des renseignements personnels, dont les exigences en matière de transparence, portent sur les contrôles dans la famille PT qui sont mis en oeuvre dans les systèmes ou qui sont propres aux activités des programmes et à l'organisation. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à l'élaboration des politiques qui visent à documenter le traitement des renseignements personnels et les procédures, ou qui ont une incidence sur ces derniers. Il convient de mettre en place des politiques et des procédures de sécurité et de protection de la vie privée au niveau de l'organisation et de renforcer les procédures de traitement des renseignements personnels propres aux activités des programmes ou aux systèmes. La politique de protection de la vie privée peut être intégrée à la politique générale de sécurité et de protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies au niveau de l'organisation, pour les activités des programmes ou les processus opérationnels, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour des politiques de protection de la vie privée et des procédures de traitement des renseignements personnels et de transparence comprennent les constatations tirées d'évaluations ou de vérifications, les effractions ou les changements apportés aux lois, à la jurisprudence, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.

PT-02 — Pouvoir en matière de collecte et d'utilisation de renseignements personnels (---)

Énoncés :

a. Déterminer et documenter [Affectation : autorité définie par l'organisation] qui permet [Affectation : collecte et utilisation définies par l'organisation] des renseignements personnels
b. Limiter [Affectation : collecte et utilisation définies par l'organisation] des renseignements personnels à ce qui est autorisé seulement

Responsable : Aucun

Discussion :

La collecte et l'utilisation des renseignements personnels sont une opération ou un ensemble d'opérations que le système d'information ou l'organisation effectue par rapport aux renseignements personnels tout au long du cycle de vie de l'information. Le traitement comprend, sans s'y limiter, la création, la collecte, l'utilisation, la correction, la modification, la conservation, la divulgation et l'élimination. Le traitement des opérations peut également comprendre l'accès, la journalisation, la création ou la génération, la transformation, ainsi que des techniques statistiques et d'analyse, comme l'exploration de données et l'analytique de pointe. Les fournisseurs de services sont souvent tenus de traiter des renseignements personnels pour fournir le service. Les organisations prennent des mesures pour s'assurer que les renseignements personnels ne soient traités qu'à des fins autorisées, notamment la formation du personnel de l'organisation sur le traitement autorisé des renseignements personnels, de même que la surveillance et la vérification de l'utilisation que fait l'organisation des renseignements personnels.

PT-02(01) — Étiquetage des données (---)

Énoncés :

Joindre les étiquettes des données contenant [Affectation : traitement autorisé défini par l'organisation] aux [Affectation : éléments de renseignements personnels définis par l'organisation].

Responsable : Aucun

Discussion :

Les étiquettes de données soutiennent le suivi et l'application du traitement autorisé en précisant les types de traitement qui sont autorisés, ainsi que les éléments pertinents des renseignements personnels dans l'ensemble du système. Les étiquettes de données peuvent également soutenir l'utilisation d'outils automatisés.

PT-02(02) — Automatisation (---)

Énoncés :

Gérer l'application du traitement autorisé des renseignements personnels au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Les mécanismes automatisés favorisent la vérification et ne permettent que le traitement autorisé.

PT-03 — Traitement, utilisation et divulgation de renseignements personnels (---)

Énoncés :

a. Reconnaître et documenter les [Affectation : utilisations et divulgations définies par l'organisation] associées aux collectes de renseignements personnels
b. Décrire le ou les buts de la collecte dans les énoncés de confidentialité et les stratégies de l'activité du programme ou de l'organisation
c. Limiter les [Affectation : utilisations et divulgations définies par l'organisation] des renseignements personnels à ce qui est compatible avec les fins mentionnées ou autorisées dans la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels
d. Surveiller les changements apportés au traitement des renseignements personnels et mettre en place les [Affectation : mécanismes définis par l'organisation] pour s'assurer que tous les changements sont apportés conformément à [Affectation : exigences prévues par la loi identifiées] a
a. Mettre à jour le FRP

Responsable : Aucun

Discussion :

Déterminer et documenter l'objectif de la collecte permet aux organisations de comprendre comment les renseignements personnels seront traités. Par traitement, on entend tout processus qui touche les renseignements personnels dans le cycle de vie de l'information, comme la collecte, la création, la correction, la modification, l'utilisation, la conservation, la divulgation et l'élimination. Déterminer et documenter le principal objectif de la collecte, ainsi que l'usage compatible ou les autorisations ou les divulgations secondaires autorisées, permet aux gardiennes et gardiens de l'information, aux exploitantes et exploitants du système et aux personnes à qui appartiennent les renseignements traités par le système de comprendre comment les renseignements seront utilisés. Les personnes peuvent ainsi prendre des décisions éclairées sur leur engagement avec les systèmes d'information et les organisations et gérer leurs intérêts en matière de respect de la vie privée. Les organisations devraient prendre les mesures nécessaires pour s'assurer que les renseignements personnels sont utilisés ou divulgués aux fins prévues seulement. Le personnel de l'organisation devrait recevoir de la formation et le traitement des renseignements personnels dans l'organisation devrait faire l'objet d'une surveillance et de vérifications.

PT-03(01) — Étiquetage des données (---)

Énoncés :

Joindre les étiquettes des données contenant les objectifs des [Affectation : éléments définis par l'organisation] suivants : [Affectation : objectifs en matière de traitement définis par l'organisation].

Responsable : Aucun

Discussion :

Les étiquettes de données soutiennent le suivi des fins du traitement en précisant les objectifs du traitement, ainsi que les éléments pertinents des renseignements personnels dans l'ensemble du système. En précisant les fins du traitement dans les étiquettes des données et les renseignements personnels à mesure que les renseignements transitent à travers un système, une ou un propriétaire de système, une exploitante ou un exploitant peut déterminer si un changement apporté au traitement est compatible ou non avec les fins établies et documentées. Les étiquettes de données peuvent également soutenir l'utilisation d'outils automatisés.

PT-03(02) — Automatisation (---)

Énoncés :

Assurer le suivi du traitement des renseignements personnels au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Les mécanismes automatisés renforcent le suivi des objectifs du traitement.

PT-04 — Consentement (---)

Énoncés :

a. S'assurer que le consentement est obtenu par écrit ou est adéquatement documenté, y compris l'information comme la date et l'heure de consentement
b. Dans le gouvernement général, mettre en place [Affectation : outils ou mécanismes désignés par l'organisation] afin que les individus puissent fournir un consentement éclairé pour les utilisations secondaires ou la collecte indirecte de leurs renseignements personnels Le consentement doit comprendre :

1. l'objectif du consentement
2. les éléments de renseignements personnels concernés
3. dans le cas d'une collecte indirecte, les sources qui seront exigées pour fournir l'information, ainsi que la raison pour laquelle il s'agit d'une collecte indirecte
4. les utilisations ou les divulgations qui ne respectent pas l'objectif initial de la collecte et pour lesquelles le consentement est demandé
5. toute conséquence qui pourrait résulter du refus d'accorder le consentement
6. toute alternative à l'accord du consentement

c. Dans le secteur privé, mettre en place [Affectation : outils ou mécanismes désignés par l'organisation] afin que les individus puissent fournir un consentement valable pour la collecte, l'utilisation et la divulgation de leurs renseignements personnels

Responsable : Aucun

Discussion :

Les organisations devraient également tenir compte des facteurs démographiques ou contextuels qui pourraient influencer la compréhension ou le comportement des individus en ce qui a trait à l'utilisation de leurs renseignements personnels par l'organisation. Lorsqu'elles demandent le consentement d'individus, les organisations devraient considérer d'avoir recours à des mécanismes appropriés pour obtenir leur consentement, notamment le type de consentement (par exemple, une option d'inclusion ou d'exclusion), la façon de les authentifier correctement et de garantir leur identité, et la façon d'obtenir leur consentement par des moyens électroniques. Le consentement devrait exiger une action positive au nom de l'individu et ne devrait pas être implicite. Par ailleurs, les organisations doivent considérer de mettre en place un mécanisme permettant aux individus de retirer leur consentement après l'avoir accordé, le cas échéant. Si le consentement est retiré, les individus pourraient avoir l'assurance que leurs renseignements personnels ont bien été supprimés de la base de données de collecte. Les organisations devraient tenir compte des facteurs en matière d'utilisabilité, comme rédiger dans un langage clair et éviter le jargon technique, pour aider les individus à comprendre les risques qu'ils acceptent lorsqu'ils donnent leur consentement. Les organismes du secteur privé doivent obtenir un consentement valable pour la collecte, l'utilisation et la divulgation de renseignements personnels. Le consentement est considéré comme étant valable si de l'information claire est fournie aux individus pour expliquer ce que l'organisation fera de leurs renseignements. Une organisation doit établir et documenter les fins pour lesquelles elle veut collecter les renseignements personnels au moment de la collecte ou par la suite. Il pourrait y avoir des exceptions où le consentement n'est pas requis.

PT-04(01) — Consentement adapté au gouvernement du Canada (---)

Énoncés :

Fournir les [Affectation : mécanismes désignés par l'organisation] pour permettre aux individus d'adapter les autorisations de traitement aux éléments sélectionnés des renseignements personnels.

Responsable : Aucun

PT-04(02) — Consentement opportun (---)

Énoncés :

Présenter les [Affectation : mécanismes de consentement désignés par l'organisation] aux individus [Affectation : fréquence définie par l'organisation] et parallèlement à [Affectation : traitement des renseignements personnels défini par l'organisation].

Responsable : Aucun

Discussion :

Un consentement opportun permet aux individus de comprendre comment leurs renseignements personnels seront traités au moment du traitement de types de données particuliers ou conjointement à un tel traitement dans la mesure où une telle participation peut être la plus utile pour l'individu. Les hypothèses individuelles concernant la façon dont les renseignements personnels sont traités pourraient ne pas être fondées ou crédibles s'il y a longtemps que l'individu a donné son consentement ou si le type de traitement pose un risque important d'atteinte à la vie privée. Les organisations devraient faire preuve de discrétion pour ce qui est de déterminer quand il convient de demander le consentement et elles peuvent utiliser des renseignements complémentaires sur la démographie, des groupes de discussion ou des sondages pour en savoir plus sur les intérêts et les préoccupations des individus en matière de respect de la vie privée.

PT-04(03) — Révocation (---)

Énoncés :

Mettre en place [Affectation : outils ou mécanismes désignés par l'organisation] afin que les individus puissent retirer leur consentement au traitement de leurs renseignements personnels.

Responsable : Aucun

Discussion :

La révocation du consentement permet aux individus d'exercer du contrôle sur leur décision d'accorder leur consentement initial lorsque les circonstances changent. Les organisations devraient considérer des facteurs en matière d'utilisabilité pour simplifier les fonctions de révocation.

PT-04(400) — Consentement adapté au secteur privé (---)

Énoncés :

Fournir les [Affectation : mécanismes désignés par l'organisation] pour permettre aux individus d'adapter les autorisations de traitement aux éléments sélectionnés des renseignements personnels.

Responsable : Aucun

Discussion :

Bien qu'il puisse être nécessaire de traiter certains renseignements personnels pour assurer les fonctionnalités de base du produit ou du service, d'autres types de traitement pourraient ne pas être nécessaires. Dans de tels cas, il convient de considérer un consentement sur mesure. Les organisations devraient informer les individus que leurs renseignements personnels seront visés par l'utilisation secondaire. Le consentement personnalisé permet aux individus de sélectionner comment les éléments des renseignements personnels seront traités. Un consentement plus adapté peut aider à réduire les risques d'atteinte à la vie privée, à accroître la satisfaction des personnes concernées et à éviter les comportements néfastes, comme l'abandon du produit ou du service.

PT-05 — Énoncé de confidentialité (---)

Énoncés :

Informer les individus de la collecte de leurs renseignements personnels, ce qui comprend :
a. l'autorisation légale de collecter les renseignements personnels
b. les conséquences juridiques et administratives de tout refus de fournir des renseignements personnels
c. le droit de protection des renseignements personnels et le droit d'y accéder et de faire des demandes de correction
d. un avertissement indiquant que l'utilisation du système peut être surveillée, enregistrée et sujette à une vérification et qu'elle inclut :
    1. un énoncé expliquant les pratiques de surveillance régulières des réseaux électroniques
    2. un énoncé expliquant que les réseaux électroniques seront surveillés à des fins professionnelles
    3. un énoncé indiquant qu'une surveillance spéciale peut être autorisée sans préavis si une utilisation illégale ou inacceptable est soupçonnée
e. une explication de la manière dont les renseignements seront utilisés
f. le droit de déposer une plainte auprès de la Commission d'accès à l'information du Québec (CAI) concernant le traitement par les institutions des renseignements personnels des individus
g. la référence au FRP pertinent, le cas échéant

Responsable : Aucun

PT-05(01) — Énoncés de confidentialité opportuns (---)

Énoncés :

Présenter l'énoncé du traitement des renseignements personnels aux individus lorsqu'ils fournissent leurs renseignements personnels.

Responsable : Aucun

PT-05(02) — Avis et énoncés de confidentialité (---)

Énoncés :

Inclure les avis et énoncés de confidentialité sur les formulaires servant à collecter l'information qui sera conservée dans un FRP.

Responsable : Aucun

PT-06 — Fichiers de renseignements personnels (---)

Énoncés :

Les activités du programme qui collectent des renseignements personnels doivent consigner et publier un FRP si de tels renseignements ont été utilisés, sont utilisés ou peuvent être utilisés à des fins administratives, ou si leur organisation ou leur récupération est effectuée en fonction du nom d'un individu ou au moyen d'un numéro d'identification, d'un symbole ou de tout autre élément particulier attribué à un individu. Les [Affectation : rôles ou personnel définis par l'organisation] sont responsables de ce qui suit :
a. enregistrer ou soumettre de nouveaux FRP ou des FRP considérablement modifiés
b. publier les FRP et mettre à jour l'information chaque année
c. faire en sorte que les FRP soient précis, à jour et pris en compte conformément à la politique

Responsable : Aucun

PT-06(01) — Usages et divulgations compatibles (---)

Énoncés :

Passer en revue tous les usages compatibles publiés dans le FRP [Affectation : fréquence définie par l'organisation] pour assurer une exactitude continue et veiller à ce que les usages compatibles continuent de correspondre aux fins pour lesquelles l'information a été collectée.

Responsable : Aucun

PT-06(02) — Fichiers inconsultables (---)

Énoncés :

Passer en revue tous les FRP qui ont été désignés comme étant des fichiers consultables [Affectation : fréquence définie par l'organisation] pour s'assurer qu'ils sont toujours appropriés et nécessaires en vertu de la loi.

Responsable : Aucun

PT-07 — Renseignements personnels particulièrement sensibles (---)

Énoncés :

Appliquer [Affectation : conditions de traitement définies par l'organisation] aux renseignements personnels particulièrement sensibles.

Responsable : Aucun

Discussion :

Les organisations devraient mettre en œuvre toutes les conditions ou protections qui pourraient être nécessaires pour des renseignements personnels particulièrement sensibles. Ces conditions pourraient être exigées par les lois, les décrets, les directives, la réglementation, les politiques, les normes ou les lignes directrices applicables. Les exigences peuvent également découler des résultats des évaluations des risques d'atteinte à la vie privée qui tiennent compte des changements contextuels susceptibles de faire en sorte que l'organisation détermine qu'une catégorie particulière de renseignements personnels est particulièrement sensible ou soulève des risques particuliers d'atteinte à la vie privée. Les organisations devraient consulter la ou le haut fonctionnaire ou cadre supérieur désigné et la conseillère ou le conseiller juridique en matière de protection de la vie privée concernant les protections qui pourraient être nécessaires.

PT-07(01) — Numéros d’assurance sociale (---)

Énoncés :

Si un programme ou une activité collecte, utilise ou divulgue des numéros d’assurance sociale (NAS) :
a. s’assurer d’avoir l’autorisation expresse de collecter et d’utiliser le NAS
b. fournir un énoncé au point de collecte concernant l’autorisation de collecter ainsi que l’utilisation ou la divulgation anticipée du NAS
c. s’assurer que la collecte et l’utilisation du NAS sont comprises dans le FRP connexe, le cas échéant

Responsable : Aucun

PT-07(02) — Charte canadienne des droits et libertés (---)

Énoncés :

Limiter le traitement de l'information décrivant la façon dont un individu exerce ses droits garantis par la Charte des droits et libertés de la personne à moins qu'il n'existe une autorité légitime ou qu'un traitement soit effectué dans le cadre d'une activité autorisée d'application de la loi.

Responsable : Aucun

PT-07(400) — Secteur privé (---)

Énoncés :

Au moment de collecter, d'utiliser ou de divulguer des renseignements personnels particulièrement sensibles, les organisations du secteur privé devraient :
a. déterminer la forme de consentement à utiliser selon la sensibilité de l'information
b. protéger les renseignements personnels avec les [Affectation : outils ou mécanismes désignés par l'organisation] appropriés à la sensibilité de l'information

Responsable : Aucun

Discussion :

En vertu de la Loi sur la protection des renseignements personnels dans le secteur privé, tout renseignement personnel peut être sensible selon le contexte. Cela dit, certains types de renseignements personnels seront généralement considérés comme étant de nature sensible en raison des risques liés aux individus associés à la collecte, à l'utilisation ou à la divulgation de ces catégories de renseignements. Parmi les renseignements qui sont généralement considérés comme étant sensibles et exigeant un degré plus élevé de protection, on retrouve les données médicales et financières, l'origine ethnique et raciale, les opinions politiques, les données génétiques et biométriques, l'information relative à la vie sexuelle ou à l'orientation sexuelle des individus, ainsi que les croyances religieuses ou philosophiques. Les faits en cause dans chaque situation dicteront si les renseignements personnels sont considérés comme étant de nature sensible en vertu de la Loi sur la protection des renseignements personnels dans le secteur privé. Le contexte est important pour ce qui est de déterminer si les renseignements personnels doivent être considérés comme étant de nature sensible.

PT-08 — Exigences de couplage de données (---)

Énoncés :

Lorsqu'une activité d'un programme vise à collecter, à utiliser ou à divulguer des renseignements personnels afin de mener une activité de couplage de données :
a. s'assurer que les autorisations nécessaires sont en place pour collecter, utiliser ou divulguer les renseignements personnels aux fins de couplage des données
b. élaborer et établir une entente ou un accord d'échange de renseignements aux fins de couplage des données
c. vérifier que [Sélection (un choix) : l'avis envoyé à l'individu; le consentement obtenu de l'individu] indique que les renseignements seront utilisés dans le cadre d'activités de couplage des données
d. vérifier que le FRP connexe indique que les renseignements seront utilisés dans le cadre d'activités de couplage des données

Responsable : Aucun

RA

Évaluation des risques

Risk Assessment

RA-01 — Politique et procédures d'évaluation des risques (---)

Énoncés :

a. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :
- **1.** une politique d'évaluation des risques [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables
- **2.** des procédures pour faciliter la mise en oeuvre de la politique d'évaluation des risques et des contrôles d'évaluation des risques connexes

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à l'évaluation des risques

c. Passer en revue et mettre à jour, par rapport à l'évaluation des risques :
- **1.** la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]
- **2.** les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La politique et les procédures d'évaluation des risques abordent les contrôles de la famille RA qui ont été mis en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à l'élaboration de la politique et des procédures d'évaluation des risques. Les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin de politiques et des procédures propres à la mission ou au système. La politique peut être intégrée à la politique générale sur la sécurité et la protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures d'évaluation des risques comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.

RA-01(400) — Évaluations des facteurs relatifs à la vie privée (---)

Énoncés :

Développer un processus d'évaluation des facteurs relatifs à la vie privée (EFVP) avec procédures connexes, qui :
a. est établi par les responsables des institutions gouvernementales
b. tient compte de la responsabilité de l'institution en ce qui a trait à l'établissement des fichiers de renseignements personnels (FRP)
c. est proportionnel à la gravité des préjudices potentiels associés au niveau de risque d'entrave à la vie privée lié aux programmes et aux activités de l'institution
d. s'assure que l'EFVP est effectuée par la ou le haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée qui est responsable des programmes ou des activités qui sont ajoutés ou considérablement modifiés au sein de l'institution

Responsable : Aucun

RA-02 — Catégorisation de la sécurité (---)

Énoncés :

a. Catégoriser le système et l'information qu'il traite, stocke et transmet
b. Documenter les résultats de la catégorisation de la sécurité, y compris les justifications, dans le plan de sécurité du système
c. S'assurer que l'autorité responsable ou sa représentante ou son représentant désigné examine et approuve la décision relative à la catégorisation de la sécurité

Responsable : Aucun

Discussion :

Les catégories de sécurité décrivent les incidences négatives ou les conséquences négatives potentielles sur les activités et les biens organisationnels, de même que sur les individus dans les cas où l'information organisationnelle ou les systèmes sont compromis à la suite d'une entorse à la confidentialité, à l'intégrité ou à la disponibilité. La catégorisation de la sécurité est aussi un type de caractérisation associé à la perte de biens dans les processus d'ingénierie de la sécurité des systèmes mis en oeuvre tout au long du cycle de développement des systèmes. Les organisations peuvent avoir recours à des évaluations des risques d'atteinte à la vie privée ou à des EFVP pour mieux comprendre les effets néfastes possibles sur les individus. Les processus de catégorisation de la sécurité permettent de réaliser les inventaires des ressources informationnelles et, de concert avec le contrôle CM-08, facilitent le mappage à certains composants des systèmes où l'information est traitée, stockée ou transmise. Le processus de catégorisation de la sécurité est revu tout au long du cycle de développement des systèmes pour s'assurer que les catégories de sécurité demeurent précises et pertinentes.

RA-02(01) — Hiérarchisation des répercussions (---)

Énoncés :

Procéder à la hiérarchisation des répercussions liées aux systèmes de l'organisation pour obtenir une plus grande granularité des niveaux d'incidence sur les systèmes.

Responsable : Aucun

Discussion :

Les organisations devraient attribuer les valeurs déterminées les plus élevées pour chaque système catégorisé de manière à attribuer une incidence très faible, faible, moyenne, élevée ou très élevé aux systèmes. La hiérarchisation des répercussions du système permet aux organisations de concentrer leurs efforts sur la sélection des contrôles de sécurité et la personnalisation des bases de référence des contrôles lorsqu'elles répondent aux risques identifiés.

RA-03 — Évaluation des risques (---)

Énoncés :

a. Mener une évaluation des risques, y compris :
- **1.** identifier les menaces et les vulnérabilités dans le système
- **2.** déterminer la probabilité et l'ampleur estimée des préjudices qui pourraient être associés à l'utilisation, à la divulgation, à l'interruption, à la modification et à l'accès non autorisés ou encore à la destruction du système, de l'information qu'il traite, stocke ou transmet, ou toute information connexe
- **3.** déterminer la probabilité et l'incidence de répercussions négatives sur les individus qui peuvent découler du traitement des renseignements personnels

b. Intégrer les résultats de l'évaluation des risques et les décisions liées à la gestion des risques du point de vue de l'organisation et du processus lié à la mission et aux activités aux évaluations des risques au niveau du système
c. Documenter les résultats de l'évaluation des risques dans [Sélection (un choix) : des plans de sécurité et de protection de la vie privée; un rapport d'évaluation des risques; {Affectation : document défini par l'organisation}]
d. Examiner les résultats de l'évaluation des risques [Affectation : fréquence définie par l'organisation]
e. Communiquer les résultats de l'évaluation des risques aux [Affectation : personnel ou rôles définis par l'organisation]
f. Mettre à jour l'évaluation des risques [Affectation : fréquence définie par l'organisation] ou chaque fois que des changements importants sont apportés au système ou à l'environnement d'exploitation, ou encore lorsque d'autres conditions sont susceptibles d'influer sur l'état de sécurité et de protection de la vie privée du système

Responsable : Aucun

Discussion :

Les évaluations des risques devraient prendre en compte les menaces, les vulnérabilités, les probabilités et les répercussions sur les activités et les biens organisationnels, les individus, d'autres organisations et le gouvernement. Les évaluations des risques devraient également considérer les risques provenant des parties externes, ce qui comprend les entrepreneures et entrepreneurs exploitant les systèmes au nom de l'organisation, les personnes accédant aux systèmes de l'organisation, les fournisseurs de services et les sous-traitantes et sous-traitants. Les organisations peuvent effectuer des évaluations des risques à chacun des trois niveaux hiérarchiques de la gestion des risques (c'est-à-dire le niveau organisationnel, le niveau du processus lié à la mission et aux activités ou le niveau du système d'information) ainsi qu'à chacune des phases du cycle de développement des systèmes. Les évaluations peuvent également être effectuées à divers stades du processus de gestion des risques, ce qui comprend la préparation, la catégorisation, la sélection, la répartition, la mise en oeuvre, l'évaluation, l'autorisation et la surveillance des contrôles. L'évaluation des risques est une activité continue réalisée tout au long du cycle de développement des systèmes. Elle peut également aborder l'information liée au système, y compris la conception du système, l'utilisation prévue du système, les résultats des tests et les artéfacts ou l'information liée à la chaîne d'approvisionnement. Les évaluations des risques peuvent jouer un rôle important dans les processus de sélection des contrôles, particulièrement pendant la mise en application des directives de personnalisation et les premières phases de la détermination des capacités.

RA-03(01) — Évaluation des risques liés à la chaîne d'approvisionnement (---)

Énoncés :

a. Évaluer les risques liés à la chaîne d'approvisionnement associés à [Affectation : systèmes, composants de systèmes et services qui s'y rapportent désignés par l'organisation]
b. Mettre à jour l'évaluation des risques liés à la chaîne d'approvisionnement [Affectation : fréquence définie par l'organisation], lorsque des changements importants sont apportés à la chaîne d'approvisionnement pertinente ou lorsque des changements sont apportés au système ou aux environnements d'exploitation ou d'autres conditions nécessitent qu'un changement soit apporté à la chaîne d'approvisionnement

Responsable : Aucun

Discussion :

Les événements liés à la chaîne d'approvisionnement comprennent les pannes, l'utilisation de composants défectueux, l'insertion de contrefaçons, le vol, des pratiques de développement malveillantes, des pratiques d'exécution inappropriées et l'insertion de code malveillant. Ces événements peuvent avoir une incidence considérable sur la confidentialité, l'intégrité et la disponibilité d'un système et de son information et, par conséquent, avoir des conséquences néfastes sur les activités de l'organisation (y compris sa mission, ses fonctions, son image ou sa réputation), les biens organisationnels, les individus, les autres organisations et le gouvernement. Les événements liés à la chaîne d'approvisionnement peuvent être accidentels ou malveillants, et survenir à n'importe quelle étape du cycle de vie des systèmes. Une analyse des risques liés à la chaîne d'approvisionnement peut aider une organisation à identifier les systèmes ou les composants pour lesquels il est nécessaire de prendre de plus amples mesures d'atténuation de tels risques.

RA-03(02) — Utilisation du renseignement de toutes sources (---)

Énoncés :

Utiliser du renseignement de toutes sources pour faciliter l'analyse du risque.

Responsable : Aucun

Discussion :

Les organisations devraient utiliser du renseignement de toutes sources pour prendre des décisions éclairées en matière d'ingénierie, d'acquisition et de gestion des risques. Le renseignement de toutes sources consiste en de l'information dérivée de toutes les sources disponibles, y compris l'information accessible au public ou de source ouverte, ou toute autre source de renseignement organisationnel disponible. Le renseignement de toutes sources est utilisé pour analyser les risques de vulnérabilités (intentionnelles ou accidentelles) pouvant découler d'interventions humaines, de l'environnement ou de processus pendant les étapes du développement, de la fabrication ou de l'expédition. Ces analyses des risques visent les fournisseurs à divers niveaux de la chaîne d'approvisionnement. Menées en nombre suffisant, elles ont pour objet d'assurer une gestion adéquate des risques. Les organisations peuvent mettre en place des accords pour échanger le renseignement de toutes sources ou les décisions qui en découlent avec leurs homologues, le cas échéant.

RA-03(03) — Sensibilisation aux menaces dynamiques (---)

Énoncés :

Déterminer l'environnement de cybermenaces actuel sur une base régulière au moyen de [Affectation : moyens définis par l'organisation].

Responsable : Aucun

Discussion :

L'information de sensibilisation aux menaces qui est recueillie s'intègre aux activités de sécurité de l'information de l'organisation pour s'assurer que les procédures sont mises à jour en réponse à un environnement de menace en constante évolution. Par exemple, à des niveaux de menace plus élevés, les organisations peuvent modifier les seuils d'autorisation ou d'authentification nécessaires pour exécuter certaines opérations.

RA-03(04) — Cybernanalyse prédictive (---)

Énoncés :

Faire appel aux capacités d'automatisation et d'analyse avancées suivantes pour prédire et identifier les risques qui pèsent sur [Affectation : systèmes ou composants de systèmes désignés par l'organisation] : [Affectation : capacités d'automatisation et d'analyse avancées définies par l'organisation].

Responsable : Aucun

Discussion :

Un COS doté des ressources appropriées ou une équipe d'intervention en cas d'incidents informatiques (CIRT pour Computer Incident Response Team) pourrait être dépassé par le volume d'information généré par la prolifération des outils et des appliances de sécurité, à moins qu'il n'ait recours à l'automatisation et à l'analyse évoluées pour analyser les données. Les capacités d'automatisation et d'analyse évoluées sont généralement prises en charge par les concepts d'intelligence artificielle (IA), dont l'apprentissage automatique (AA). Les exemples comprennent la découverte de menaces et l'intervention automatisées (ce qui inclut les capacités de collecte à grande échelle, d'analyse basée sur le contexte et d'intervention adaptative), les opérations de flux de travail automatisées et les outils de prise de décision assistée par ordinateur. Il convient de remarquer que les adversaires dotés de moyens sophistiqués pourraient être en mesure d'extraire l'information relative aux paramètres d'analyse et d'entraîner l'AA de nouveau pour classifier une activité malveillante comme étant anodine. Par conséquent, l'AA devrait faire l'objet d'une surveillance humaine pour veiller à ce que ces adversaires dotés de moyens sophistiqués ne puissent pas camoufler leurs activités.

RA-04 — Mise à jour de l’évaluation des risques (---)

Énoncés :

Annulé : Intégré au contrôle RA-03.

Responsable : Aucun

RA-05 — Surveillance et analyse des vulnérabilités (Nc--)

Énoncés :

a. Surveiller et analyser les vulnérabilités dans le système et les applications hébergées [Affectation : fréquence définie par l'organisation ou de manière aléatoire conformément au processus défini par l'organisation] et lorsque de nouvelles vulnérabilités susceptibles d'influer sur le système sont identifiées et signalées
b. Utiliser des outils et des techniques de surveillance des vulnérabilités qui facilitent l'interopérabilité et automatisent les composantes du processus de gestion des vulnérabilités en appliquant des normes sur :
- **1.** les relevés des plateformes, des lacunes logicielles et des configurations inappropriées
- **2.** le formatage des listes de vérification et des procédures de test
- **3.** la mesure de l'incidence des vulnérabilités

c. Analyser les rapports d'analyse des vulnérabilités et les résultats de la surveillance des vulnérabilités
d. Corriger les vulnérabilités légitimes [Affectation : temps de réponse défini par l'organisation] conformément à l'évaluation des risques de l'organisation
e. Communiquer l'information découlant du processus de surveillance des vulnérabilités et des évaluations des contrôles à [Affectation : personnel ou rôles définis par l'organisation] pour faciliter l'élimination de vulnérabilités semblables dans les autres systèmes
f. Employer des outils de surveillance des vulnérabilités qui sont dotés de la capacité de mettre à jour rapidement les vulnérabilités à analyser

Responsable : Aucun

Discussion :

La catégorisation de la sécurité de l'information et des systèmes aide à définir la fréquence et le niveau d'exhaustivité de la surveillance des vulnérabilités (y compris des analyses). Les organisations devraient déterminer la surveillance des vulnérabilités requise pour les composants des systèmes et s'assurer que les sources potentielles de vulnérabilités, comme les composants des infrastructures (par exemple, les commutateurs, les routeurs, les mécanismes de protection, les capteurs), les imprimantes, les numériseurs et les photocopieurs en réseau, ne sont pas ignorées. La capacité permettant d'actualiser aisément les outils de surveillance des vulnérabilités à mesure que de nouvelles vulnérabilités sont découvertes, annoncées, et que de nouvelles méthodes d'analyse sont établies, aide à s'assurer que les nouvelles vulnérabilités sont prises en compte par les outils de surveillance des vulnérabilités employés. Le processus de mise à jour de la surveillance des vulnérabilités permet d'identifier les éventuelles vulnérabilités auxquelles s'exposent les systèmes et d'intervenir dans les plus brefs délais. Les analyses et la surveillance des vulnérabilités visant les logiciels sur mesure pourraient nécessiter des mesures additionnelles, comme des analyses statiques, des analyses dynamiques, des analyses binaires ou encore des analyses recourant à une combinaison de ces trois approches. Les organisations peuvent utiliser ces analyses dans les examens de code source et dans divers outils, notamment dans les outils d'analyse statique, les analyseurs d'application Web et des analyseurs binaires. La surveillance des vulnérabilités comprend l'analyse des niveaux de correctifs; l'analyse des fonctions, des ports, des protocoles et des services qui ne doivent pas être accessibles aux utilisatrices et utilisateurs ou aux dispositifs; et l'analyse des mécanismes de contrôle de flux qui sont mal configurés ou défectueux. Cette surveillance peut également comprendre les outils de surveillance continue des vulnérabilités qui se servent de l'instrumentation pour analyser sans cesse les composants. Les outils axés sur l'instrumentation peuvent améliorer la précision et fonctionner dans l'ensemble de l'organisation sans avoir recours à l'analyse. Parmi les outils de surveillance des vulnérabilités qui facilitent l'interopérabilité, on retrouve ceux qui sont validés par le protocole SCAP (Security Content Automated Protocol). Ainsi, les organisations devraient considérer l'utilisation d'outils d'analyse qui expriment les vulnérabilités selon la convention d'appellation des vulnérabilités et expositions courantes (CVE pour Common Vulnerabilities and Exposures) et qui emploient l'analyse OVAL (Open Vulnerability Assessment Language) pour déceler la présence de vulnérabilités. Les sources d'information sur les vulnérabilités comprennent la liste des lacunes courantes (CWE pour Common Weakness Enumeration) et la base de données nationale sur les vulnérabilités (NVD pour National Vulnerability Database). Des évaluations des contrôles, comme les exercices effectués par l'équipe de testeuses et testeurs, donnent des sources additionnelles de vulnérabilités possibles à analyser. Les organisations devraient aussi envisager le recours à des outils d'analyse qui expriment l'incidence des vulnérabilités par l'entremise du système de notation des vulnérabilités courantes (CVSS pour Common Vulnerability Scoring System). La surveillance des vulnérabilités comprend un canal et un processus permettant d'obtenir des rapports des vulnérabilités informatiques provenant du grand public. Les programmes de divulgation des vulnérabilités peuvent être aussi simples que la publication d'une adresse courriel surveillée. Il pourrait aussi s'agir d'un formulaire Web permettant de recevoir des rapports, dont des notifications qui autorisent une recherche ou une divulgation de vulnérabilités informatiques faite de bonne foi. Les organisations s'attendent en général à ce qu'une telle recherche se fasse avec ou sans leur autorisation et qu'elles soient en mesure de se servir des canaux de divulgation des vulnérabilités pour accroître la probabilité que les vulnérabilités relevées soient signalées directement à l'organisation concernée pour lui permettre de les corriger. Les organisations peuvent également avoir recours à des incitatifs financiers (aussi appelés primes de bogues) pour inciter davantage les chercheuses et chercheurs en sécurité à signaler les vulnérabilités relevées. Des programmes de prime de bogues peuvent être adaptés en fonction des besoins de l'organisation. Les primes peuvent être en vigueur indéfiniment ou pour une période déterminée, et elles peuvent être offertes au grand public ou à un groupe prédéterminé. Les organisations peuvent exécuter des

programmes de prime de bogues privés ou ouverts au public simultanément et pourraient choisir d'offrir un accès avec justificatifs d'identité à des participantes et participants afin d'évaluer les vulnérabilités informatiques de points de vue privilégiés.

RA-05(01) — Mise à jour de la capacité des outils (---)

Énoncés :

Annulé : Intégré au contrôle RA-05.

Responsable : Aucun

RA-05(02) — Mise à jour de la liste de vulnérabilités à analyser (---)

Énoncés :

Mettre à jour le registre des vulnérabilités des systèmes [Sélection (un choix ou plus) : {Affectation : fréquence définie par l'organisation}; avant une nouvelle analyse; lorsque de nouvelles vulnérabilités sont identifiées et signalées].

Responsable : Aucun

Discussion :

En raison de la complexité des logiciels, des systèmes et d'autres facteurs modernes, de nouvelles vulnérabilités sont régulièrement découvertes. Il est important d'ajouter les vulnérabilités nouvellement découvertes à la liste des vulnérabilités à analyser pour s'assurer que l'organisation peut prendre les mesures nécessaires pour les atténuer en temps opportun.

RA-05(03) — Étendue et profondeur de la couverture (---)

Énoncés :

Définir l'étendue et la profondeur de la couverture de l'analyse des vulnérabilités.

Responsable : Aucun

Discussion :

L'étendue de la couverture de l'analyse des vulnérabilités peut être exprimée sous forme de pourcentage des composants dans le système, selon les types particuliers de systèmes, selon la criticité des systèmes ou selon le nombre de vulnérabilités à vérifier. Inversement, la profondeur de la couverture de l'analyse des vulnérabilités peut être exprimée comme le niveau de conception du système que l'organisation entend surveiller (par exemple, un composant, un module, un sous-système ou un élément). Les organisations peuvent déterminer que la couverture de l'analyse des vulnérabilités est suffisante pour satisfaire sa tolérance aux risques et d'autres facteurs. Les outils d'analyse et la façon dont ils sont configurés peuvent avoir une incidence sur la profondeur et la couverture. Plusieurs outils d'analyse pourraient être nécessaires pour offrir la profondeur et la couverture voulues.

RA-05(04) — Information découvrable (---)

Énoncés :

Déterminer l'information relative au système qui est découvrable et prendre [Affectation : mesures correctives définies par l'organisation].

Responsable : Aucun

Discussion :

L'information découvrable comprend notamment celle que les adversaires pourraient obtenir sans compromettre le système ou s'y introduire – par exemple, en collectant de l'information exposée par le système ou en menant des recherches extensives sur le Web. Les mesures correctives peuvent comprendre, par exemple, la notification du personnel approprié dans l'organisation, le retrait de certaines informations ou l'introduction de modifications du système visant à rendre l'information en question moins pertinente ou attrayante pour les adversaires. Cette amélioration ne tient pas compte de l'information intentionnellement découvrable qui peut faire partie d'une fonction de leurre (par exemple des pièges à pirates, des réseaux leurres ou des réseaux de déception) déployée par l'organisation.

RA-05(05) — Accès privilégiés (---)

Énoncés :

Mettre en œuvre l'autorisation des accès privilégiés aux [Affectation : composants de systèmes désignés par l'organisation] pour [Affectation : activités d'analyse des vulnérabilités définies par l'organisation].

Responsable : Aucun

Discussion :

Dans certains cas, les analyses des vulnérabilités pourraient s'avérer plus intrusives ou les systèmes faisant l'objet d'une analyse pourraient contenir de l'information protégée, dont des renseignements personnels. L'accès privilégié accordé à certains composants du système permet de procéder à une analyse plus approfondie des vulnérabilités et de protéger la nature sensible d'une telle analyse.

RA-05(06) — Automatisation des analyses de tendances (---)

Énoncés :

Comparer les résultats de multiples analyses des vulnérabilités au moyen de [Affectation : mécanismes automatisés désignés par l'organisation].

Responsable : Aucun

Discussion :

Utiliser des mécanismes automatisés pour analyser de multiples analyses des vulnérabilités au fil du temps peut aider à déterminer les tendances dans les vulnérabilités du système et à relever les modèles d'attaque.

RA-05(07) — Automatisation de la détection et du signalement des composants non autorisés (---)

Énoncés :

Annulé : Intégré au contrôle CM-08.

Responsable : Aucun

RA-05(08) — Examiner les journaux de vérification historiques (---)

Énoncés :

Examiner les journaux de vérification historiques pour déterminer si une vulnérabilité identifiée dans [Affectation : système désigné par l'organisation] a été exploitée précédemment au cours de [Affectation : période définie par l'organisation].

Responsable : Aucun

Discussion :

Examiner les journaux de vérification historiques pour déterminer si une vulnérabilité détectée récemment dans un système qui a été précédemment exploitée par une ou un adversaire peut fournir de l'information importante pour les analyses criminalistiques. De telles analyses peuvent aider à établir, par exemple, l'ampleur d'une intrusion précédente, le savoir-faire employé durant l'attaque, l'information organisationnelle ayant été exfiltrée ou modifiée, les capacités liées à la mission et aux activités ayant été touchées et la durée de l'attaque.

RA-05(09) — Tests d’intrusion et analyses (---)

Énoncés :

Annulé : Intégré au contrôle CA-08.

Responsable : Aucun

RA-05(10) — Corrélation de l’information tirée des analyses (---)

Énoncés :

Établir une corrélation entre les résultats produits par les outils d’analyse des vulnérabilités dans le but de déceler la présence de vecteurs d’attaque visant plusieurs vulnérabilités ou se déplaçant sur plusieurs bonds.

Responsable : Aucun

Discussion :

Un vecteur d’attaque est une voie ou des moyens qui permettent à une ou un adversaire d’obtenir accès à un système pour injecter du code malveillant ou exfiltrer de l’information. Les organisations peuvent utiliser des arbres d’attaque pour illustrer comment les activités hostiles des adversaires interagissent et se regroupent pour produire des incidences ou des conséquences négatives pour les systèmes et les organisations. Lorsqu’elle est associée aux données corrélées des outils d’analyse des vulnérabilités, une telle information peut apporter plus de clarté sur les vecteurs d’attaque à vulnérabilité et à bonds multiples. La corrélation de l’information sur l’analyse des vulnérabilités est particulièrement importante lorsque les organisations passent des anciennes aux nouvelles technologies (par exemple, le passage des protocoles réseau IPv4 à IPv6). Au cours de telles transitions, certains composants de systèmes peuvent être mal gérés par mégarde et pourraient créer des occasions d’exploitation pour les adversaires.

RA-05(11) — Programme de divulgation publique (---)

Énoncés :

Mettre en place un canal de signalement public pour la soumission de rapports de vulnérabilités touchant les systèmes et les composants de systèmes de l'organisation.

Responsable : Aucun

Discussion :

Le canal de signalement devrait être découvrable par le public et contenir un langage clair autorisant une recherche et une divulgation de vulnérabilités faites de bonne foi à l'organisation. L'organisation ne devrait pas soumettre son autorisation à des conditions et exiger que l'entité à l'origine du signalement assure une non-divulgation indéfinie au public. Elle pourrait toutefois exiger le respect d'un délai particulier pour atténuer la vulnérabilité de façon appropriée.

RA-06 — Dépistage des contre-mesures de surveillance technique (---)

Énoncés :

Avoir recours à un dépistage des contre-mesures de surveillance technique aux [Affectation : lieux définis par l'organisation] [Sélection (un choix ou plus) : {Affectation : fréquence définie par l'organisation}; lorsque les événements suivants se produisent : {Affectation : événements ou indicateurs définis par l'organisation}].

Responsable : Aucun

Discussion :

Le dépistage des contre-mesures de surveillance technique est un service exécuté par du personnel qualifié dans le but de détecter la présence de dispositifs et de méthodes de surveillance technique et de relever les lacunes de sécurité technique qui pourraient servir à mener des tentatives de pénétration technique des installations en cause. Le dépistage des contre-mesures de surveillance technique permet également d'évaluer la posture de sécurité technique de l'organisation et des installations et d'inclure des examens visuels, électroniques et physiques internes et externes de ces installations. Les mesures de dépistage fournissent de l'information pouvant servir aux évaluations des risques et permettant de signaler les brèches susceptibles d'être exploitées par des adversaires.

RA-07 — Réponse aux risques (---)

Énoncés :

Répondre aux conclusions tirées des évaluations de la sécurité et de la protection de la vie privée, de la surveillance et des vérifications conformément à la tolérance aux risques de l'organisation.

Responsable : Aucun

Discussion :

Plusieurs options s'offrent aux organisations pour répondre aux risques, notamment atténuer le risque par la mise en œuvre de nouveaux contrôles ou renforcer les contrôles existants, accepter le risque avec une justification ou une explication adéquate, partager ou transférer le risque, ou éviter le risque. La tolérance aux risques de l'organisation a une incidence sur les décisions et les mesures appropriées de réponse aux risques. La réponse aux risques traite de la nécessité de déterminer une réaction appropriée aux risques avant de générer une entrée dans le plan d'action et d'établir les jalons. Par exemple, la réponse peut être l'acceptation du risque ou son rejet, ou il pourrait être possible d'atténuer le risque immédiatement pour que le recours à un plan d'action et à des jalons ne soit pas nécessaire. Toutefois, si la réponse aux risques est d'atténuer le risque, et que l'atténuation ne peut pas être effectuée immédiatement, un plan d'action et des jalons sont alors générés.

RA-08 — Évaluations des facteurs relatifs à la vie privée (---)

Énoncés :

Effectuer des EFVP pour les systèmes, les programmes et les autres activités au moment de :
a. concevoir, développer ou livrer des moyens de traiter les renseignements personnels
b. procéder à une nouvelle collecte des renseignements personnels a
a. apporter des modifications importantes aux systèmes, aux programmes ou aux activités lorsque des renseignements personnels sont traités

Responsable : Aucun

Discussion :

Pour gérer le risque lié à la sécurité, il convient d'effectuer une évaluation des préjudices. Plusieurs systèmes traiteront des renseignements personnels susceptibles de donner lieu à un préjudice advenant une atteinte à la vie privée (contrairement aux données financières ou à la propriété intellectuelle, par exemple). En plus du préjudice potentiel dont pourraient faire l'objet les individus concernés, il pourrait également y avoir des répercussions à considérer sur le plan juridique et réglementaire ou la situation pourrait porter atteinte à la réputation ou aux activités de l'organisation. Par conséquent, une évaluation des préjudices potentiels propres à la protection de la vie privée est nécessaire pour déterminer la catégorisation de la sécurité du système prévu. Une EFVP est une analyse qui démontre comment les renseignements personnels sont traités pour assurer que ce traitement est conforme aux exigences applicables en matière de protection de la vie privée et qu'il est possible de déterminer les préjudices possibles au respect de la vie privée qui sont associés à un système d'information ou à une activité. Une EFVP est à la fois une analyse et un document officiel qui donne en détail le processus et les résultats de l'analyse. Les organisations effectuent et élaborent une EFVP suffisamment claire et précise pour démontrer que l'organisation a pleinement pris en compte le respect de la vie privée et a incorporé les menaces liées à la vie privée dès les premières étapes de l'activité de l'organisation et tout au long du cycle de vie de l'information. Afin d'effectuer une EFVP significative, la ou le haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée peut collaborer étroitement avec les gestionnaires du programme, les gardiennes et gardiens de l'information, les praticiennes et praticiens de la gestion de l'information, les expertes et experts des TI, les architectes de la sécurité, les conseillères et conseillers juridiques, et autres membres du personnel de l'organisation. Une EFVP ne se veut pas une activité limitée dans le temps qui est réservée à un jalon ou à un stade particulier du cycle de vie des systèmes d'information ou des renseignements personnels. Elle est plutôt une analyse relative à la vie privée qui se poursuit tout au long du cycle de vie du système et des renseignements personnels. Par conséquent, une EFVP est un document qui doit constamment faire l'objet d'un examen et être mis à jour chaque fois que des changements sont apportés aux TI ou aux pratiques de l'organisation, ou que d'autres facteurs modifient les préjudices possibles au respect de la vie privée qui sont associés à l'emploi de ces technologies. Après avoir effectué l'EFVP, les organisations peuvent se servir de cette information pour communiquer les évaluations des risques relatifs à la sécurité et à la protection de la vie privée. Les organisations peuvent également avoir recours à d'autres processus connexes pouvant porter des noms différents, notamment les évaluations de l'incidence algorithmique. Une EFVP peut aussi informer le public de la posture de l'organisation sur le plan de la protection de la vie privée.

RA-09 — Analyse de criticité (---)

Énoncés :

Déterminer les composants et les fonctions des systèmes en procédant à une analyse de criticité de [Affectation : systèmes, composants de systèmes ou services qui s'y rapportent désignés par l'organisation] à [Affectation : points de décision du cycle de développement des systèmes définis par l'organisation].

Responsable : Aucun

Discussion :

Ce ne sont pas tous les composants des systèmes, les services ou toutes les fonctions qui ont besoin de protections importantes. Par exemple, l'analyse de criticité est un principe clé en gestion des chaînes d'approvisionnement, puisqu'elle permet d'optimiser la hiérarchisation des activités de protection. L'identification de fonctions et de composants des systèmes essentiels tient compte des lois, des décrets, de la réglementation, des directives, des politiques, des normes, des exigences de fonctionnalité du système, des interfaces des systèmes et des composants, et des dépendances des systèmes et des composants applicables. Les ingénieures et ingénieurs des systèmes procèdent à une décomposition fonctionnelle d'un système dans le but d'identifier les fonctions et les composants essentiels à la mission. La décomposition fonctionnelle comprend l'identification des missions organisationnelles qui jouissent du soutien des systèmes, la décomposition en fonctions précises permettant l'exercice des missions, ainsi que la traçabilité vers les composants matériels, logiciels et micrologiciels qui sert à mettre les fonctions en œuvre, et ce, même lorsque ces fonctions sont partagées parmi de multiples composants pouvant se trouver à l'extérieur comme à l'intérieur du système. L'environnement opérationnel d'un système ou d'un composant sur système peut avoir une incidence sur la criticité, y compris les dépendances ou les connexions aux systèmes cyberphysiques, aux dispositifs, au système de systèmes, et aux services de TI externalisés. Les composants de systèmes qui permettent un accès direct aux fonctions ou aux composants essentiels des systèmes sont considérés comme étant essentiels en raison de la vulnérabilité qu'ils engendrent. La criticité des composants et des fonctions est évaluée selon l'incidence de leurs défaillances sur les missions organisationnelles qui sont prises en charge par le système contenant les composants et les fonctions en question. Une analyse de criticité est effectuée lorsqu'une architecture ou une conception est en cours de développement, de modification ou de mise à niveau. Si une telle analyse est effectuée tôt dans le cycle de développement du système, les organisations peuvent être en mesure de modifier la conception du système pour réduire la nature critique de ces composants et de ces fonctions en ajoutant, notamment, de la redondance ou des chemins alternatifs dans la conception du système. L'analyse de criticité peut également avoir une influence sur les mesures de protection exigées par les entrepreneures et entrepreneurs chargés du développement. En plus de l'analyse de criticité des systèmes, des composants de systèmes et les services qui s'y rapportent, il est important de tenir compte de l'analyse de criticité de l'information. Une telle analyse est réalisée dans le cadre du processus de catégorisation de la sécurité du contrôle RA-02.

RA-10 — Chasse aux cybermenaces (---)

Énoncés :

a. Établir et maintenir une capacité de chasse aux cybermenaces de manière à :
- **1.** relever les indicateurs de compromission dans les systèmes organisationnels
- **2.** détecter, suivre et contrer les menaces qui visent les contrôles existants

b. Avoir recours à la capacité de chasse aux cybermenaces [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

La chasse aux cybermenaces est un moyen de cyberdéfense actif contrairement aux mesures de protection passives traditionnelles, comme les pare-feu, les systèmes de détection et de prévention des incidents, la mise en quarantaine du code malveillant dans des bacs à sable et les technologies et systèmes de GIES. La chasse aux cybermenaces porte sur la recherche proactive des systèmes, des réseaux et de l'infrastructure d'une organisation pour des menaces avancées. L'objectif consiste à suivre les cyberadversaires et à contrer leurs activités le plus tôt possible dans la séquence d'attaque afin d'accroître de façon mesurable la vitesse et l'exactitude des réponses de l'organisation. Les indicateurs de compromission comprennent le trafic réseau inhabituel, les changements inhabituels apportés aux fichiers et la présence de code malveillant. Les équipes de chasse aux cybermenaces tirent avantage du renseignement sur les menaces existant et peuvent en créer du nouveau, qu'elles échangent ensuite avec des organisations homologues, des organisations d'échange et d'analyse de l'information (ISAO pour Information Sharing and Analysis Organizations), des Centres d'échange et d'analyse de l'information (ISAC pour Information Sharing and Analysis Centers) et les ministères et organismes concernés du gouvernement.

SA

Acquisition sécurisée des systèmes/services

System and Services

SA-01 — Politique et procédures d'acquisition des systèmes et des services (---)

Énoncés :

a. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :

1. une politique d'acquisition des systèmes et des services [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables

2. des procédures pour faciliter la mise en oeuvre de la politique d'acquisition des systèmes et des services ainsi que des contrôles connexes

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures d'acquisition des systèmes et des services

c. Passer en revue et mettre à jour, par rapport à l'acquisition des systèmes et des services :

1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La politique et les procédures d'acquisition des systèmes et des services abordent les contrôles de la famille SA qui ont été mis en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à l'élaboration de la politique et des procédures d'acquisition des systèmes et des services. En règle générale, les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin pour des politiques et des procédures propres à la mission ou au système. La politique peut être intégrée à la politique générale de sécurité et de protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures d'acquisition des systèmes et des services comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.

SA-02 — Affectation des ressources (---)

Énoncés :

a. Déterminer les exigences de haut niveau en matière de sécurité et de protection de la vie privée de l'information pour le système ou les services connexes lors de la planification des processus liés à la mission et aux activités
b. Déterminer, documenter et affecter les ressources nécessaires pour protéger le système ou les services connexes dans le cadre du processus de planification des immobilisations et de contrôle des investissements
c. Établir un poste distinct pour la sécurité et la protection de la vie privée de l'information dans sa documentation de programmation et de budgétisation

Responsable : Aucun

Discussion :

L'attribution des ressources pour la sécurité et la protection de la vie privée de l'information comprend le financement pour l'acquisition et le maintien des systèmes et des services, et les risques liés à la chaîne d'approvisionnement tout au long du cycle de développement des systèmes.

SA-03 — Cycle de développement des systèmes (---)

Énoncés :

a. Acquérir, développer et gérer le système au moyen de [Affectation : cycle de développement des systèmes défini par l'organisation] qui comprend les facteurs à considérer en matière de sécurité et de protection de la vie privée de l'information
b. Définir et documenter les rôles et les responsabilités en matière de sécurité et de protection de la vie privée de l'information tout au long du cycle de développement des systèmes
c. Identifier les personnes qui assument des rôles et des responsabilités en matière de sécurité et de protection de la vie privée de l'information
d. Intégrer le processus de gestion des risques liés à la sécurité et à la protection de la vie privée de l'information de l'organisation dans les activités du cycle de développement des systèmes

Responsable : Aucun

Discussion :

Un processus de cycle de développement des systèmes constitue une condition essentielle à la réussite des étapes de développement, de mise en oeuvre et d'exploitation des systèmes. L'intégration précoce des facteurs à considérer en matière de sécurité et de protection de la vie privée dans le cadre du cycle de développement des systèmes est un principe fondamental de l'ingénierie de la sécurité et de la protection de la vie privée des systèmes. L'application des contrôles nécessaires pendant le cycle de développement des systèmes exige une compréhension élémentaire de la sécurité et de la protection de la vie privée de l'information, des menaces, des vulnérabilités, des effets négatifs et des risques auxquels s'exposent les missions et les activités prioritaires de l'organisation. Les principes d'ingénierie de la sécurité du contrôle SA-08 aident les personnes à concevoir, à coder et à tester adéquatement les systèmes et les services connexes. Les organisations comprennent le personnel qualifié (par exemple, une ou un cadre supérieur de la gouvernance en matière de sécurité du ministère, une ou un haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée, les architectes en sécurité et en protection de la vie privée, et les ingénieures et ingénieurs en sécurité et en protection de la vie privée) qui prend part aux processus du cycle de développement des systèmes et veille à que les exigences définies en matière de sécurité et de protection de la vie privée soient intégrées dans les systèmes de l'organisation. Les programmes de formation en sécurité et en protection de la vie privée basée sur les rôles peuvent permettre aux personnes qui assument des rôles clés en matière de sécurité et de protection de la vie privée d'acquérir l'expérience, les compétences et l'expertise nécessaires à la conduite des activités constitutives du cycle de développement des systèmes. La parfaite intégration des exigences de sécurité et de protection de la vie privée à l'architecture d'entreprise permet également d'assurer que les facteurs importants à considérer en matière de sécurité et de protection de la vie privée sont pris en compte tout au long du cycle de vie des systèmes et qu'ils sont directement liés aux processus liés à la mission et aux activités de l'organisation. Le processus facilite également l'intégration des architectures de sécurité et de protection de la vie privée de l'information à l'architecture d'entreprise, conformément aux stratégies de gestion des risques de l'organisation. Comme le cycle de développement des systèmes comprend plusieurs organisations (par exemple, des fournisseurs externes, des développeuses et développeurs, des intégratrices et intégrateurs, des fournisseurs de service), les fonctions et les contrôles de gestion des risques liés à la chaîne d'approvisionnement jouent des rôles importants dans la gestion efficace du système durant leur cycle de vie.

SA-03(01) — Gestion de l’environnement de préproduction (---)

Énoncés :

S’assurer que la protection des environnements de préproduction est proportionnelle au risque tout au long du cycle de développement du système, du composant de système ou du service qui s’y rapporte.

Responsable : Aucun

Discussion :

L’environnement de préproduction comprend les environnements de développement, de test et d’intégration. L’analyse de criticité et l’application de contrôles aux développeuses et développeurs permettent également d’offrir un environnement de développement de système plus sécurisé.

SA-03(02) — Utilisation de données opérationnelles et en temps réel (---)

Énoncés :

a. Approuver, documenter et contrôler l'utilisation de données en temps réel dans les environnements de préproduction pour le système, le composant de système ou le service qui s'y rapporte
b. Protéger les environnements de préproduction pour le système, le composant de système ou le service qui s'y rapporte de manière à avoir le même niveau d'incidence ou le même niveau de classification que toute donnée en cours d'utilisation en temps réel dans les environnements de préproduction

Responsable : Aucun

Discussion :

Les données en temps réel sont également appelées « données opérationnelles ». L'utilisation de données opérationnelles ou en temps réel dans les environnements de préproduction (c'est-à-dire, de développement, de test et d'intégration) peut poser des risques importants pour les organisations. De plus, l'utilisation de données en temps réel qui contiennent des renseignements personnels aux fins de test, de recherche et de formation augmente le risque de divulgation ou d'utilisation non autorisée de tels renseignements. Par conséquent, il est important pour l'organisation de gérer tout risque additionnel qui pourrait découler de l'utilisation de données opérationnelles ou en temps réel. Les organisations peuvent réduire les risques au minimum en utilisant de fausses données pendant les activités de conception, de développement et de test menées sur les systèmes, les composants de systèmes ou les services qui s'y rapportent. Les techniques d'évaluation des risques peuvent être utilisées pour déterminer si l'utilisation de données opérationnelles ou en temps réel pose un risque acceptable. L'utilisation de renseignements personnels aux fins de test exige que les individus soient informés à l'avance d'une telle utilisation.

SA-03(03) — Mise à jour technologique (---)

Énoncés :

Planifier et mettre en œuvre un calendrier de mise à jour technologique pour le système tout au long du cycle de développement du système.

Responsable : Aucun

Discussion :

La planification de la mise à jour technologique peut comprendre le matériel, les logiciels, les micrologiciels, les processus, les compétences du personnel, les fournisseurs, les fournisseurs de services et les installations. L'utilisation d'une technologie obsolète ou quasi obsolète peut augmenter les risques pour la sécurité et la protection de la vie privée associés aux composants non pris en charge, aux composants contrefaits ou recyclés, aux composants incapables de mettre en œuvre les exigences de sécurité et de protection de la vie privée, les composants lents ou non fonctionnels, les composants provenant de sources non fiables, les erreurs commises par le personnel par inadvertance ou une complexité accrue. Les mises à jour technologiques sont effectuées au cours de la phase d'exploitation et de maintenance du cycle de développement de systèmes.

SA-04 — Processus d'acquisition (---)

Énoncés :

Inclure, explicitement ou en référence, les exigences, les descriptions et les critères suivants en utilisant [Sélection (un choix ou plus) : langage contractuel normalisé; {Affectation : langage contractuel défini par l'organisation}] dans le contrat d'acquisition du système, des composants du système ou des services qui s'y rapportent :
a. exigences fonctionnelles de sécurité et de protection de la vie privée
b. exigences en matière de robustesse du mécanisme
c. exigences d'assurance de sécurité et de protection de la vie privée
d. contrôles nécessaires pour satisfaire les exigences de sécurité et de protection de la vie privée
e. exigences liées à la documentation sur la sécurité et la protection de la vie privée
f. exigences liées à la protection de la documentation sur la sécurité et la protection de la vie privée
g. description de l'environnement de développement du système et de l'environnement dans lequel on prévoit exploiter le système
h. affectation de responsabilités ou identification des parties responsables de la sécurité et la protection de la vie privée de l'information et de la gestion des risques liés à la chaîne d'approvisionnement
i. critères d'acceptation

Responsable : Aucun

Discussion :

Les exigences fonctionnelles de sécurité et de protection de la vie privée sont habituellement dérivées des exigences de haut niveau en matière de sécurité et de protection de la vie privée décrites au contrôle SA-02. Les exigences dérivées comprennent les capacités, les fonctions et les mécanismes de sécurité et de protection de la vie privée. Les exigences en matière de robustesse qui s'appliquent aux capacités, aux fonctions et aux mécanismes énoncent le degré d'exactitude, d'achèvement, de résistance au trafiquage ou aux contournements, et de résistance aux attaques directes. Les exigences en matière d'assurance peuvent être indiquées dans l'énoncé des travaux dans le cadre du processus de passation du marché et inclure les processus, les procédures et les méthodologies de développement, ainsi que les données des activités de développement et d'évaluation qui prouvent que la fonctionnalité requise a bien été mise en œuvre et que son mécanisme offre la robustesse nécessaire. La publication Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes (ITSP.10.037) du Centre pour la cybersécurité décrit le processus d'ingénierie des exigences dans le cadre du cycle de vie des systèmes. Les contrôles se veulent une description des mesures et des capacités de protection qu'il convient de mettre en œuvre pour atteindre les objectifs précis de l'organisation sur le plan de la sécurité et de la protection de la vie privée, et tenir compte des exigences en matière de sécurité et de protection de la vie privée des parties prenantes. Les contrôles sont sélectionnés et mis en œuvre de manière à satisfaire les exigences du système et à inclure les responsabilités de l'organisation et celles des développeuses et développeurs. Les contrôles peuvent comprendre les aspects techniques, administratifs, physiques et liés à la protection de la vie privée. Dans certains cas, la sélection et la mise en œuvre d'un contrôle peuvent nécessiter de la part de l'organisation des spécifications additionnelles sous la forme d'exigences dérivées ou de valeurs de paramètres de contrôle instanciés. Les exigences dérivées et les valeurs de paramètres de contrôle peuvent s'avérer nécessaires pour fournir le niveau approprié de détail de mise en œuvre des contrôles pendant le cycle de développement des systèmes. Les exigences liées à la documentation sur la sécurité et la protection de la vie privée portent sur toutes les phases du cycle de développement des systèmes. La documentation fournit aux utilisatrices, aux utilisateurs, aux administratrices et aux administrateurs des conseils sur la mise en œuvre et le fonctionnement des contrôles. Le degré de détail requis dans une telle documentation se fonde sur la catégorisation de la sécurité ou sur le niveau de classification du système, de même que sur l'ampleur de la dépendance à l'égard des capacités, des fonctions ou des mécanismes dont dépendent les organisations pour satisfaire les attentes en matière de réponse aux risques. Les exigences peuvent comprendre les paramètres de configuration imposés qui précisent les fonctions, les ports, les protocoles et les services qui sont autorisés. Les critères d'acceptation visant les systèmes, les composants de systèmes et les services qui s'y rapportent sont définis de la même façon que les critères visant toute acquisition ou tout approvisionnement organisationnels. Les organisations peuvent établir d'autres exigences qui soutiennent la sécurité et les activités afin de tenir compte de leurs responsabilités et de celles de la développeuse ou du développeur, ainsi que des exigences en matière de notification et d'échéanciers aux fins de soutien, de maintenance et de mise à jour.

SA-04(01) — Propriétés fonctionnelles des contrôles (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte donne une description des propriétés fonctionnelles des contrôles à mettre en œuvre.

Responsable : Aucun

Discussion :

Les propriétés fonctionnelles des contrôles de sécurité et de protection de la vie privée décrivent une fonctionnalité (par exemple, une capacité de sécurité et de protection de la vie privée, une fonction ou un mécanisme) qui est visible par l'intermédiaire de l'interface des contrôles. De plus, elles excluent les fonctionnalités et les structures de données qui sont au cœur du fonctionnement des contrôles.

SA-04(02) — Renseignements relatifs à la conception et à la mise en œuvre des contrôles (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte fournisse des renseignements sur la conception et la mise en œuvre des contrôles, ce qui comprend : [Sélection (un choix ou plus) : interfaces de systèmes externes servant à la sécurité; conception de haut niveau; conception de bas niveau; code source ou schémas des composants matériels; {Affectation : renseignements produits par l'organisme sur la conception et sur la mise en œuvre}] selon [Affectation : degré de détails défini par l'organisation].

Responsable : Aucun

Discussion :

Les organisations pourraient exiger un degré différent de détail dans la documentation relative à la conception et à la mise en œuvre des contrôles à employer dans les systèmes organisationnels, les composants de systèmes ou les services qui s'y rapportent en fonction des exigences de la mission ou des activités, des exigences en matière de résilience et de robustesse, et des exigences en matière d'analyse et de tests. Les systèmes peuvent être partitionnés en plusieurs sous-systèmes. Chacun de ces sous-systèmes peut également comprendre un ou plusieurs modules. La conception de haut niveau pour les systèmes se traduit par des sous-systèmes interreliés par des interfaces qui fournissent des fonctionnalités de sécurité. La conception de bas niveau du système donne lieu à des modules interreliés par des interfaces qui fournissent des fonctionnalités de sécurité. La documentation de conception et de mise en œuvre peut comprendre le fabricant, la version, le numéro de série, la signature hachée de vérification, les bibliothèques de logiciels utilisées, la date d'achat ou de téléchargement, ainsi que le fournisseur ou la source du téléchargement. Le code source et les schémas de composants matériels sont considérés comme des représentations de la mise en œuvre du système.

SA-04(03) — Méthodes, techniques et pratiques en matière de développement (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte démontre que le cycle de développement du système comprend :
a. [Affectation : méthodes d'ingénierie définies par l'organisation]
b. [Sélection (un choix ou plus) : {Affectation : méthodes d'ingénierie de la sécurité de système définies par l'organisation}; {Affectation : méthodes d'ingénierie de la protection de la vie privée définies par l'organisation}]
c. [Affectation : méthodes de développement logiciel définies par l'organisation; méthodes de test, d'évaluation, de vérification et de validation; et processus de contrôle de la qualité]

Responsable : Aucun

Discussion :

Le fait de suivre un cycle de développement de système qui comprend des méthodes de développement de logiciels conformes aux normes en vigueur, des méthodes d'ingénierie de système, des méthodes d'ingénierie de sécurité et de protection de la vie privée de système et des processus de contrôle de la qualité contribue à réduire le nombre et la sévérité des éventuelles erreurs pouvant survenir dans les systèmes, les composants de systèmes ou les services qui s'y rapportent. La réduction du nombre et de la sévérité de telles erreurs diminue également le nombre des vulnérabilités d'un système donné, de ses composants et de ses services. La transparence dans les méthodes et les techniques sélectionnées et mises en œuvre par les développeuses et développeurs pour l'ingénierie de systèmes, l'ingénierie de la sécurité et de la protection de la vie privée des systèmes, le développement logiciel, les évaluations des composants et des systèmes et les processus de contrôle de la qualité offre un niveau plus élevé d'assurance dans la fonctionnalité de sécurité du système, les composants du système ou les services du système que les organisations se procurent.

SA-04(04) — Attribution de composants à des systèmes (---)

Énoncés :

Annulé : Intégré au contrôle CM-08(09).

Responsable : Aucun

SA-04(05) — Configurations de systèmes, de composants et de services (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de :
a. produire un système, des composants ou des services dont les [Affectation : configurations de sécurité définies par l'organisation] sont mises en œuvre
b. utiliser les configurations comme valeurs par défaut pour tout système, composant ou service devant faire ultimement l'objet d'une réinstallation ou d'une mise à niveau

Responsable : Aucun

Discussion :

Les exemples de configurations de la sécurité comprennent le document Exigences de base en matière de sécurité pour les zones de sécurité de réseau (ITSP.80.022), les STIG, ainsi que les limitations liées aux fonctions, aux ports, aux protocoles et aux services. Les caractéristiques de sécurité peuvent comprendre l'exigence selon laquelle les mots de passe par défaut doivent avoir été changés.

SA-04(06) — Utilisation de produits de cybersécurité (---)

Énoncés :

a. Utiliser uniquement les produits gouvernementaux sur étagère (GOTS pour Government Off-the-Shelf) ou COTS de cybersécurité pour protéger l'information classifiée lorsque les réseaux servant à transmettre cette information ont un niveau de classification inférieur à celui de l'information transmise
b. Exiger que ces produits soient évalués ou validés

Responsable : Aucun

SA-04(07) — Profils de protection reconnus par le Programme canadien lié aux Critères communs (---)

Énoncés :

a. Limiter l'utilisation de produits commerciaux de cybersécurité et de produits informatiques sécurisés à ceux qui ont déjà été évalués selon un profil de protection reconnu par le Programme canadien lié aux Critères communs (PCCC) pour un type de technologie particulier, si un tel profil existe
b. S'il n'y a aucun profil de protection reconnu par le PCCC pour un type de technologie en particulier et qu'un produit de TI commercial a recours à une fonctionnalité cryptographique pour appliquer sa stratégie de sécurité, exiger que le module cryptographique soit validé selon la norme FIPS (Federal Information Processing Standard) ou reconnu par le PCCC

Responsable : Aucun

Discussion :

Le Centre pour la cybersécurité assure les activités du PCCC et certifie les produits. Prière de consulter le Portail des Critères communs (en anglais seulement) pour plus de renseignements sur les profils de protection. Prière de se reporter au Programme de validation des modules cryptographiques (PVMC) du Centre pour la cybersécurité pour plus de renseignements sur les modules cryptographiques homologués FIPS.

SA-04(08) — Plan de surveillance continue des contrôles (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte élabore un plan pour assurer une surveillance continue de l'efficacité des contrôles, conformément au programme de surveillance continue de l'organisation.

Responsable : Aucun

Discussion :

Les plans de surveillance continue visent à établir si les contrôles qui sont planifiés, exigés et déployés au sein du système, des composants du système ou des services qui s'y rapportent continuent d'être efficaces, en se fondant sur les changements inévitables appelés à survenir. Les plans de surveillance continue des développeuses et développeurs produisent un degré de détails tel que l'information fournie peut être intégrée aux programmes de surveillance continue mis en œuvre par les organisations. Les plans de surveillance continue peuvent inclure les types d'activités d'évaluation et de surveillance des contrôles prévus, la fréquence de la surveillance continue et les mesures à prendre advenant l'échec ou l'inefficacité des contrôles.

SA-04(09) — Fonctions, ports, protocoles et services utilisés (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte détermine les fonctions, les ports, les protocoles et les services qui seront utilisés dans l'organisation.

Responsable : Aucun

Discussion :

La détermination précoce des fonctions, des ports, des protocoles et des services (par exemple, pendant les phases initiales de définition des besoins et de conception) permet aux organisations d'influer sur la modélisation d'un système, de ses composants ou des services qui s'y rapportent. Cette intervention précoce dans le cycle de développement des systèmes permet aux organisations d'éviter ou de réduire au minimum l'utilisation des fonctions, des ports, des protocoles ou des services pouvant poser des risques tout aussi importants qu'inutiles, et de comprendre les avantages de bloquer l'accès à certains ports, protocoles ou services, ou de demander à des fournisseurs de services de systèmes de faire de même. Une détermination hâtive des fonctions, des ports, des protocoles et des services évite d'avoir à reconfigurer les contrôles après la mise en œuvre d'un système, de ses composants ou des services qui s'y rapportent. Le contrôle SA-09 décrit les exigences liées aux services de systèmes externes. Les organisations déterminent les fonctions, les ports, les protocoles et les services qui sont fournis depuis des sources externes.

SA-04(10) — Utilisation de produits de justificatifs d'identité numériques approuvés (---)

Énoncés :

Utiliser seulement les produits informatiques recommandés par le Centre pour la cybersécurité pour la capacité des justificatifs d'identité numériques mise en œuvre dans les systèmes de l'organisation.

Responsable : Aucun

Discussion :

Les produits doivent se conformer aux exigences relativement au niveau d'assurance et au niveau de robustesse de l'authentification des justificatifs d'identité numériques des employées, des employés, des entrepreneures et des entrepreneurs du gouvernement. Les systèmes et les organisations ont recours à des jetons d'authentification, comme les cartes à puce, pour l'AMF.

SA-04(11) — Système d'enregistrement (---)

Énoncés :

Inclure les [Affectation : exigences en matière de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels définies par l'organisation] dans le contrat d'acquisition relatif à l'exploitation d'un système d'enregistrement au nom d'une organisation afin d'assurer la mission ou les activités de cette dernière.

Responsable : Aucun

Discussion :

Lorsqu'une organisation assure l'exploitation d'un système d'enregistrement dans le cadre d'un contrat pour réaliser sa mission ou ses activités, elle doit appliquer les exigences imposées par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels aux systèmes d'enregistrement conformément à ses pouvoirs. À l'occasion, les entrepreneures et entrepreneurs représenteront le gouvernement et recueilleront les renseignements personnels associés aux programmes d'exploitation ou aux services. Les entrepreneures et entrepreneurs doivent faire preuve de transparence en indiquant qu'ils représentent le gouvernement et informer les individus de la façon dont leurs renseignements personnels pourraient être communiqués au gouvernement. Les obligations en matière de protection de la vie privée et de sécurité s'appliquent lorsque les entrepreneures et entrepreneurs représentent le gouvernement. Préciser dans le contrat d'acquisition les droits de garde des renseignements personnels advenant le cas où l'entrepreneure ou entrepreneur représenterait le gouvernement et collecterait les renseignements personnels d'individus.

SA-04(12) — Propriété des données (---)

Énoncés :

a. Inclure les exigences relatives à la propriété des données organisationnelles dans le contrat d'acquisition
b. Exiger que toutes les données soient supprimées du système de l'entrepreneure ou entrepreneur et retournées à l'organisation dans les [Affectation : délais définis par l'organisation]

Responsable : Aucun

Discussion :

Les entrepreneures et entrepreneurs qui exploitent un système contenant des données appartenant à une organisation doivent inclure dans le contrat les stratégies et les procédures en place pour supprimer les données de leurs systèmes et/ou retourner les données dans les délais stipulés dans le contrat.

SA-05 — Documentation relative aux systèmes (---)

Énoncés :

a. Obtenir ou élaborer la documentation à l'intention des administratrices et administrateurs d'un système, d'un composant du système ou du service qui s'y rapporte, qui décrit :

1. la configuration, l'installation et l'exploitation sécurisées du système, du composant ou du service

2. l'utilisation et la maintenance efficaces des fonctions et mécanismes de sécurité et de protection de la vie privée

3. les vulnérabilités connues associées à la configuration et à l'utilisation des fonctions administratives et privilégiées

b. Obtenir ou élaborer la documentation des utilisatrices et utilisateurs d'un système, d'un composant du système ou du service qui s'y rapporte, laquelle décrit :

1. les fonctions et mécanismes de sécurité et de protection de la vie privée accessibles aux utilisatrices et utilisateurs, et la façon d'utiliser efficacement ces fonctions et mécanismes

2. les méthodes d'interaction utilisateur qui permettent aux utilisatrices et utilisateurs d'utiliser le système, le composant ou le service de façon plus sécurisée et de protéger leur vie privée

3. les responsabilités des utilisatrices ou utilisateurs concernant le maintien de la sécurité du système, de ses composants ou des services qui s'y rapportent, et de la vie privée de ces personnes

c. Documenter les tentatives visant à obtenir des documents sur le système, ses composants ou les services qui s'y rapportent, qui n'existent pas ou qui ne sont pas disponibles, et réagir en [Affectation : mesures définies par l'organisation]

d. Distribuer la documentation à [Affectation : personnel ou rôles définis par l'organisation]

Responsable : Aucun

Discussion :

La documentation et les artéfacts créés par la développeuse ou le développeur aident le personnel à comprendre la mise en œuvre et le fonctionnement des contrôles. Les organisations envisagent d'établir des mesures particulières afin de définir le degré de qualité et d'achèvement du contenu fourni. La documentation relative aux systèmes peut être utilisée pour déterminer les rôles, les responsabilités et les attentes de la développeuse, du développeur et de l'organisation, et pour soutenir la gestion des risques liés à la chaîne d'approvisionnement, le processus d'intervention en cas d'incident et d'autres fonctions. Le personnel ou les rôles qui ont besoin de la documentation comprennent les propriétaires de systèmes, les responsables de la sécurité des systèmes et les administratrices et administrateurs de systèmes. Les tentatives d'obtenir la documentation consistent à communiquer avec les fabricants ou les fournisseurs, et à procéder à des recherches en ligne. L'incapacité d'obtenir la documentation peut survenir en raison de la désuétude d'un système ou d'un composant, ou d'un manque de soutien de la part des développeuses, des développeurs, des entrepreneures et des entrepreneurs. S'il est impossible d'obtenir la documentation, les organisations pourraient devoir recréer une partie de la documentation, si celle-ci s'avère nécessaire à la mise en œuvre ou au fonctionnement efficaces des contrôles. La protection s'appliquant à la documentation est proportionnelle à la catégorie de sécurité ou à la classification du système. La documentation portant sur les vulnérabilités des systèmes pourrait nécessiter un niveau de protection accru. L'exploitation sécurisée d'un système comprend le démarrage initial du système et la reprise sûre des opérations du système après une anomalie.

SA-05(01) — Propriétés fonctionnelles des contrôles de sécurité (---)

Énoncés :

Annulé : Intégré au contrôle SA-04(01).

Responsable : Aucun

SA-05(02) — Interfaces des systèmes externes servant à la sécurité (---)

Énoncés :

Annulé : Intégré au contrôle SA-04(02).

Responsable : Aucun

SA-05(03) — Conception de haut niveau (---)

Énoncés :

Annulé : Intégré au contrôle SA-04(02).

Responsable : Aucun

SA-05(04) — Conception de bas niveau (---)

Énoncés :

Annulé : Intégré au contrôle SA-04(02).

Responsable : Aucun

SA-05(05) — Code source (---)

Énoncés :

Annulé : Intégré au contrôle SA-04(02).

Responsable : Aucun

SA-06 — Restrictions relatives à l'utilisation des logiciels (---)

Énoncés :

Annulé : Intégré aux contrôles CM-10 et SI-07.

Responsable : Aucun

SA-07 — Logiciels installés par les utilisatrices et utilisateurs (---)

Énoncés :

Annulé : Intégré aux contrôles CM-11 et SI-07.

Responsable : Aucun

SA-08 — Principes d'ingénierie de la sécurité et de la protection de la vie privée (---)

Énoncés :

Appliquer les principes d'ingénierie de la sécurité et de la protection de la vie privée des systèmes suivants pour la spécification, la conception, le développement, la mise en œuvre et la modification des systèmes et des composants de systèmes : [Affectation : principes d'ingénierie de la sécurité et de la protection de la vie privée des systèmes définis par l'organisation].

Responsable : Aucun

Discussion :

Les principes d'ingénierie de la sécurité et de la protection de la vie privée des systèmes sont étroitement liés au cycle de développement des systèmes et mis en œuvre au cours de celui-ci (voir le contrôle SA-03). Les organisations peuvent appliquer les principes d'ingénierie de la sécurité et de la protection de la vie privée aux nouveaux systèmes en cours de développement ou aux systèmes faisant l'objet d'une mise à niveau. Dans le cas des systèmes existants, les organisations appliquent, dans la mesure du possible, les principes d'ingénierie de la sécurité et de la protection de la vie privée aux mises à niveau et aux modifications en tenant compte de l'état actuel du matériel, des logiciels et des micrologiciels des systèmes en question. L'application des principes d'ingénierie de la sécurité et de la protection de la vie privée des systèmes aide les organisations à développer des systèmes fiables, sécurisés et résilients et à réduire l'exposition aux interruptions, aux risques, aux menaces et aux problèmes de protection de la vie privée pour les utilisatrices et utilisateurs. Les exemples des principes d'ingénierie de la sécurité et de la protection de la vie privée des systèmes comprennent le développement de mesures de protection en couches; l'établissement de stratégies, d'architectures et de contrôles de sécurité et de protection de la vie privée comme base de la conception et du développement des systèmes; l'intégration d'exigences de sécurité et de protection de la vie privée au cycle de développement des systèmes; la délimitation des frontières de sécurité physiques et logiques; l'assurance que les développeuses et développeurs sont formés pour concevoir des logiciels sécurisés; l'adaptation des contrôles pour répondre aux besoins de l'organisation; et la modélisation des menaces afin d'établir les cas d'utilisation, les agents de menace, les vecteurs et schémas d'attaque, les schémas de conception et les contrôles compensatoires nécessaires pour atténuer les risques. Les organisations qui appliquent des principes et concepts d'ingénierie de la sécurité et de protection de la vie privée des systèmes peuvent faciliter le développement de systèmes, de composants de systèmes et des services sécurisés et dignes de confiance, réduire les risques à des niveaux acceptables et prendre des décisions éclairées en matière de gestion des risques. Les principes d'ingénierie de la sécurité des systèmes peuvent également être utilisés pour protéger contre certains risques liés à la chaîne d'approvisionnement, dont l'intégration de matériel résistant au trafiquage dans la conception.

SA-08(01) — Abstractions claires (---)

Énoncés :

Mettre en place le principe de la conception sécurisée des abstractions claires.

Responsable : Aucun

Discussion :

Le principe d'abstractions claires repose sur le fait qu'un système est composé d'interfaces et de fonctions simples et bien définies offrant une vue uniforme et intuitive des données et de la façon dont les données sont gérées. La clarté, la simplicité, la nécessité et la suffisance des interfaces de système – combinées à une définition précise du comportement fonctionnel – favorisent l'analyse, l'inspection et la mise à l'essai, ainsi qu'une utilisation appropriée et sécurisée du système. La clarté d'une abstraction est subjective. Parmi les exemples de l'application de ce principe : éviter les interfaces redondantes et inutiles, masquer l'information et éviter la surcharge sémantique des interfaces ou de leurs paramètres. Le masque d'information (c'est-à-dire, une programmation indépendante de la représentation) est une discipline de conception utilisée pour s'assurer que la représentation interne de l'information dans un composant du système n'est pas visible par les autres composants du système qui évoquent ou appellent le premier composant. Il est ainsi possible de faire en sorte que l'abstraction publiée ne soit pas influencée par la façon dont les données sont gérées à l'interne.

SA-08(02) — Mécanisme moindre commun (---)

Énoncés :

Mettre en place le principe du moindre mécanisme commun dans la conception sécurisée des [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe du moindre mécanisme commun repose sur le fait qu'il faut minimiser les mécanismes communs à plus d'une utilisatrice ou un utilisateur et ceux qui sont nécessaires à tous les utilisateurs (Popek, 1974). La minimisation des mécanismes sous-entend que différents composants d'un système font en sorte de ne pas utiliser le même mécanisme pour accéder à une ressource du système. Chaque mécanisme partagé (en particulier un mécanisme employant des variables communes) représente un chemin d'accès potentiel à l'information entre les utilisatrices et utilisateurs et est conçu avec soin pour veiller à ce qu'il ne compromette pas accidentellement la sécurité (Saltzer & Schroeder, 1975). La mise en place du principe du moindre mécanisme commun aide à réduire les conséquences négatives du partage d'états du système entre différents programmes. Un seul programme arrivant à corrompre un état partagé (y compris des variables communes) a le potentiel de corrompre d'autres programmes qui dépendent de cet état. Le principe du moindre mécanisme commun prend également en charge le principe de simplicité de la conception et permet de corriger le problème des canaux mémoire secrets (Lampson, 1973).

SA-08(03) — Modularité et structuration en couches (---)

Énoncés :

Mettre en place les principes de conception sécurisée de la modularité et de la structuration en couches dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Les principes de modularité et de structuration en couches sont à la base des disciplines d'ingénierie des systèmes. La modularité et la structuration en couches dérivées de la décomposition fonctionnelle permettent de gérer efficacement la complexité des systèmes et font en sorte qu'il est possible de comprendre la structure du système. La décomposition modulaire – ou l'amélioration de la conception du système – pose des défis et résiste aux énoncés de principe généraux. La modularité sert à isoler les fonctions et les structures de données connexes dans des unités logiques bien définies. La structuration en couches permet de mieux comprendre les relations entre ces unités afin de clarifier les dépendances et d'éviter toute complexité indésirable. Le principe de conception sécurisée de la modularité s'ajoute à la modularité fonctionnelle pour inclure des considérations basées sur les relations d'approbation, les privilèges et la stratégie de sécurité. La décomposition modulaire axée sur la sécurité comprend l'affectation de stratégies aux systèmes d'un réseau, la séparation des applications du système dans des processus comportant des espaces d'adresses distinctes, l'affectation de stratégies de système aux couches ainsi que la séparation des processus en des sujets avec privilèges distincts basés sur les domaines de privilèges pris en charge par le matériel.

SA-08(04) — Dépendances partiellement hiérarchisées (---)

Énoncés :

Mettre en place le principe de conception sécurisée des dépendances partiellement hiérarchisées dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe des dépendances partiellement hiérarchisées repose sur le fait que la synchronisation, l'appel et les autres dépendances du système sont partiellement hiérarchisées. Un concept fondamental de la conception de système est la structuration en couches dans le cadre de laquelle le système est organisé en des modules ou des composants bien définis et fonctionnellement reliés. Les couches sont hiérarchisées de façon linéaire pour ce qui est des dépendances entre les couches, faisant en sorte que les couches supérieures soient dépendantes des couches inférieures. Alors qu'elles fournissent les fonctionnalités aux couches supérieures, certaines couches peuvent être autonomes et ne pas dépendre des couches inférieures. Bien qu'il soit impossible de hiérarchiser partiellement toutes les fonctions dans un système donné, les problèmes inhérents de la circularité peuvent être plus faciles à gérer si des dépendances circulaires doivent survenir dans les couches. Les dépendances partiellement hiérarchisées et la structuration en couches du système contribuent considérablement à la simplicité et à l'uniformité de la conception du système. Les dépendances partiellement hiérarchisées facilitent également la mise à l'essai et l'analyse des systèmes.

SA-08(05) — Accès avec médiation efficace (---)

Énoncés :

Mettre en place le principe de conception sécurisée de l'accès avec médiation efficace dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe d'accès avec médiation efficace repose sur le fait que les mécanismes d'application des stratégies utilisent le moindre mécanisme commun disponible pour satisfaire les exigences des parties prenantes tout en respectant les limites imposées. La médiation de l'accès aux ressources du système (c'est-à-dire l'UCT, la mémoire, les dispositifs, les ports de communications, les services, l'infrastructure, les données et l'information) est souvent la principale fonction de sécurité des systèmes sécurisés. Elle permet également d'offrir les protections nécessaires à la capacité que le système fournit aux parties prenantes. La médiation de l'accès aux ressources peut donner lieu à des goulots d'étranglement au niveau des performances si le système n'a pas été conçu correctement. Par exemple, l'accès avec médiation efficace peut être réalisé en faisant appel à des mécanismes matériels. Après avoir obtenu accès à une ressource de niveau inférieur, comme la mémoire, les mécanismes de protection matérielle peuvent s'assurer d'interdire tout accès sortant.

SA-08(06) — Échange minimal (---)

Énoncés :

Mettre en place le principe de conception sécurisée de l'échange minimal dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe d'échange minimal repose sur le fait qu'aucune ressource informatique n'est partagée entre des composants du système (par exemple, les sujets, les processus et les fonctions) à moins qu'il ne soit absolument nécessaire de le faire. L'échange minimal aide à simplifier la conception et la mise en œuvre du système. Pour protéger les ressources des domaines utilisateur contre les entités actives arbitraires, aucune ressource n'est partagée à moins que l'échange n'ait été explicitement demandé et autorisé. Le besoin d'avoir recours au partage de ressources peut être motivé par le principe de conception du moindre mécanisme commun dans les cas des entités internes ou découler des exigences des parties prenantes. Cela dit, l'échange interne est soigneusement conçu pour éviter les problèmes de performances, ainsi que les problèmes liés aux canaux temporels et aux canaux mémoire secrets. L'échange effectué au moyen d'un mécanisme commun peut rendre les données et l'information plus susceptibles de faire l'objet d'une divulgation, d'une utilisation, d'une modification ou d'un accès non autorisé et avoir une incidence négative sur la capacité inhérente fournie par le système. Pour minimiser l'échange causé par les mécanismes communs, il est possible de concevoir ces derniers de manière à ce qu'ils soient réentrants ou virtualisés afin de préserver la séparation. Par ailleurs, l'utilisation de données globales pour l'échange d'information est examinée en profondeur. L'absence d'encapsulation peut brouiller les relations parmi les entités prenant part à l'échange.

SA-08(07) — Complexité réduite (---)

Énoncés :

Mettre en place le principe de conception sécurisée de la complexité réduite dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de complexité réduite repose sur le fait que la conception du système est aussi simple et petite que possible. Une conception simple et petite est plus facile à comprendre et à analyser, et moins sujette aux erreurs. Le principe de complexité réduite s'applique à tous les aspects d'un système, mais il est particulièrement important pour la sécurité en raison des diverses analyses réalisées pour obtenir des preuves de la propriété de sécurité émergente du système. Pour assurer la réussite de telles analyses, il est essentiel de faire appel à une conception simple et de petite taille. L'application du principe de complexité réduite permet aux développeuses et développeurs de système de comprendre l'exactitude et l'exhaustivité des fonctions de sécurité du système. Elle facilite également l'identification des vulnérabilités potentielles. La conséquence de la complexité réduite veut que la simplicité du système soit directement liée au nombre de vulnérabilités qu'il contiendr
a. En d'autres mots, les systèmes plus simples contiennent moins de vulnérabilités. Les avantages de la complexité réduite font en sorte qu'il est plus facile de comprendre si la stratégie de sécurité a bien été intégrée dans la conception du système et qu'il y a moins de vulnérabilités susceptibles d'être introduites lors du processus de développement technique. Un autre avantage est qu'on peut en venir à une conclusion par rapport à l'exactitude, à l'exhaustivité et à l'existence des vulnérabilités avec un degré élevé d'assurance comparativement aux conclusions formulées dans des situations où la conception du système est fondamentalement plus complexe. La transition de technologies plus anciennes à de plus nouvelles (par exemple, la transition de IPv4 à IPv6) peut exiger une mise en œuvre simultanée des technologies anciennes et nouvelles au cours de la période de transition. Cela pourrait donner lieu à une hausse temporaire dans la complexité du système durant la transition.

SA-08(08) — Évolutivité sécurisée (---)

Énoncés :

Mettre en place le principe de conception sécurisée de l'évolutivité dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe d'évolutivité sécurisée repose sur le fait qu'un système est développé de manière à faciliter la maintenance de ses propriétés de sécurité lorsque des changements sont apportés à la structure du système, à ses interfaces, à ses interconnexions (c'est-à-dire l'architecture du système), à ses fonctionnalités ou à ses configurations (c'est-à-dire la mise en application des stratégies de sécurité). Les changements comprennent une capacité nouvelle, améliorée ou mise à niveau du système, les activités de maintenance et de maintien, et la reconfiguration. Bien qu'il ne soit pas possible de planifier tous les aspects de l'évolution du système, on peut anticiper les mises à niveau et les changements du système en procédant à l'analyse de l'orientation stratégique de la mission ou des activités, des changements anticipés dans l'environnement de menace et des besoins anticipés en matière de maintenance et de maintien. Il n'est pas réaliste de s'attendre à ce que des systèmes complexes demeurent sécurisés dans des contextes non envisagés lors de leur développement, peu importe si de tels contextes sont liés à l'environnement opérationnel ou à l'utilisation. Un système peut être sécurisé dans certains nouveaux contextes, mais on ne peut garantir qu'un comportement émergent sera toujours sécurisé. Il est plus facile d'intégrer la robustesse dans un système dès le départ. Par conséquent, le maintien de la robustesse du système exige que l'on planifie les changements plutôt que de s'adapter de manière spontanée ou non méthodique. Les avantages de ce principe comprennent des coûts moindres pour le cycle de vie du fournisseur, des coûts de possession moins élevés, une plus grande sécurité du système, une gestion plus efficace des risques liés à la sécurité et moins d'incertitude quant au risque.

SA-08(09) — Composants fiables (---)

Énoncés :

Mettre en place le principe de conception sécurisée des composants fiables dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe des composants fiables repose sur le fait qu'un composant est, au minimum, à la fois fiable et robuste à un niveau proportionnel aux dépendances de sécurité qu'il prend en charge (c'est-à-dire dans quelle mesure les autres composants peuvent garantir qu'il accomplit ses fonctions de sécurité). Le principe permet de composer les composants de manière à ce que la fiabilité et la robustesse ne soient pas réduites par inadvertance et que la confiance ne soit pas accordée de façon injustifiée par la suite. En définitive, ce principe exige quelques mesures au moyen desquelles la confiance accordée à un composant, ainsi que sa fiabilité et sa robustesse, peuvent être mesurées sur une même échelle d'abstraction. Le principe des composants fiables est particulièrement pertinent si on considère des systèmes et des composants dans lesquels on retrouve des dépendances complexes aux chaînes d'approbation. La dépendance fiable est également appelée une relation d'approbation et on peut retrouver des chaînes de relations d'approbation. Le principe des composants fiables s'applique aussi à un composant complexe qui est composé de sous-composants (par exemple, un sous-système) susceptibles d'avoir différents niveaux de fiabilité. L'hypothèse conservatrice est que la fiabilité d'un composant complexe repose sur le sous-composant le moins fiable. Il peut être possible de justifier l'ingénierie de la sécurité en déterminant que la fiabilité d'un composant complexe en particulier est supérieure à l'hypothèse conservatrice. Cela dit, une telle justification reflète le raisonnement logique résultant d'une déclaration claire des objectifs de fiabilité, ainsi que de preuves pertinentes et crédibles. La fiabilité d'un composant complexe n'est pas la même que celle d'une application plus grande de la mise en couches de la défense en profondeur dans le composant ou d'une duplication des composants. Les techniques de défense en profondeur n'accroissent pas la fiabilité de l'ensemble au-delà de celle du composant le moins fiable.

SA-08(10) — Confiance hiérarchique (---)

Énoncés :

Mettre en place le principe de conception sécurisée de la confiance hiérarchique dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de confiance hiérarchique des composants repose sur le principe des composants fiables et sur le fait que les dépendances de sécurité d'un système formeront un ordre partiel si elles permettent d'assurer le principe des composants fiables. L'ordre partiel offre les bases nécessaires au raisonnement de la fiabilité et de la robustesse lorsqu'il s'agit de composer un système sécurisé à partir de composants développés ou acquis indépendamment. Pour analyser la fiabilité et la robustesse d'un système composé de composants développés ou acquis indépendamment, il est essentiel d'éliminer les dépendances circulaires. Si un composant plus fiable ou plus robuste situé sur une couche inférieure du système en venait à dépendre d'un composant moins fiable et moins robuste sur une couche supérieure, il en résulterait une réduction globale de la fiabilité ou de la robustesse du système en raison de l'élément plus faible dont dépend le système. Les relations d'approbation (ou chaînes d'approbation) peuvent se manifester de plusieurs manières. Par exemple, le certificat racine d'une hiérarchie de certificats est le nœud le plus fiable de la hiérarchie, ce qui fait en sorte que les branches de la hiérarchie constituent des nœuds moins fiables. C'est également le cas dans un système multicouche à assurance élevée lorsque le noyau de sécurité (y compris la base matérielle) situé sur la couche la plus basse du système constitue le composant le plus fiable. Toutefois, le principe de confiance hiérarchique n'interdit pas l'utilisation de composants excessivement fiables. Dans un système à fiabilité faible, il arrive qu'il soit raisonnable de faire appel à un composant à fiabilité élevée plutôt qu'à un composant moins fiable (par exemple, pour des raisons de disponibilité ou de rentabilité). Dans de tels cas, toute dépendance d'un composant à fiabilité élevée à un composant moins fiable ne mine pas la fiabilité du système à faible fiabilité qui en résulte ni n'augmente sa fiabilité ou sa robustesse.

SA-08(11) — Seuil de modification inverse (---)

Énoncés :

Mettre en place le principe de conception sécurisée du seuil de modification inverse dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de seuil de modification inverse repose sur les principes de composants fiables et de confiance hiérarchique et sur le fait que le degré de protection fourni à un composant est proportionnel à sa fiabilité. À mesure que la confiance conférée à un composant augmente, la protection contre la modification non autorisée du composant augmente dans la même mesure. La protection contre la modification non autorisée peut prendre la forme d'une autoprotection du composant et d'une robustesse intrinsèque, ou encore provenir des protections accordées au composant par d'autres éléments ou attributs de l'architecture de sécurité (pour inclure les protections dans l'environnement d'exploitation).

SA-08(12) — Protection hiérarchique (---)

Énoncés :

Mettre en place le principe de conception sécurisée de la protection hiérarchique dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de protection hiérarchique repose sur le fait qu'un composant ne doit pas être protégé des composants plus fiables. Dans le cas limite d'un composant offrant la fiabilité la plus élevée, celui-ci se protège de tous les autres composants. Par exemple, si le noyau d'un système d'exploitation est considéré comme étant le composant le plus fiable d'un système, alors il se protège lui-même contre les applications non fiables qu'il prend en charge, mais, à l'inverse, les applications n'ont pas à se protéger du noyau. La fiabilité des utilisatrices et utilisateurs est un facteur à considérer dans l'application du principe de protection hiérarchique. Un système approuvé n'a pas à se protéger d'une utilisatrice ou un utilisateur d'une fiabilité équivalente dans la mesure où l'utilisation de systèmes non fiables dans des environnements au niveau de sécurité le plus élevé où les utilisatrices et utilisateurs font l'objet d'une fiabilité élevée et où d'autres protections sont mises en place pour restreindre et protéger l'environnement d'exécution au niveau de sécurité le plus élevé.

SA-08(13) — Éléments de sécurité minimisés (---)

Énoncés :

Mettre en place le principe de conception sécurisée des éléments de sécurité minimisés dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe des éléments de sécurité minimisés repose sur le fait que le système ne comporte aucun composant fiable superflu. Le principe des éléments de sécurité minimisés comporte deux aspects : le coût global et la complexité de l'analyse de la sécurité. Les composants fiables sont généralement plus coûteux à construire et à mettre en œuvre en raison de la rigueur accrue nécessaire au développement des processus et des exigences liées à l'intégrité de la chaîne d'approvisionnement. Les composants fiables exigent une analyse plus poussée de la sécurité pour déterminer leur robustesse et la mise en place de plus amples contrôles dans la chaîne d'approvisionnement pour déterminer leur fiabilité. Pour réduire les coûts et la complexité de l'analyse de la sécurité, un système devrait ainsi contenir le moins de composants fiables possible. L'analyse de l'interaction des composants fiables avec les autres composants du système est l'un des aspects les plus importants de la vérification de la sécurité des systèmes. Si les interactions entre les composants sont inutilement complexes, la sécurité du système sera également plus difficile à évaluer que celle dont les relations d'approbation internes sont simples et élégamment élaborées. En règle générale, miser sur moins de composants fiables donne lieu à moins de relations d'approbation internes et à un système plus simple.

SA-08(14) — Droit d'accès minimal (---)

Énoncés :

Mettre en place le principe de conception sécurisée du droit d'accès minimal dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de droit d'accès minimal repose sur le fait que l'on doit affecter suffisamment de privilèges à chaque composant du système pour accomplir ses fonctions, mais sans plus. L'application du principe de droit d'accès minimal limite la portée des actions du composant, ce qui a deux conséquences désirées : l'incidence sur la sécurité d'un composant sera moindre advenant une défaillance, une corruption ou une mauvaise utilisation et il sera plus facile de procéder à l'analyse de la sécurité du composant. Le principe de droit d'accès minimal est un principe omniprésent qui se reflète dans tous les aspects de la conception d'un système sécurisé. Les interfaces utilisées pour appeler les capacités du composant ne sont accessibles que par certains sous-ensembles de la population d'utilisatrices et utilisateurs, et la conception du composant prend en charge un degré de granularité suffisamment précis pour assurer la décomposition des privilèges. Par exemple, dans le cas d'un mécanisme de vérification, on pourrait retrouver une interface pour la ou le gestionnaire des vérifications, qui configure les paramètres de vérification, une interface pour l'exploitante ou exploitant des vérifications, qui s'assure que les données de vérification sont collectées et stockées en toute sécurité et, pour finir, une autre interface pour la réviseuse ou le réviseur des vérifications, qui doit afficher les données de vérification collectées sans toutefois effectuer d'opérations à partir de ces données. En plus de ses manifestations dans l'interface du système, le principe de droit d'accès minimal peut être utilisé comme principe directeur pour la structure interne du système en tant que tel. Un aspect du droit d'accès minimal interne est de construire des modules de manière à ce que seules les fonctions d'un module puissent effectuer des opérations directes sur les éléments encapsulés par ce module. Il est possible d'accéder indirectement aux éléments externes à un module susceptibles d'être touchés par l'exploitation de ce module dans le cadre d'une interaction (par exemple, lors d'un appel de fonction) avec le module qui contient ces éléments. Un autre aspect du droit d'accès minimal interne veut que la portée d'un module ou d'un composant donné comprenne uniquement les éléments du système qui sont nécessaires pour son fonctionnement et que les modes d'accès des éléments (par exemple, lecture, écriture) soient minimaux. La minimisation des fonctions qui utilisent des privilèges élevés (par exemple, la restriction des outils et des fonctions qui s'exécutent en mode noyau) est un exemple de droit d'accès minimal dans le développement logiciel.

SA-08(15) — Autorisation des prédicats (---)

Énoncés :

Mettre en place le principe de conception sécurisée de l'autorisation des prédicats dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe d'autorisation des prédicats repose sur le fait que les conceptrices et concepteurs de système doivent considérer d'exiger que de multiples entités autorisées donnent leur consentement avant de permettre l'exécution d'une opération très critique ou l'accès à des données, de l'information ou des ressources hautement sensibles. À l'origine, Saltzer (Saltzer & Schroeder, 1975) a nommé l'autorisation des prédicats « la séparation des privilèges ». C'est en quelque sorte l'équivalent de la séparation des tâches. La division des privilèges parmi plusieurs partis diminue la probabilité d'une utilisation abusive et fournit l'assurance qu'un incident, une déception ou un abus de confiance ne peut à lui seul déclencher une action définitive qui pourrait causer des dommages importants. Les options de conception pour un tel mécanisme peuvent exiger une action simultanée (par exemple, larguer un missile nucléaire exige que deux personnes autorisées différentes donnent la bonne commande dans un délai très court) ou une séquence d'opérations où chaque action successive est déclenchée par une certaine action antérieure, sans qu'une seule personne ne puisse être en mesure de déclencher plus d'une action.

SA-08(16) — Fiabilité autonome (---)

Énoncés :

Mettre en place le principe de conception sécurisée de la fiabilité autonome dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de fiabilité autonome repose sur le fait que les systèmes doivent réduire leur dépendance envers les autres systèmes pour assurer leur propre fiabilité. Un système est fiable par défaut et toute connexion à une entité externe sert à compléter ses fonctions. Si un système doit maintenir une connexion à une autre entité externe afin de maintenir sa fiabilité, alors ce système est vulnérable aux menaces malveillantes et non malveillantes, ce qui pourrait donner lieu à une perte ou à une dégradation de cette connexion. L'avantage du principe de fiabilité autonome est que l'isolation d'un système le rendra moins vulnérable aux attaques. Une conséquence de ce principe touche la capacité du système (ou d'un composant du système) à fonctionner en isolation pour ensuite se synchroniser de nouveau avec les autres composants une fois la connexion établie.

SA-08(17) — Composition distribuée sécurisée (---)

Énoncés :

Mettre en place le principe de conception sécurisée de la composition distribuée sécurisée dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de composition distribuée sécurisée repose sur le fait que la composition distribuée sécurisée qui permet d'appliquer la même stratégie de sécurité au système donne lieu à un système qui applique, au minimum, cette stratégie avec autant d'efficacité que les composants individuels. Plusieurs des principes de conception de systèmes sécurisés abordent la façon dont les composants peuvent ou devraient interagir. La nécessité de créer ou d'activer une capacité à partir de la composition de composants distribués peut accroître la pertinence de ces principes. Plus particulièrement, la transition d'une stratégie de sécurité d'un système autonome à un système distribué ou à un système de systèmes peut avoir des résultats inattendus ou émergents. Les mécanismes d'uniformité des protocoles de communications et des données distribuées aident à assurer une application uniforme de la stratégie dans l'ensemble d'un système distribué. L'architecture de sécurité d'un système à composition distribuée fait l'objet d'une analyse rigoureuse pour assurer le niveau d'assurance d'une application appropriée de la stratégie à l'échelle du système.

SA-08(18) — Voies de communication fiables (---)

Énoncés :

Mettre en place le principe de conception sécurisée des voies de communication fiables dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe des voies de communication fiables repose sur le fait qu'au moment de composer un système dans lequel une menace potentielle pèse sur les communications entre les composants (c'est-à-dire les interconnexions entre chaque composant), chaque voie de communication est fiable à un niveau proportionnel aux dépendances de sécurité qu'elle prend en charge (c'est-à-dire dans quelle mesure les autres composants lui font confiance pour exécuter ses fonctions de sécurité). Les voies de communication fiables sont mises en place en combinant un accès restreint à la voie de communication (pour assurer une correspondance acceptable dans la fiabilité et la robustesse des points d'extrémité prenant part à la communication) et le recours à des mesures de protection de bout en bout pour les données transmises par l'intermédiaire de la voie de communication (pour protéger contre l'interception et la modification, et pour accroître l'assurance d'une communication de bout en bout appropriée).

SA-08(19) — Protection continue (---)

Énoncés :

Mettre en place le principe de conception sécurisée de la protection continue dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de protection continue repose sur le fait que les composants et les données servant à appliquer la stratégie de sécurité sont soumis à une protection interrompue qui est conforme à la stratégie de sécurité et aux hypothèses de l'architecture de sécurité. On ne peut offrir aucune assurance que le système est en mesure de protéger la protection de la vie privée, l'intégrité et la disponibilité de sa capacité de conception s'il y a des lacunes dans la protection. Toute assurance quant à la capacité de sécuriser une fonctionnalité fournie exige que les données et l'information fassent l'objet d'une protection continue. Cela signifie qu'il n'y a aucune période au cours de laquelle les données et l'information sont laissées sans protection alors qu'elles sont sous le contrôle du système (c'est-à-dire au cours de la création, du stockage, du traitement ou de la communication des données et de l'information, ainsi que lors de l'initialisation, de l'exécution, de la défaillance, de l'interruption et de l'arrêt du système). Une protection continue exige l'adoption des principes du concept de contrôleur de référence selon lequel chaque requête est validée par le contrôleur de référence, faisant en sorte que ce dernier soit en mesure de se protéger contre le trafiquage et qu'il soit possible d'établir une assurance suffisante de l'exactitude et de l'exhaustivité du mécanisme à partir de l'analyse et des tests. De plus, elle exige l'adoption du principe de défaillance et de reprise sécurisées (à savoir la préservation d'un état sécurisé lors d'une erreur, d'un défaut, d'une défaillance et d'une attaque fructueuse; la préservation d'un état sécurisé lors d'une reprise à des modes opérationnels normaux, dégradés ou autres). Une protection continue s'applique également aux systèmes conçus pour s'exécuter dans différentes configurations, y compris celles qui fournissent une capacité opérationnelle totale et les configurations en mode dégradé qui fournissent une capacité opérationnelle partielle. Le principe de protection continue exige que les changements apportés aux stratégies de sécurité du système puissent être retracés jusqu'au besoin opérationnel qui guide la configuration et être vérifiés (c'est-à-dire pouvoir s'assurer que les changements proposés ne poussent pas le système à passer à un état non sécurisé). Une traçabilité et une vérification insuffisantes peuvent mener à des états irréguliers ou à une discontinuité de la protection en raison de la nature complexe et indécidable du problème. L'utilisation de définitions de configuration prévérifiées qui reflètent la nouvelle stratégie de sécurité permet de réaliser l'analyse nécessaire pour déterminer si la transition des anciennes stratégies aux nouvelles est essentiellement atomique et s'il est garanti que les effets résiduels de l'ancienne stratégie n'entreront pas en conflit avec la nouvelle stratégie. La capacité de démontrer une protection continue est fondée sur une articulation claire des besoins de protection du cycle de vie en tant qu'exigences des parties prenantes en matière de sécurité.

SA-08(20) — Gestion sécurisée des métadonnées (---)

Énoncés :

Mettre en place le principe de conception sécurisée de la gestion sécurisée des métadonnées dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de gestion sécurisée des métadonnées repose sur le fait que les métadonnées sont des objets de première classe en ce qui concerne la stratégie de sécurité lorsque la stratégie exige une protection complète de l'information ou que le sous-système de sécurité doit se protéger lui-même. Le principe de gestion sécurisée des métadonnées est axé sur la reconnaissance qu'un système, un sous-système ou un composant ne peut se protéger lui-même que s'il protège les données dont il dépend pour s'exécuter correctement. Les données ne sont généralement pas interprétées par le système sur lequel elles sont stockées. Ce dernier peut avoir une valeur sémantique (il contient l'information) pour les utilisatrices, les utilisateurs et les programmes qui traitent les données. À l'inverse, les métadonnées sont de l'information sur les données, comme un nom de fichier ou la date à laquelle le fichier a été créé. Les métadonnées sont liées aux données cibles qu'elles décrivent d'une manière que le système peut interpréter, mais elles n'ont pas à être stockées avec les données cibles ou à proximité de celles-ci. Certaines métadonnées peuvent avoir pour cible d'autres métadonnées (par exemple, le niveau de classification ou d'incidence sur un nom de fichier), ce qui est notamment le cas pour les métadonnées autoréférentes. La seconde nature apparente des métadonnées peut entraîner la négligence de son besoin de protection légitime, ce qui va à l'encontre de la stratégie de sécurité qui comprend l'exfiltration de l'information. Une préoccupation particulière associée à la protection insuffisante des métadonnées touche les systèmes à sécurité multiniveau (MLS pour Multilevel Secure). Les systèmes MLS gèrent l'accès d'une personne à un objet en fonction des niveaux de sensibilité relative. Par conséquent, les étiquettes du niveau de sensibilité sont apposées directement ou affectées indirectement aux personnes et aux objets qui relèvent du contrôle du système MLS. La conséquence des métadonnées étiquetées pour les systèmes MLS veut qu'une étiquette soit ajoutée aux objets contenant des métadonnées. Comme pour les évaluations des besoins de protection des données, il convient de s'assurer que les mesures de protection de la confidentialité et de l'intégrité soient évaluées, précisées et affectées aux métadonnées, comme ça serait le cas pour les données de la mission, de l'organisation ou des systèmes.

SA-08(21) — Auto-analyse (---)

Énoncés :

Mettre en place le principe de conception sécurisée de l'auto-analyse dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe d'auto-analyse repose sur le fait qu'un composant de système est en mesure d'évaluer son état interne et sa fonctionnalité dans une certaine mesure à plusieurs phases d'exécution et que cette capacité d'auto-analyse est proportionnelle au niveau de robustesse conféré au système. Au niveau du système, l'auto-analyse peut être effectuée dans le cadre des évaluations hiérarchiques de la robustesse réalisées en partant de la base. Selon cette approche, les composants des niveaux inférieurs vérifient l'intégrité des données et corrigent la fonctionnalité (dans une certaine mesure) des composants de niveaux supérieurs. Par exemple, des séquences de démarrage fiables comprennent un composant approuvé d'un niveau inférieur qui atteste de l'intégrité des composants des niveaux supérieurs suivants de manière à établir une chaîne d'approbation transmissible. À la racine, un composant s'atteste lui-même, ce qui sous-entend généralement une présomption axiomatique ou de nature environnementale par rapport à son intégrité. Les résultats des auto-analyses peuvent être utilisés pour offrir une protection contre les erreurs induites à l'externe, les défectuosités internes ou les erreurs temporaires. L'adoption de ce principe permet de détecter certaines défectuosités ou erreurs simples sans laisser les conséquences de l'erreur ou de la défectuosité se propager à l'extérieur du composant. Par ailleurs, l'autotest peut être utilisé pour attester de la configuration du composant en détectant les conflits potentiels dans la configuration par rapport à la configuration prévue.

SA-08(22) — Responsabilisation et traçabilité (---)

Énoncés :

Mettre en place le principe de conception sécurisée de la responsabilisation et de la traçabilité dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de responsabilisation et de traçabilité repose sur le fait qu'il est possible d'établir la trace des mesures relatives à la sécurité (c'est-à-dire les interactions entre sujet et objet) pour l'entité au nom de laquelle l'action a été prise. Ce principe exige une infrastructure fiable qui peut consigner les détails des actions qui touchent la sécurité du système (par exemple, un sous-système de vérification). Pour ce faire, le système doit être en mesure d'identifier de façon unique l'entité au nom de laquelle l'action est exécutée et d'enregistrer la séquence pertinente des actions exécutées. La stratégie de responsabilisation exige également que la piste de vérification elle-même soit protégée contre l'accès et la modification non autorisés. Le principe de droit d'accès minimal facilite le traçage des actions d'entités en particulier, puisqu'il accroît la granularité de la responsabilisation. Le fait d'associer les actions aux entités du système, et ultimement aux utilisatrices et utilisateurs, et de sécuriser la piste de vérification contre les accès et les modifications non autorisés favorise la non-répudiation, car une fois qu'une action est enregistrée, il n'est pas possible de modifier la piste de vérification. Une autre fonction importante de la responsabilisation et de la traçabilité est liée à l'analyse régulière et judiciaire des événements associés à la violation de la politique de sécurité. L'analyse des journaux de vérification peut fournir des renseignements supplémentaires qui peuvent permettre de déterminer non seulement le chemin ou la composante qui a permis la violation de la stratégie de sécurité, mais aussi les actions des personnes associées à cette violation.

SA-08(23) — Valeurs par défaut sécurisées (---)

Énoncés :

Mettre en place le principe de conception sécurisée des valeurs par défaut sécurisées dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe des valeurs par défaut sécurisées repose sur le fait que la configuration par défaut d'un système (y compris ses sous-systèmes, ses composants et ses mécanismes sous-jacents) constitue une application restrictive et conservatrice de la stratégie de sécurité. Le principe des valeurs par défaut sécurisées s'applique à la configuration initiale (c'est-à-dire par défaut) d'un système, ainsi qu'à l'ingénierie et à la conception de sécurité du contrôle de l'accès et des autres fonctions de sécurité qui suivent une stratégie consistant à tout refuser à l'exclusion de ce qui est explicitement autorisé. L'aspect initial de la configuration de ce principe exige que toute configuration d'usine d'un système, d'un sous-système ou d'un composant de système n'aide pas à contrevenir à la stratégie de sécurité et puisse empêcher le système de s'exécuter dans la configuration par défaut dans les cas où la stratégie de sécurité à propre dit exige que l'utilisatrice ou utilisateur opérationnel procède à la configuration. Les valeurs par défaut restrictives font en sorte que le système s'exécute comme en usine avec l'autoprotection adéquate et soit en mesure d'éviter les atteintes à la sécurité avant que la stratégie de sécurité et la configuration du système aient été établies. Dans les cas où la protection fournie par le produit d'usine est inadéquate, les parties prenantes évaluent le risque posé par l'utilisation du produit en question avant d'établir un état sécurisé initial. Le respect du principe des valeurs par défaut sécurisées permet de garantir qu'un système est dans un état sécurisé au moment de terminer son initialisation. Dans les situations où le système n'arrive pas à terminer l'initialisation, il exécutera une opération demandée au moyen des valeurs par défaut sécurisées ou n'exécutera aucune opération. Il convient de se référer aux principes de protection continue et de défaillance et reprise sécurisées qui sont similaires à ce principe pour fournir la capacité de détecter les défaillances et d'assurer la reprise par la suite. L'approche en matière d'ingénierie de la sécurité relative à ce principe repose sur le fait que les mécanismes de sécurité refusent les requêtes à moins qu'on puisse établir qu'elles ont été formées adéquatement et qu'elles respectent la stratégie de sécurité. L'option sécurisée est d'autoriser une requête dans la mesure où l'on peut établir qu'elle respecte la stratégie. Dans un large système, les conditions à respecter pour accepter une demande qui est refusée par défaut sont souvent plus concises et complètes que celles qu'il faudrait vérifier pour refuser une demande autorisée par défaut.

SA-08(24) — Défaillance et reprise sécurisées (---)

Énoncés :

Mettre en place le principe de conception sécurisée de la défaillance et de la reprise sécurisées dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de défaillance et de reprise sécurisées repose sur le fait que ni la défaillance d'une fonction ou d'un mécanisme d'un système ni la reprise effectuée advenant une défaillance ne saurait donner lieu à la violation d'une stratégie de sécurité. Le principe de défaillance et de reprise sécurisées est similaire au principe de protection continue qui vise à s'assurer qu'un système est en mesure de détecter (dans les limites fixées) les défaillances actuelles et imminentes à toutes les étapes de son exécution (c'est-à-dire l'initialisation, l'exécution normale, l'arrêt et la maintenance) et à prendre les mesures appropriées pour veiller à ne pas enfreindre les stratégies de sécurité. Dans les cas précisés, le système est de plus capable de rétablir ses activités après une défaillance actuelle ou imminente afin d'assurer une reprise des activités sécurisées normales, dégradées ou autres tout en veillant à ce qu'un état sécurisé soit maintenu de manière à ne pas enfreindre les stratégies de sécurité. Une défaillance est une condition dans le cadre de laquelle le comportement d'un composant déroge du comportement indiqué ou attendu pour le résultat explicitement documenté. Advenant la détection d'une fonction de sécurité défaillante, le système peut se reconfigurer de manière à contourner le composant défectueux tout en maintenant la sécurité et à fournir la totalité ou une partie de la fonctionnalité au système d'origine, ou il peut s'éteindre entièrement pour éviter d'enfreindre davantage les stratégies de sécurité. Pour ce faire, les fonctions de reconfiguration du système sont conçues pour assurer une application continue de la stratégie de sécurité au cours des diverses phases de reconfiguration. Une autre technique à utiliser pour assurer la reprise advenant des défaillances consiste à procéder à une restauration à un état sécurisé (lequel peut correspondre à l'état initial), puis à éteindre ou à remplacer le service ou le composant défaillant de manière à pouvoir reprendre les activités sécurisées. La défaillance d'un composant peut être détectée ou non par les composants qui l'utilisent. Le principe de défaillance sécurisée veut que les composants plantent dans un état qui refuse l'accès plutôt que de l'autoriser. Par exemple, une opération nominalement atomique qui est interrompue avant sa complétion n'enfreint pas la stratégie de sécurité et est conçue de manière à gérer les événements d'interruption en faisant appel à un niveau d'atomicité plus élevé et à des mécanismes de restauration (par exemple, des transactions). Si un service est utilisé, ses propriétés d'atomicité sont bien documentées et caractérisées de manière à ce que le composant qui a recours à ce service puisse détecter et gérer les événements d'interruption de façon appropriée. Par exemple, un système est conçu pour répondre en douceur à la déconnexion et prendre en charge la resynchronisation et l'uniformité des données après la déconnexion. Les stratégies de protection contre les défaillances qui font appel à la réplication des mécanismes d'application des stratégies (ce qu'on appelle parfois la défense en profondeur) peuvent permettre au système de continuer à un état sécurisé même si un mécanisme n'a pas réussi à le protéger. Si les mécanismes sont similaires, par contre, la protection additionnelle peut être illusoire, car l'adversaire n'a qu'à mener une série d'attaques. Dans un système en réseau, percer la sécurité d'un système ou d'un service peut permettre à un attaquant de faire la même chose pour tous les autres systèmes et services reproduits qui sont similaires. En utilisant plusieurs mécanismes de protection aux fonctions considérablement différentes, on peut réduire la probabilité qu'une attaque soit répliquée ou répétée. Des analyses sont effectuées pour évaluer les coûts et les avantages de telles techniques de redondance par rapport à l'utilisation accrue des ressources et aux effets négatifs sur les performances globales du système. Des analyses supplémentaires sont effectuées à mesure que la complexité de ces mécanismes augmente, comme ça pourrait être le cas pour les comportements dynamiques. Une complexité accrue réduit généralement la robustesse. Lorsqu'une ressource ne peut pas faire l'objet d'une protection continue, il est capital de détecter et de réparer toute brèche de sécurité avant que la ressource soit utilisée de nouveau dans un contexte sécurisé.

SA-08(25) — Sécurité économique (---)

Énoncés :

Mettre en place le principe de conception sécurisée de la sécurité économique dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de sécurité économique repose sur le fait que les mécanismes de sécurité ne coûtent pas plus que les dommages potentiels qui pourraient découler d'une violation de la sécurité. Il s'agit d'une forme d'analyse coûts-avantages axée sur la sécurité qui sert à la gestion des risques. Les hypothèses en matière de coûts formulées dans l'analyse coûts-avantages permettent d'éviter que les conceptrices et concepteurs de système incorporent des mécanismes de sécurité offrant une robustesse plus importante que nécessaire lorsque la robustesse d'un mécanisme est proportionnelle au coût. Le principe de sécurité économique exige également l'analyse des avantages de l'assurance par rapport au coût de cette assurance pour ce qui est de l'effort nécessaire pour obtenir des preuves pertinentes et crédibles.

SA-08(26) — Sécurité des performances (---)

Énoncés :

Mettre en place le principe de conception sécurisée de la sécurité des performances dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de la sécurité des performances repose sur le fait que les mécanismes de sécurité sont construits de manière à ne pas dégrader inutilement les performances des systèmes. Les exigences de conception des parties prenantes et des systèmes en matière de performances et de sécurité sont articulées et hiérarchisées de façon précise. Pour que la mise en œuvre des systèmes respecte ses exigences de conception et soit acceptée par les parties prenantes (c'est-à-dire la validation par rapport aux exigences des parties prenantes), les conceptrices et concepteurs sont soumis aux contraintes précises que les besoins en matière de performances des capacités imposent aux besoins de protection. Les services de sécurité intensifs sur le plan des calculs, comme la cryptographie, sont évalués afin de démontrer qu'ils n'auront aucune incidence importante sur les considérations prioritaires en matière de performances ou qu'ils peuvent fournir un compromis acceptable entre les performances et une protection fiable. Parmi les compromis à considérer, on retrouve des services de sécurité qui sont moins intensifs sur le plan des calculs dans la mesure où de tels services sont disponibles et suffisants. L'insuffisance d'un service de sécurité est déterminée par la capacité et la robustesse fonctionnelles du mécanisme. La robustesse d'un mécanisme est sélectionnée en fonction des exigences de sécurité, des problèmes de temps système essentiels aux performances (par exemple, la gestion des clés cryptographiques) et d'une évaluation de la capacité de la menace. Le principe de la sécurité des performances mène à l'incorporation de fonctionnalités qui facilitent l'application de la stratégie de sécurité, mais qui nécessitent un temps système minimal, comme les mécanismes matériels de bas niveau sur lesquels les services de niveaux supérieurs sont élaborés. De tels mécanismes de bas niveau sont généralement très spécifiques; leurs fonctionnalités sont limitées et ils sont optimisés aux fins de performances. Par exemple, une fois que les droits d'accès pour une partie de la mémoire sont accordés, plusieurs systèmes utilisent les mécanismes matériels pour s'assurer que tous les accès futurs utilisent la bonne adresse dans la mémoire et le bon mode d'accès. L'application de ce principe réitère la nécessité de concevoir la sécurité du système à partir de zéro et d'intégrer des mécanismes simples aux couches inférieures qui peuvent servir de fondement pour les mécanismes de niveau supérieur.

SA-08(27) — Sécurité tenant compte du facteur humain (---)

Énoncés :

Mettre en place le principe de conception sécurisée de la sécurité tenant compte du facteur humain dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de la sécurité tenant compte du facteur humain repose sur le fait que l'interface utilisateur des fonctions de sécurité et des services de soutien est intuitive et conviviale et qu'elle permet de fournir une rétroaction des actions effectuées par les utilisatrices et utilisateurs qui ont une incidence sur une telle stratégie et son application. Les mécanismes qui permettent d'appliquer la stratégie de sécurité ne sont pas intrusifs pour les utilisatrices et utilisateurs et sont conçus de manière à ne pas nuire à l'efficacité de ces derniers. Les mécanismes d'application des stratégies de sécurité offrent également aux utilisatrices et utilisateurs une rétroaction claire, utile et pertinente et des avertissements lorsque des choix non sécurisés sont effectués. Une attention particulière est accordée aux interfaces par l'entremise desquelles le personnel responsable de l'administration et de l'exploitation des systèmes configure et met en place les stratégies de sécurité. Idéalement, les membres du personnel devraient être en mesure de comprendre les conséquences de leurs choix. Le personnel qui assume des responsabilités d'administration et d'exploitation de systèmes est en mesure de configurer les systèmes avant leur démarrage et de les administrer lors de leur exécution tout en étant persuadé que ses intentions ont bien été prises en compte dans les mécanismes des systèmes. Les services, les fonctions et les mécanismes de sécurité ne nuisent pas à l'utilisation prévue du système et ne compliquent pas son utilisation inutilement. Il convient de faire un compromis entre l'utilisabilité du système et la robustesse nécessaire pour appliquer les stratégies de sécurité. Si les mécanismes de sécurité sont frustrants ou difficiles à utiliser, les utilisatrices et utilisateurs pourraient les désactiver, les éviter ou les utiliser d'une manière qui va à l'encontre des exigences de sécurité et des besoins de protection pour lesquels les mécanismes ont été conçus.

SA-08(28) — Sécurité acceptable (---)

Énoncés :

Mettre en place le principe de conception sécurisée de la sécurité acceptable dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de sécurité acceptable exige que le niveau de protection de la vie privée et de performances fourni par le système réponde aux attentes des utilisatrices et utilisateurs. La perception du respect de la vie privée peut avoir une incidence sur les comportements, le moral et l'efficacité des utilisatrices et utilisateurs. Selon la stratégie de protection de la vie privée de l'organisation et la conception du système, les utilisatrices et utilisateurs devraient être en mesure de limiter leurs actions de manière à protéger leur vie privée. Si les systèmes ne parviennent pas à fournir des interfaces intuitives ou à répondre aux attentes en matière de protection de la vie privée et de performances, les utilisatrices et utilisateurs peuvent choisir d'éviter entièrement le système ou de l'utiliser d'une façon qui pourrait être inefficace, voire non sécurisée.

SA-08(29) — Procédures reproduisibles et documentées (---)

Énoncés :

Mettre en place le principe de conception sécurisée des procédures reproduisibles et documentées dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe des procédures reproduisibles et documentées repose sur le fait que les techniques et les méthodes employées pour construire un composant de système permettent au même composant d'être reconstruit entièrement et correctement à une date ultérieure. Les procédures reproduisibles et documentées soutiennent le développement d'un composant qui est identique au composant créé plus tôt, dont l'utilisation peut être répandue. Dans le cas des autres artéfacts de système (par exemple, la documentation et les résultats des tests), la reproductibilité permet d'assurer l'uniformité et d'inspecter les artéfacts. Les procédures reproduisibles et documentées peuvent être introduites à différentes phases du cycle de développement des systèmes et contribuer à la capacité d'évaluer les énoncés d'assurance du système. Il s'agit notamment des procédures systématiques pour le développement et l'examen du code, les procédures de gestion des configurations pour les outils de développement et les artéfacts de systèmes, ainsi que les procédures pour la livraison des systèmes.

SA-08(30) — Rigueur procédurale (---)

Énoncés :

Mettre en place le principe de conception sécurisée de la rigueur procédurale dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de rigueur procédurale repose sur le fait qu'un processus du cycle de vie des systèmes est proportionnel à sa fiabilité et à sa robustesse prévues. La rigueur procédurale définit la portée, la profondeur et la granularité des procédures du cycle de vie des systèmes. De rigoureuses procédures du cycle de vie des systèmes aident à renforcer l'assurance que le système est adéquat et exempt de fonctionnalités imprévues de nombreuses façons. Premièrement, les procédures imposent des automatismes régulateurs au processus du cycle de vie, comme interdire l'introduction de fonctionnalités non définies. Deuxièmement, les procédures rigoureuses appliquées aux activités d'ingénierie de la sécurité des systèmes qui génèrent les spécifications et les autres documents de conception des systèmes aident à mieux comprendre le système tel qu'il a été conçu plutôt que de se fier au composant et d'espérer que sa mise en œuvre repose sur une spécification faisant autorité (et pouvant être trompeuse). Pour finir, il est plus facile d'apporter des modifications à un composant de système existant lorsque les spécifications détaillées décrivent sa conception actuelle que lorsqu'on ne peut se référer au code source ou aux schémas pour tenter d'en comprendre le fonctionnement. La rigueur procédurale permet de s'assurer que les exigences fonctionnelles de sécurité et d'assurance sont satisfaites et elle permet d'éclairer la détermination de la fiabilité et de la robustesse. La rigueur procédurale est proportionnelle au degré d'assurance demandé au système. Si l'assurance requise pour le système est faible, un niveau élevé de rigueur procédurale peut générer des coûts inutiles. Cela dit, s'il est essentiel d'offrir une assurance élevée, le coût associé à la rigueur procédurale est justifié.

SA-08(31) — Modification de systèmes sécurisés (---)

Énoncés :

Mettre en place le principe de conception sécurisée de la modification de systèmes sécurisés dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de modification de systèmes sécurisés repose sur le fait que la modification d'un système maintient sa sécurité pour ce qui a trait aux exigences de sécurité et à la tolérance au risque des parties prenantes. Les mises à niveau ou les modifications apportées aux systèmes peuvent transformer les systèmes sécurisés en systèmes non sécurisés. Les procédures liées à la modification des systèmes garantissent que si le système doit maintenir sa fiabilité et sa robustesse, la même rigueur appliquée à son développement initial sera également appliquée à tous les changements apportés au système. Comme les modifications peuvent avoir une incidence sur la capacité du système à maintenir son état sécurisé, une analyse méticuleuse de la sécurité de la modification est nécessaire avant de procéder à sa mise en œuvre et à son déploiement. Ce principe est similaire au principe d'évolutivité sécurisée.

SA-08(32) — Documentation adéquate (---)

Énoncés :

Mettre en place le principe de conception sécurisée de la documentation adéquate dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le principe de documentation adéquate repose sur le fait que le personnel organisationnel responsable d'interagir avec le système dispose de la documentation adéquate et de l'information nécessaire pour contribuer à la sécurité du système plutôt que d'y nuire. Malgré les tentatives de se conformer à des principes tels que la sécurité tenant compte du facteur humain et la sécurité acceptable, les systèmes sont fondamentalement complexes et il n'est pas toujours facile de déterminer le but de la conception des mécanismes de sécurité et les ramifications d'une mauvaise utilisation ou configuration de ces mécanismes. Des utilisatrices et utilisateurs mal informés et insuffisamment formés peuvent introduire des vulnérabilités en raison d'omissions et d'erreurs réelles. La disponibilité de la documentation et de la formation peut aider à fournir aux membres du personnel les connaissances nécessaires pour assumer le rôle essentiel qu'elles et ils jouent dans l'application de principes tels que la protection continue. La documentation est écrite clairement et étayée par une formation offrant une sensibilisation en matière de sécurité et la compréhension des responsabilités relatives à la sécurité.

SA-08(33) — Minimisation (---)

Énoncés :

Mettre en place le principe de protection de la vie privée de la minimisation au moyen de [Affectation : processus définis par l'organisation].

Responsable : Aucun

Discussion :

Le principe de minimisation repose sur le fait que les organisations ne doivent collecter que les renseignements personnels ou l'information sensible qui concernent directement un programme opérationnel ou une activité de l'institution. Dans le même sens, les organisations ne doivent conserver les renseignements personnels et l'information sensible que pour la période nécessaire à l'atteinte du but fixé. Advenant le cas où l'information sensible ou les renseignements personnels doivent être communiqués à d'autres programmes ou organisations, il convient de les limiter à ce qui est expressément exigé par le programme ou l'organisation destinataire. Les organisations devraient mettre en place des processus pour appliquer le principe de minimisation conformément aux lois et aux politiques applicables.

SA-08(400) — Ingénieures et ingénieurs brevetés et agréés (---)

Énoncés :

Avoir recours à des ingénieures et ingénieurs brevetés et agréés en sécurité qui assument la responsabilité des spécifications, de la conception, du développement et de la mise en œuvre de solutions de sécurité et de protection de la vie privée du système d'information.

Responsable : Aucun

SA-09 — Services de systèmes externes (---)

Énoncés :

a. Exiger que les fournisseurs de services de systèmes externes respectent les exigences organisationnelles en matière de sécurité et de protection de la vie privée et aient recours aux contrôles suivants : [Affectation : contrôles définis par l'organisation];
b. Définir et documenter la surveillance organisationnelle, de même que les rôles et responsabilités des utilisatrices et utilisateurs en ce qui a trait aux services de systèmes externes;
c. Mettre en oeuvre sur une base continue des processus, des méthodes et des techniques pour surveiller la conformité aux contrôles des fournisseurs de services externes : [Affectation : méthodes, techniques et processus définis par l'organisation].

Responsable : Aucun

Discussion :

Les services de systèmes externes sont fournis par un fournisseur externe et l'organisation n'exerce aucun contrôle direct sur le plan de la mise en oeuvre des contrôles requis ou de l'évaluation de l'efficacité de ces contrôles. Les organisations peuvent établir des relations avec des fournisseurs de services externes de nombreuses façons, y compris au moyen de partenariats, de contrats, d'ententes interorganismes, d'ententes liées aux secteurs d'activités, d'accords de licence, de coentreprises et d'échanges de chaîne d'approvisionnement. La responsabilité en matière de gestion des risques pouvant découler du recours à des services de systèmes externes continue d'incomber aux autorités responsables. Dans le cas des services externes, la chaîne d'approbation exige que les organisations créent et maintiennent un certain niveau de confiance en la capacité de chaque fournisseur participant à une relation client-fournisseur d'assurer une protection adéquate des services rendus. La portée et la nature de cette chaîne d'approbation varient en fonction des relations établies entre les organisations et les fournisseurs externes. Les organisations documentent les bases de la relation d'approbation pour que celle-ci puisse faire l'objet d'une surveillance. La documentation des services de systèmes externes comprend les rôles et responsabilités du gouvernement, des fournisseurs de services et des utilisatrices et utilisateurs terminaux en matière de sécurité, ainsi que tout accord sur les niveaux de service pertinent. Les accords sur les niveaux de service définissent les attentes de rendement pour les contrôles mis en oeuvre, décrivent les résultats mesurables et identifient les exigences en matière de solution et d'intervention pour les situations de non-respect qui ont été relevées.

SA-09(01) — Évaluations des risques et approbations organisationnelles (---)

Énoncés :

a. Procéder à une évaluation des risques organisationnels avant d'acquérir ou d'externaliser des services de sécurité de l'information
b. S'assurer que l'acquisition ou l'externalisation des services de sécurité de l'information est approuvée par [Affectation : personnel ou rôles définis par l'organisation]

Responsable : Aucun

Discussion :

Les services de sécurité de l'information comprennent l'utilisation de dispositifs de sécurité, comme des pare-feu ou des services de gestion des clés, ainsi que la surveillance des incidents, leur analyse et les interventions connexes. Les risques évalués peuvent comprendre les risques liés au système, à la mission ou aux activités, à la sécurité, à la protection de la vie privée ou à la chaîne d'approvisionnement.

SA-09(02) — Établissement des fonctions, des ports, des protocoles et des services (---)

Énoncés :

Exiger que les fournisseurs de services de systèmes externes identifient les fonctions, les ports, les protocoles et les autres services nécessaires à l'utilisation des services en question : [Affectation : services de systèmes externes définis par l'organisation].

Responsable : Aucun

Discussion :

L'information provenant de fournisseurs de services externes en ce qui a trait aux fonctions, aux ports, aux protocoles et aux services utilisés aux fins de la prestation des services en question peut s'avérer utile lorsqu'il s'agit de comprendre pourquoi il est avantageux d'imposer certaines restrictions à des services ou à des fonctions ou encore de bloquer certains ports ou protocoles.

SA-09(03) — Établissement et maintien d'une relation de confiance avec les fournisseurs de services (---)

Énoncés :

Établir, documenter et maintenir des relations de confiance avec les fournisseurs de services externes en fonction des exigences, des propriétés, des conditions ou des facteurs suivants : [Affectation : exigences de sécurité et de protection de la vie privée, propriétés, conditions ou facteurs définis par l'organisation qui constituent des relations de confiance acceptables].

Responsable : Aucun

Discussion :

Les relations de confiance entre les organisations et les fournisseurs de services externes reflètent le degré de confiance que le risque associé à l'utilisation des services externes se situe à un niveau acceptable. La relation de confiance permet aux organisations d'accroître le degré de certitude à l'égard de l'aptitude des fournisseurs de services à garantir un rendement adéquat en matière de sécurité. Elle peut également s'avérer utile au moment de prendre des mesures d'intervention en cas d'incident ou de planifier des mises à niveau ou une obsolescence. De telles relations peuvent s'avérer compliquées en raison du nombre potentiellement élevé d'entités qui prennent part aux interactions avec la clientèle, des relations hiérarchiques et des niveaux de confiance, ainsi que de la nature des interactions entre les diverses parties. Dans certains cas, le degré de confiance se fonde sur le niveau de contrôle que les organisations peuvent exercer sur les fournisseurs de services externes pour ce qui a trait aux contrôles nécessaires pour assurer la protection du service, de l'information ou de la vie privée des individus, ainsi que sur les facteurs permettant de prouver l'efficacité des contrôles mis en place. Le niveau de contrôle est déterminé par les conditions générales d'utilisation énoncées dans les contrats ou les accords sur les niveaux de service.

SA-09(04) — Concordance des intérêts des clients et des fournisseurs (---)

Énoncés :

Prendre les mesures suivantes pour confirmer que les intérêts de [Affectation : fournisseurs de services externes désignés par l'organisation] répondent aux intérêts de l'organisation : [Affectation : actions définies par l'organisation].

Responsable : Aucun

Discussion :

Comme les organisations comptent de plus en plus sur les services de fournisseurs externes, il est possible que les intérêts des organisations et des fournisseurs divergent. Dans de telles situations, la simple application de contrôles techniques, procéduraux ou opérationnels pourrait s'avérer insuffisante, particulièrement lorsque les fournisseurs responsables de la mise en œuvre et de la gestion de ces contrôles fonctionnent selon des modalités qui ne correspondent pas aux intérêts des organisations clientes. Pour résoudre de telles questions, les organisations peuvent prendre diverses mesures, comme exiger des vérifications des antécédents de certaines et certains membres du personnel des fournisseurs externes, examiner les registres de propriété, embaucher des fournisseurs de services dont la fiabilité est démontrée (comme des fournisseurs qui ont satisfait aux exigences d'autres organisations) et procéder à des visites périodiques, routinières ou inopinées des installations de fournisseurs de services.

SA-09(05) — Lieux de traitement, de stockage et de service (---)

Énoncés :

Circonscrire les lieux de [Sélection (un choix ou plus) : traitement de l'information; stockage de l'information ou de données; services de systèmes] à [Affectation : lieux désignés par l'organisation] en se fondant sur [Affectation : exigences ou conditions définies par l'organisation].

Responsable : Aucun

Discussion :

Le choix des lieux de prestation des services essentiels de traitement et de stockage de l'information, ou l'emplacement des systèmes peut avoir une incidence directe sur l'aptitude des organisations à exécuter adéquatement les fonctions liées à leur mission et à leurs activités. Ce type de situation se présente lorsque des fournisseurs externes administrent eux-mêmes les lieux de traitement, de stockage ou de service. Les critères que les fournisseurs de services utilisent pour sélectionner les lieux de traitement, de stockage ou de service peuvent être différents de ceux employés par l'organisation. Par exemple, les organisations pourraient vouloir restreindre les emplacements de stockage des données ou de l'information à certains lieux pour faciliter les activités d'intervention lors d'incidents touchant la sécurité de l'information ou de violations de données. Les activités d'intervention en cas d'incident, notamment les analyses criminalistiques et les enquêtes après coup des incidents, pourraient être entravées par les lois ou les protocoles en vigueur dans les sites où le traitement et le stockage ont lieu ou dans les sites depuis lesquels les services de systèmes s'exécutent.

SA-09(06) — Clés cryptographiques contrôlées par l'organisation (---)

Énoncés :

Maintenir un contrôle exclusif des clés cryptographiques pour le matériel chiffré stocké ou transmis par l'entremise d'un système externe.

Responsable : Aucun

Discussion :

Maintenir le contrôle exclusif des clés cryptographiques dans un système externe empêche le personnel du système externe de déchiffrer les données organisationnelles. Le contrôle organisationnel des clés cryptographiques peut être mis en place en chiffrant et déchiffrant les données dans l'organisation alors que les données sont envoyées et reçues depuis un système externe ou en ayant recours à un composant qui permet d'utiliser localement les fonctions de chiffrement et de déchiffrement sur le système externe tout en permettant un accès organisationnel exclusif aux clés de chiffrement.

SA-09(07) — Vérification de l'intégrité contrôlée par l'organisation (---)

Énoncés :

Fournir la capacité de vérifier l'intégrité de l'information qui réside sur le système externe.

Responsable : Aucun

Discussion :

Le stockage de l'information organisationnelle dans un système externe ne devrait permettre qu'une visibilité limitée de l'état de sécurité de ses données. La capacité de l'organisation de vérifier et de valider l'intégrité des données qui y sont stockées sans les transférer du système externe offre une telle visibilité.

SA-09(08) — Lieu de stockage et de traitement (au Canada) (---)

Énoncés :

Restreindre le lieu géographique du traitement de l'information et du stockage des données aux installations situées dans la frontière gouvernementale et juridique du Canada.

Responsable : Aucun

Discussion :

Le choix du lieu géographique de la prestation des services essentiels de traitement et de stockage de l'information peut avoir une incidence directe sur l'aptitude des organisations à exécuter adéquatement les fonctions liées à leur mission et à leurs activités. Une compromission ou une violation de l'information et des systèmes à incidence élevée peut avoir des conséquences négatives ou catastrophiques sur les biens ou les activités de l'organisation, les individus, les autres organisations et le Canad
a. Restreindre le traitement et le stockage de l'information à incidence élevée aux installations dans la frontière gouvernementale et juridique du Canada permet de fournir un plus grand contrôle sur un tel traitement et un tel stockage.

SA-10 — Gestion des configurations par les développeuses et développeurs (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de :
a. procéder à la gestion des configurations au cours [Sélection (un choix ou plus) : de la conception; du développement; de la mise en œuvre; de l'exploitation; de l'élimination] du système, du composant ou du service
b. documenter, gérer et contrôler l'intégrité des changements apportés aux [Affectation : éléments de configuration définis par l'organisation dans le cadre de la gestion des configurations]
c. mettre en œuvre uniquement les changements approuvés par l'organisation au système, au composant ou au service
d. documenter les changements approuvés apportés au système, au composant ou au service et les répercussions potentielles de tels changements sur la sécurité et la protection de la vie privée
e. assurer le suivi des failles de sécurité informatique et de leur résolution dans le système, le composant ou le service et faire rapport des conclusions au [Affectation : personnel désigné par l'organisation]

Responsable : Aucun

Discussion :

Les organisations considèrent la qualité et l'achèvement des activités de gestion des configurations menées par les développeuses et développeurs comme des preuves directes de l'application efficace des contrôles de sécurité. Les contrôles comprennent la protection contre la modification ou la destruction non autorisée des copies maîtresses de tout le matériel utilisé pour générer certains aspects de la sécurité matérielle, logicielle ou micrologicielle du système. Le maintien de l'intégrité des changements apportés au système, au composant du système ou au service qui s'y rapporte exige que le contrôle rigoureux des configurations tout au long du cycle de développement du système fasse en sorte d'enregistrer les changements autorisés et d'empêcher les changements non autorisés. Les éléments de configuration qui font partie de la gestion des configurations sont les suivants : le modèle formel; les spécifications de conception fonctionnelles, de haut niveau et de bas niveau; les autres données de conception; la documentation relative à la mise en œuvre; les schémas relatifs au code source et aux composants matériels; la version actuelle du code objet; les outils de comparaison des descriptions de nouvelles versions de composants matériels et de code source servant à la sécurité avec les versions précédentes; ainsi que les accessoires et la documentation de test. Selon les besoins liés à la mission et aux activités des organisations ou la nature des relations contractuelles en vigueur, les développeuses et développeurs peuvent assurer la gestion des configurations pendant les phases d'exploitation et de maintenance du cycle de développement du système.

SA-10(01) — Vérification de l’intégrité des logiciels et des micrologiciels (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant de système ou du service qui s’y rapporte vérifie l’intégrité des composants logiciels et micrologiciels.

Responsable : Aucun

Discussion :

La vérification de l’intégrité des logiciels et des micrologiciels permet aux organisations de détecter les changements non autorisés apportés aux composants logiciels et micrologiciels au moyen d’outils, de techniques et de mécanismes fournis par la développeuse ou le développeur. Les mécanismes de vérification de l’intégrité peuvent également détecter la contrefaçon de composants logiciels et micrologiciels. Les organisations vérifient l’intégrité des logiciels et des micrologiciels au moyen, par exemple, du hachage unidirectionnel sécurisé fourni par les développeuses et développeurs. Les logiciels et micrologiciels qui sont produits incluent également les mises à jour qui doivent être appliquées à ces logiciels et micrologiciels.

SA-10(02) — Processus de gestion des configurations de rechange (---)

Énoncés :

Prévoir un processus de gestion des configurations de rechange auquel participent des membres du personnel en l'absence d'une équipe de développeuses et développeurs ou d'intégratrices et intégrateurs spécialisés en gestion des configurations.

Responsable : Aucun

Discussion :

Le processus de gestion des configurations de rechange peut être requis si les organisations utilisent des produits informatiques COTS. Les processus de gestion des configurations de rechange comprennent le personnel de l'organisation qui examine et approuve les changements proposés à apporter aux systèmes, aux composants de systèmes et aux services qui s'y rapportent, et qui est chargé de mener des analyses des répercussions sur la sécurité et la protection de la vie privée avant la mise en œuvre de tout changement apporté aux systèmes, aux composants ou aux services.

SA-10(03) — Vérification de l’intégrité du matériel (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant de système ou du service qui s’y rapporte vérifie l’intégrité des composants matériels.

Responsable : Aucun

Discussion :

La vérification de l’intégrité du matériel permet aux organisations de détecter les changements non autorisés apportés aux composants matériels au moyen d’outils, de techniques, de méthodes et de mécanismes fournis par la développeuse ou le développeur. Les organisations peuvent vérifier l’intégrité des composants matériels en exigeant des étiquettes irreproductibles et des numéros de série vérifiables fournis par les développeuses et développeurs et en imposant l’utilisation de mécanismes d’inviolabilité. Les composants matériels qui sont produits incluent également les mises à jour matérielles et micrologicielles qui doivent être appliquées à ces composants.

SA-10(04) — Génération fiable (---)

Énoncés :

Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou d'un service qui s'y rapporte emploie des outils permettant de comparer les versions nouvellement générées aux versions précédentes des descriptions, du code source et du code objet des composants matériels servant à la sécurité.

Responsable : Aucun

Discussion :

La génération fiable des descriptions, du code source et du code objet tient compte des changements autorisés apportés aux composants matériels, logiciels et micrologiciels d'une version à l'autre au cours de leur développement. Elle met l'accent sur l'efficacité du processus de gestion des configurations des développeuses et développeurs et visent à s'assurer que les versions nouvellement générées des descriptions, du code source et du code objet du matériel servant à la sécurité continuent d'appliquer la stratégie de sécurité du système, du composant de système ou du service qui s'y rapporte. En revanche, les contrôles SA-10(01) et SA-10(03) permettent aux organisations de détecter les changements non autorisés apportés aux composants matériels, logiciels et micrologiciels au moyen des outils, des techniques ou des mécanismes fournis par les développeuses et développeurs.

SA-10(05) — Intégrité du mappage pour le contrôle des versions (---)

Énoncés :

Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou d'un service qui s'y rapporte maintienne l'intégrité du mappage entre les données de la version maîtresse qui décrivent, d'une part, la version actuelle du matériel, des logiciels et des micrologiciels servant à la sécurité et, d'autre part, la copie maîtresse des données de la version qui se trouve actuellement sur le site.

Responsable : Aucun

Discussion :

L'intégrité du mappage pour le contrôle des versions permet de résoudre la question des changements apportés aux composants matériels, logiciels et micrologiciels au cours du développement initial et des mises à jour du cycle de vie du système. Il est essentiel de maintenir l'intégrité entre les copies maîtresses des composants matériels, logiciels et micrologiciels servant à la sécurité (y compris les éléments de conception, les schémas du matériel et le code source) et les données équivalentes des copies maîtresses dans les environnements opérationnels pour garantir la disponibilité des systèmes organisationnels dont dépendent les fonctions liées à la mission et aux activités de l'organisation.

SA-10(06) — Distribution fiable (---)

Énoncés :

Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou d'un service qui s'y rapporte exécute les procédures visant à garantir que les mises à jour des composants matériels, logiciels et micrologiciels servant à la sécurité, qui sont distribuées à l'organisation sont en tout point conformes aux spécifications des copies maîtresses.

Responsable : Aucun

Discussion :

La distribution fiable des mises à jour des composants matériels, logiciels et micrologiciels servant à la sécurité permet de garantir que les mises à jour en question constituent des représentations fidèles des copies maîtresses maintenues par la développeuse ou le développeur et qu'elles n'ont pas été trafiquées en cours de distribution.

SA-10(07) — Représentantes et représentants de la sécurité et de la protection de la vie privée (---)

Énoncés :

Exiger que [Affectation : représentante ou représentant de la sécurité et de la protection de la vie privée désigné par l'organisation] soit membre de [Affectation : processus de gestion et de contrôle des configurations défini par l'organisation].

Responsable : Aucun

Discussion :

Les représentantes et représentants en matière de sécurité et de protection de la vie privée de l'information peuvent comprendre les responsables de la sécurité des systèmes, les cadres supérieures et supérieurs de la gouvernance en matière de sécurité du ministère, les hauts fonctionnaires ou cadres supérieures et supérieurs en matière de protection de la vie privée et les responsables de la protection de la vie privée des systèmes. Il est important d'avoir parmi le personnel des représentantes et représentants qui sont dotés d'une expertise en sécurité de l'information, car les changements aux configurations des systèmes peuvent avoir des répercussions imprévues, dont certaines pouvant avoir trait à la sécurité ou à la protection de la vie privée. La détection rapide de ces changements permet d'éviter des conséquences négatives inattendues qui pourraient avoir des conséquences sur l'état de sécurité et de protection de la vie privée des systèmes. Le processus de gestion et de contrôle des configurations de cette amélioration reflète celui défini par l'organisation dans le contrôle SA-10B.

SA-11 — Évaluations et tests effectués par les développeuses et développeurs (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte fasse ce qui suit à toutes les phases de postconception du cycle de développement du système de manière à :
a. élaborer et mettre en oeuvre un plan pour les évaluations des contrôles de sécurité et de protection de la vie privée en cours
b. procéder au test ou à l'évaluation [Sélection (un choix ou plus) : unité; intégration; système; régression] tous les [Affectation : fréquence définie par l'organisation] selon [Affectation : profondeur et couverture définies par l'organisation]
c. fournir une preuve de l'élaboration d'un plan d'évaluation et des résultats des tests ou de l'évaluation
d. mettre en oeuvre un processus vérifiable de correction des défauts
e. corriger les défauts relevés au cours des tests et de l'évaluation

Responsable : Aucun

Discussion :

Des tests et des évaluations confirment que les contrôles requis ont été adéquatement mis en oeuvre, qu'ils fonctionnent selon les attentes, qu'ils permettent d'appliquer la stratégie de sécurité et de protection de la vie privée en vigueur et qu'ils répondent aux exigences de sécurité et de protection de la vie privée établies. L'interconnexion des composants de systèmes ou les changements apportés à ces derniers pourraient influer sur les propriétés de sécurité des systèmes et la vie privée des utilisatrices et utilisateurs. Ces interconnexions ou changements, comme la mise à niveau ou le remplacement d'applications, de systèmes d'exploitation et de micrologiciels, peuvent avoir un effet défavorable sur les contrôles mis en oeuvre précédemment. Une évaluation continue au cours du développement fournit des modalités de test et d'évaluation complémentaires que les développeuses et développeurs peuvent utiliser dans le but de réduire ou d'éliminer les défauts éventuels. Les tests liés à des applications logicielles sur mesure peuvent exiger le recours à des approches, comme l'examen manuel du code, l'examen de l'architecture de sécurité, les tests d'intrusion, ainsi que l'analyse statique, l'analyse dynamique, l'analyse binaire ou une combinaison de ces trois types d'analyse. Les développeuses et développeurs peuvent utiliser les approches d'analyse, ainsi que l'instrumentation de sécurité et les tests à données aléatoires, dans une gamme d'outils et dans le cadre des examens du code source. Les plans d'évaluation de la sécurité et de la protection de la vie privée comprennent les activités que les développeuses et développeurs seront appelés à mener, notamment des analyses, des tests, des évaluations et des examens visant des composants logiciels ou micrologiciels, le degré de rigueur à respecter, la fréquence des tests et des évaluations en cours, ainsi que les types d'artéfacts produits durant ces activités. La profondeur des tests et des évaluations porte sur le degré de rigueur et de détail associé au processus d'évaluation. L'envergure des tests et des évaluations renvoie à la portée (par exemple, le nombre et le type) des artéfacts compris dans le processus d'évaluation. Les contrats contiennent les critères d'acceptation relatifs aux plans d'évaluation de la sécurité et de la protection de la vie privée, les processus de correction des lacunes ainsi que les preuves que les plans et les processus ont été appliqués rigoureusement et en temps opportun. Les méthodes d'examen et de protection des plans d'évaluation, des preuves et de la documentation sont proportionnelles à la catégorie de sécurité ou au niveau de classification du système visé. Les contrats peuvent préciser les exigences relatives à la protection des documents.

SA-11(01) — Analyse statique du code (---)

Énoncés :

Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou du service qui s'y rapporte utilise des outils d'analyse statique du code pour identifier les défauts courants et documenter les résultats de l'analyse.

Responsable : Aucun

Discussion :

L'analyse statique du code dicte la technologie et la méthodologie employées pour les examens de sécurité et comprend une vérification des lacunes dans le code, ainsi que l'intégration de code ou de bibliothèques qui contiennent des vulnérabilités connues ou qui sont désuets et non pris en charge. L'analyse statique du code peut être utilisée pour relever les vulnérabilités et imposer l'adoption des pratiques de codage sécurisé. Elle est particulièrement efficace lorsqu'elle est utilisée dans les premières phases du processus de développement, au moment où les changements de code peuvent être automatiquement analysés dans le but de trouver les lacunes. L'analyse statique du code peut fournir des conseils clairs en matière de correction et relever les défauts à corriger par les développeuses et développeurs. Les preuves d'une mise en oeuvre adéquate de l'analyse statique peuvent comprendre l'agrégation de la densité des défauts pour les types de défauts critiques, la preuve que les défauts ont été inspectés par les développeuses, les développeurs ou les spécialistes de la sécurité et les preuves que les défauts ont été corrigés. Une forte densité de résultats ignorés (couramment appelés de faux positifs) pourrait être le symptôme d'un problème lié au processus ou à l'outil d'analyse. Dans de tels cas, les organisations établissent la validité des preuves en les comparant à celles obtenues d'autres sources.

SA-11(02) — Modélisation des menaces et analyses des vulnérabilités (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant ou du service qui s'y rapporte effectue une modélisation des menaces et des analyses des vulnérabilités au cours du développement, ainsi que des tests et une évaluation du système, du composant ou du service qui :
a. utilise l'information contextuelle suivante : [Affectation : information relative aux répercussions définie par l'organisation, environnement opérationnel, menaces connues ou présumées, et niveaux acceptables de risque]
b. utilise les méthodes et les outils suivants : [Affectation : méthodes et outils définis par l'organisation]
c. procède à la modélisation et à l'analyse du niveau de rigueur suivant : [Affectation : profondeur et étendue de modélisation et d'analyse définies par l'organisation]
d. démontre que les critères d'acceptation suivants ont été respectés : [Affectation : critères d'acceptation définis par l'organisation]

Responsable : Aucun

Discussion :

Les systèmes, les composants de systèmes et les services qui s'y rapportent peuvent s'écarter considérablement des spécifications fonctionnelles et de conception qui ont été créées pendant les phases de conception et de formulation des exigences du cycle de développement des systèmes. Par conséquent, les mises à jour des analyses des menaces et des vulnérabilités de ces systèmes, de ces composants de systèmes ou des services qui s'y rapportent, qui sont effectuées en cours de développement et avant la mise en service, sont essentielles à une exploitation efficace des systèmes, des composants et des services en question. Les analyses des vulnérabilités et la modélisation des menaces, à cette phase du cycle de développement des systèmes, permettent de veiller à ce que les changements apportés à la conception et à la mise en œuvre soient pris en compte et que les vulnérabilités résultant de ces changements soient examinées et fassent l'objet de mesures d'atténuation.

SA-11(03) — Vérification indépendante des plans d'évaluation et des preuves (---)

Énoncés :

a. Exiger que [Affectation : critères d'indépendance définis par l'organisation] soit en mesure d'attester de l'adéquation de la mise en œuvre du plan d'évaluation de sécurité et de vérifier les preuves produites pendant les tests et les évaluations
b. Veiller à ce que l'agente ou agent indépendant ait reçu suffisamment d'information pour mener à bien le processus de vérification ou qu'il dispose de l'autorité nécessaire pour obtenir l'information en question

Responsable : Aucun

Discussion :

Les agentes et agents indépendants possèdent les compétences nécessaires (par exemple, l'expertise, les aptitudes, la formation, les certifications et l'expérience) pour attester de l'adéquation de la mise en œuvre des plans d'évaluation de la sécurité et de la protection de la vie privée formulés par les développeuses ou développeurs.

SA-11(04) — Revues manuelles du code (---)

Énoncés :

Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou du service qui s'y rapporte procède à la revue manuelle du code de [Affectation : code particulier désigné par l'organisation] au moyen des procédures, des techniques ou des processus suivants : [Affectation : procédures, techniques et processus définis par l'organisation].

Responsable : Aucun

Discussion :

Les revues manuelles du code sont généralement réservées aux composants fondamentaux (logiciels et micrologiciels) des systèmes. Ces revues de code sont efficaces, lorsqu'il s'agit de relever les lacunes nécessitant une connaissance des exigences ou du contexte relatifs à l'application, lesquels sont généralement inaccessibles aux techniques et aux outils automatisés d'analyse comme les analyses statiques ou dynamiques. Les avantages de la revue manuelle du code comprennent la possibilité de comparer les matrices de contrôle d'accès aux contrôles d'application et l'examen approfondi des mises en œuvre et des contrôles cryptographiques.

SA-11(05) — Tests d'intrusion (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte procède à des tests d'intrusion :
a. au niveau de rigueur suivant : [Affectation : profondeur et étendue des tests définies par l'organisation]
b. selon les contraintes suivantes : [Affectation : contraintes définies par l'organisation]

Responsable : Aucun

Discussion :

Le test d'intrusion est une méthodologie d'évaluation au cours de laquelle les évaluatrices et évaluateurs ont recours à toute la documentation accessible sur des produits informatiques ou des systèmes et se conforment à des contraintes prédéterminées pour tenter de contourner les fonctions de sécurité et de protection de la vie privée mises en œuvre dans les produits informatiques et les systèmes. Parmi les renseignements utiles nécessaires aux évaluatrices et évaluateurs qui effectuent les tests d'intrusion, on retrouve les spécifications de conception des produits et des systèmes, le code source et les guides d'administration et d'utilisation. Les tests d'intrusion peuvent comprendre notamment les tests en boîte blanche, grise ou noire combinés à des analyses menées par des spécialistes chevronnées et chevronnés, qui visent à simuler des attaques. L'objectif des tests d'intrusion est de découvrir les vulnérabilités dans les systèmes, les composants de systèmes et les services qui peuvent résulter d'erreurs de mise en œuvre, de fautes de configuration ou encore de lacunes ou défectuosités opérationnelles. Les tests d'intrusion peuvent être effectués conjointement avec les revues manuelles et automatisées du code dans le but de produire un niveau d'analyse plus élevé que celui que l'on retrouve couramment. Si l'information des sessions utilisateur et d'autres renseignements personnels sont collectés ou enregistrés au cours des tests d'intrusion, il convient de les traiter de façon appropriée pour en protéger la protection de la vie privée.

SA-11(06) — Examens de la surface d’attaque (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s’y rapporte procède à des examens de la surface d’attaque.

Responsable : Aucun

Discussion :

Les surfaces d’attaque des systèmes et des composants de systèmes sont des secteurs exposés qui accentuent la vulnérabilité des systèmes aux cyberattaques. Les surfaces d’attaque comprennent tous les secteurs accessibles où des faiblesses ou des défauts touchant les composants matériels, logiciels et micrologiciels pourraient être exploités par des adversaires. Les examens de la surface d’attaque visent à s’assurer que les développeuses et développeurs analysent les changements de conception et de mise en œuvre apportés aux systèmes et atténuent les vecteurs d’attaque générés consécutivement aux changements. La correction des défauts signalés comprend la proscription des fonctions risquées.

SA-11(07) — Vérification de la portée des tests et des évaluations (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure que la portée des tests et des évaluations fournit une couverture complète des contrôles requis au niveau de rigueur suivant : [Affectation : profondeur et étendue des tests et des évaluations définies par l'organisation].

Responsable : Aucun

Discussion :

Il est possible de vérifier si les tests et les évaluations fournissent une couverture complète des contrôles requis en faisant appel à diverses techniques d'analyse formelle ou informelle. Chacune de ces techniques fournit un niveau d'assurance accru qui correspond au degré de formalité de l'analyse. Il est possible de rigoureusement démontrer que la couverture des contrôles atteint des niveaux supérieurs d'assurance en recourant à la modélisation formelle et à des techniques d'analyse comme la corrélation entre la mise en œuvre de contrôles et des scénarios de tests comparables.

SA-11(08) — Analyse dynamique du code (---)

Énoncés :

Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou du service qui s'y rapporte utilise des outils d'analyse dynamique du code pour relever les défauts courants et documenter les résultats de l'analyse.

Responsable : Aucun

Discussion :

L'analyse dynamique du code fournit une vérification d'exécution des programmes informatiques au moyen d'outils permettant de signaler l'occurrence de corruption de la mémoire, ainsi que les problèmes liés aux privilèges des utilisatrices et utilisateurs ou d'autres éventuels problèmes de sécurité. L'analyse dynamique du code met à profit des outils d'exécution pour vérifier si les fonctionnalités de sécurité s'exécutent comme prévu. Il existe un type d'analyse dynamique, que l'on nomme également test à données aléatoires, qui provoque des défaillances de programme en introduisant délibérément des données mal formatées ou aléatoires dans les programmes informatiques. Les stratégies des tests à données aléatoires se fondent sur l'utilisation prévue des applications et sur les spécifications de fonctions et de conception des applications. Pour comprendre la portée des analyses dynamiques du code et de l'assurance qu'elle fournit, les organisations peuvent également envisager de mener des analyses de couverture de code (par exemple, la vérification du degré auquel le code a été testé au moyen de mesures, comme le pourcentage des sous-routines testées ou le pourcentage des instructions de programme appelées pendant l'exécution de la suite de tests) et/ou des analyses de concordance (par exemple, le signalement des mots qui sont mal placés dans le code du logiciel, notamment les termes dérogatoires ou les mots qui ne sont pas de l'anglais ou du français).

SA-11(09) — Tests de sécurité des applications interactives (---)

Énoncés :

Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou du service qui s'y rapporte utilise des outils de tests de la sécurité des applications interactives pour relever les défauts et documenter les résultats.

Responsable : Aucun

Discussion :

Les tests de sécurité des applications interactives (également connus pour être axés sur l'instrumentation) permettent de détecter les vulnérabilités en observant les applications lors de leur exécution dans le cadre du test. Le recours à l'instrumentation repose sur des mesures directes des applications en cours d'exécution et utilise l'accès au code, aux interactions avec les utilisatrices et utilisateurs, aux bibliothèques, aux cadres d'applications, aux connexions d'arrière-plan et aux configurations pour mesurer directement l'efficacité des contrôles. Lorsqu'ils sont combinés à des techniques d'analyse, les tests de sécurité des applications interactives peuvent relever les vulnérabilités potentielles et confirmer l'efficacité des contrôles. Les tests axés sur l'instrumentation s'effectuent en temps réel et peuvent être utilisés tout au long du cycle de développement des systèmes.

SA-12 — Protection de la chaîne d’approvisionnement (---)

Énoncés :

Annulé : Transféré sous la famille de contrôles SR.

Responsable : Aucun

SA-12(01) — Stratégies, outils et méthodes d'acquisition (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-05.

Responsable : Aucun

SA-12(02) — Examen des fournisseurs (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-06.

Responsable : Aucun

SA-12(03) — Expédition et entreposage sécurisés (---)

Énoncés :

Annulé : Intégré au contrôle SR-03.

Responsable : Aucun

SA-12(04) — Diversité des fournisseurs (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-03(01).

Responsable : Aucun

SA-12(05) — Limitation des dommages (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-03(02).

Responsable : Aucun

SA-12(06) — Réduction du temps d'approvisionnement (---)

Énoncés :

Annulé : Intégré au contrôle SR-05(01).

Responsable : Aucun

SA-12(07) — Évaluation préalable à la sélection, à l'acceptation et à la mise à jour (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-05(02).

Responsable : Aucun

SA-12(08) — Utilisation du renseignement de toutes sources (---)

Énoncés :

Annulé : Intégré au contrôle RA-03(02).

Responsable : Aucun

SA-12(09) — Sécurité opérationnelle (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-07.

Responsable : Aucun

SA-12(10) — Attestation de l’authenticité et de la non-altérité (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-04(03).

Responsable : Aucun

SA-12(11) — Tests d'intrusion et analyse d'éléments, de processus et des parties prenantes (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-06(01).

Responsable : Aucun

SA-12(12) — Accords interorganisationnels (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-08.

Responsable : Aucun

SA-12(13) — Composants de systèmes d'information essentiels (---)

Énoncés :

Annulé : Intégré aux contrôles MA-06 et RA-09.

Responsable : Aucun

SA-12(14) — Identité et traçabilité (---)

Énoncés :

Annulé : Transféré sous les contrôles SR-04(01) et SR-04(02).

Responsable : Aucun

SA-12(15) — Processus visant à réagir aux faiblesses et aux lacunes (---)

Énoncés :

Annulé : Intégré au contrôle SR-03.

Responsable : Aucun

SA-13 — Fiabilité (---)

Énoncés :

Annulé : Intégré au contrôle SA-08.

Responsable : Aucun

SA-14 — Analyse de criticité (---)

Énoncés :

Annulé : Intégré au contrôle RA-09.

Responsable : Aucun

SA-14(01) — Composants essentiels sans autre source d'approvisionnement viable (---)

Énoncés :

Annulé : Intégré au contrôle SA-20.

Responsable : Aucun

SA-15 — Processus, normes et outils de développement (---)

Énoncés :

a. Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou d'un service qui s'y rapporte suive un processus de développement documenté qui permet :

1. de répondre explicitement aux exigences de sécurité et de protection de la vie privée
2. d'identifier les normes et les outils devant servir au processus de développement
3. de documenter les options et les configurations particulières aux outils utilisés dans le processus de développement
4. de documenter, de gérer et de garantir l'intégrité des changements apportés aux processus et aux outils servant au développement

b. Examiner les processus, les normes, les outils, les options d'outils et les configurations d'outils liés au développement [Affectation : fréquence définie par l'organisation] pour établir si les processus, les normes, les outils, les options des outils et les configurations des outils peuvent répondre aux exigences de sécurité et de protection de la vie privée suivantes : [Affectation : exigences de sécurité et de protection de la vie privée définies par l'organisation]

Responsable : Aucun

Discussion :

Les outils de développement comprennent les langages de programmation et les systèmes de conception assistée par ordinateur. L'examen des processus de développement peut inclure l'utilisation de modèles d'évolution dans le but de définir l'efficacité potentielle des processus en question. Le maintien de l'intégrité des changements dans les outils et les processus facilite une évaluation et une atténuation efficaces de la chaîne d'approvisionnement. Une telle intégrité exige un contrôle des configurations tout au long du cycle de développement des systèmes afin d'assurer le suivi des changements autorisés et de prévenir les changements non autorisés.

SA-15(01) — Mesure de la qualité (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de :
a. définir les mesures de la qualité au début du processus de développement
b. fournir des preuves que les critères de qualité sont respectés à [Sélection (un choix ou plus) : [Affectation : fréquence définie par l'organisation]; [Affectation : échéancier d'examen de programmes défini par l'organisation]; au moment de la mise en service]

Responsable : Aucun

Discussion :

Les organisations ont recours à des paramètres de mesure de la qualité pour établir les niveaux acceptables de qualité des systèmes. Ces paramètres peuvent comprendre des jalons de qualité, qui représentent un ensemble de critères d'accomplissement ou de normes de suffisance qui définissent l'exécution adéquate de phases particulières du projet de développement des systèmes. Par exemple, un jalon de qualité pourrait exiger l'élimination de tous les avertissements de compilateurs ou établir que les avertissements n'ont aucune incidence sur l'efficacité des capacités de sécurité et de protection de la vie privée requises. Pendant l'exécution des phases des projets de développement, les jalons de qualité s'avèrent des indicateurs de progression clairs et précis. D'autres paramètres de mesure s'appliquent à l'intégralité du projet de développement. Les mesures peuvent également inclure la définition des seuils de sévérité des vulnérabilités selon la tolérance au risque de l'organisation, comme exiger l'élimination de toute vulnérabilité connue des systèmes mis en service et la définition des niveaux de sévérité Moyen et Élevé du Common Vulnerability Scoring System (CVSS).

SA-15(02) — Outils de traçabilité des contrôles de sécurité et de protection de la vie privée (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte utilise des outils de traçabilité des contrôles de sécurité et de protection de la vie privée au cours du processus de développement.

Responsable : Aucun

Discussion :

L'objectif est de créer une matrice de traçabilité des exigences de sécurité et de protection de la vie privée. Les équipes de développement de systèmes sélectionnent et déploient des outils de suivi de la sécurité et de la protection de la vie privée, notamment des systèmes de suivi de la vulnérabilité ou des éléments de travail visant à faciliter l'attribution, le triage, le filtrage et le suivi des éléments de travail accomplis ou des tâches associées aux processus de développement.

SA-15(03) — Analyse de criticité (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte procède à une analyse de criticité :
a. aux points de décision suivants dans le cycle de développement du système : [Affectation : points de décision dans le cycle de développement du système définis par l'organisation]
b. au niveau de rigueur suivant : [Affectation : profondeur et étendue de l'analyse de criticité définies par l'organisation]

Responsable : Aucun

Discussion :

L'analyse de criticité effectuée par la développeuse ou le développeur fournit l'information nécessaire à l'analyse de criticité réalisée par les organisations. L'apport des développeuses et développeurs est essentiel à l'analyse de criticité, puisque les organisations pourraient ne pas avoir accès à la documentation détaillée sur la conception des composants des systèmes qui sont développés en tant que produits COTS. Une telle documentation de conception comprend les spécifications fonctionnelles, les conceptions de haut niveau, les conceptions de bas niveau, le code source et les schémas du matériel. L'analyse de criticité est importante pour les systèmes organisationnels qui ont été désignés en tant que biens de grande importance. Les biens de grande importance peuvent être des systèmes à incidence moyenne ou élevée en raison de l'intérêt accru des adversaires ou les conséquences potentiellement négatives sur l'entreprise gouvernementale. L'apport des développeuses et développeurs est particulièrement important lorsque les organisations procèdent à des analyses de criticité de la chaîne d'approvisionnement.

SA-15(04) — Modélisation des menaces et analyse des vulnérabilités (---)

Énoncés :

Annulé : Intégré au contrôle SA-11(02).

Responsable : Aucun

SA-15(05) — Réduction de la surface d’attaque (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s’y rapporte réduise les surfaces d’attaque à [Affectation : limites définies par l’organisation].

Responsable : Aucun

Discussion :

La réduction de la surface d’attaque s’aligne étroitement sur les analyses de menaces et de vulnérabilité ainsi que sur l’architecture et la conception des systèmes. La réduction de la surface d’attaque constitue un moyen de réduire les risques encourus par les organisations en limitant considérablement les occasions d’exploiter les faiblesses et les lacunes (par exemple, les vulnérabilités potentielles) inhérentes aux systèmes, aux composants de systèmes et aux services qui s’y rapportent. La réduction de la surface d’attaque comprend la mise en place du concept des défenses par couche, l’application des principes de droit d’accès minimal et de fonctionnalité minimale, l’adoption des pratiques de développement logiciel sécurisé, la proscription des fonctions risquées, la réduction des points d’entrée disponibles aux utilisatrices et utilisateurs non autorisés, la réduction de la quantité de code à exécuter et l’élimination des interfaces de programmation d’application (API pour Application Programming Interface) qui sont vulnérables aux attaques.

SA-15(06) — Amélioration continue (---)

Énoncés :

Exiger que la développeuse ou le développeur d'un système d'information, d'un composant du système ou du service qui s'y rapporte mette en œuvre un processus détaillé visant expressément à améliorer continuellement le processus de développement.

Responsable : Aucun

Discussion :

Les développeuses et développeurs de systèmes, de composants de systèmes et de services qui s'y rapportent évaluent l'efficacité et l'efficience de leurs processus de développement pour faire en sorte qu'ils répondent toujours mieux aux objectifs de qualité et qu'ils soient dotés des capacités de sécurité et de protection de la vie privée requises compte tenu des environnements de menaces.

SA-15(07) — Analyse automatisée des vulnérabilités (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte, [Affectation : fréquence définie par l'organisation] :
a. réalise une analyse automatisée des vulnérabilités au moyen de [Affectation : outils définis par l'organisation]
b. définisse les possibilités d'exploitation des vulnérabilités relevées
c. définisse les mesures d'atténuation des risques liés aux vulnérabilités décelées
d. fournisse les données produites par les outils et les résultats des analyses à [Affectation : personnel ou rôles définis par l'organisation]

Responsable : Aucun

Discussion :

Les outils automatisés peuvent analyser plus efficacement les faiblesses ou lacunes exploitables dans les systèmes vastes et complexes, puisqu'ils hiérarchisent les vulnérabilités selon leur gravité et formulent des recommandations pour l'atténuation des risques.

SA-15(08) — Réutilisation de l’information sur les menaces et les vulnérabilités (---)

Énoncés :

Exiger que la développeuse ou le développeur d’un système, d’un composant du système ou d’un service qui s’y rapporte utilise une modélisation des menaces et des analyses des vulnérabilités exécutées sur des systèmes, des composants ou des services semblables de façon à éclairer le processus de développement en cours.

Responsable : Aucun

Discussion :

Les analyses des vulnérabilités menées sur des applications logicielles semblables peuvent fournir de précieux renseignements susceptibles de résoudre d’éventuels problèmes de conception et de mise en œuvre dans les systèmes en cours de développement. Des systèmes ou des composants de systèmes semblables pourraient exister au sein des organisations des développeuses et développeurs. De l’information en matière de vulnérabilité est disponible auprès d’une diversité de sources des secteurs privé et public, notamment la National Vulnerability Database du NIST (en anglais seulement).

SA-15(09) — Utilisation de données en temps réel (---)

Énoncés :

Annulé : Intégré au contrôle SA-03(02).

Responsable : Aucun

SA-15(10) — Plan d’intervention en cas d’incident (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s’y rapporte s’assure d’élaborer, de mettre en œuvre et de mettre à l’essai un plan d’intervention en cas d’incident.

Responsable : Aucun

Discussion :

Le plan d’intervention en cas d’incident remis par les développeuses et développeurs peut fournir de l’information qui n’est pas aisément accessible aux organisations et peut être intégrée aux plans d’intervention en cas d’incident de l’organisation. L’information des développeuses et développeurs peut également être extrêmement utile, notamment lorsque les organisations doivent réagir aux vulnérabilités décelées dans les produits COTS.

SA-15(11) — Système ou composant d’archivage (---)

Énoncés :

Exiger que la développeuse ou le développeur d’un système ou d’un composant du système archive le système ou le composant à mettre en service avec les preuves connexes qui appuient l’examen de sécurité et de protection de la vie privée final.

Responsable : Aucun

Discussion :

L’archivage du système ou des composants du système exige que la développeuse ou le développeur conserve les principaux artéfacts de développement, ce qui comprend les spécifications du matériel, le code source, le code objet et les documents pertinents du processus de développement susceptibles de fournir une configuration de référence facilement accessible pour les mises à niveau ou les modifications du système et des composants.

SA-15(12) — Réduction des renseignements personnels (---)

Énoncés :

Exiger que la développeuse ou le développeur du système ou du composant du système limite l'utilisation de renseignements personnels dans les environnements de développement et de test.

Responsable : Aucun

Discussion :

Les organisations peuvent minimiser le risque qui pèse sur la vie privée des individus en faisant appel à des techniques comme la dépersonnalisation ou les données synthétiques. Limiter l'utilisation de renseignements personnels dans les environnements de développement et de test aide à réduire le niveau de risque d'atteinte à la vie privée créé par un système.

SA-15(13) — Syntaxe de journalisation (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte utilise [Affectation : format de journalisation sécurisée défini par l'organisation] pour journaliser [Affectation : types d'événements définis par l'organisation] au [Affectation : niveau de détail défini par l'organisation].

Responsable : Aucun

Discussion :

Pour assurer une intervention plus efficace en cas d'incident et permettre de rétablir plus rapidement les actions liées à la sécurité, il convient d'établir des exigences précises pour la journalisation sécurisée et de faire en sorte qu'il soit facile d'associer les données opérationnelles aux journaux d'événements de vérification produits par les applications. Les types d'événements sont conformes à ceux définis au contrôle AU-02.

SA-16 — Formation offerte par la développeuse ou le développeur (---)

Énoncés :

Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou d'un service qui s'y rapporte fournisse la formation portant sur l'utilisation et l'exploitation adéquates des fonctions, des contrôles et des mécanismes de sécurité et de protection de la vie privée mis en œuvre : [Affectation : formation définie par l'organisation].

Responsable : Aucun

Discussion :

La formation fournie par la développeuse ou le développeur concerne les développeuses et développeurs externes et internes (de l'organisation en question). L'efficacité des contrôles mis en œuvre dans les systèmes de l'organisation repose sur la formation du personnel. Il peut s'agir d'une formation en ligne et assistée par ordinateur, d'une formation en classe ou d'une formation pratique (comme une microformation). Les organisations peuvent également demander que les développeuses et développeurs fournissent du matériel de formation afin d'offrir des options de formation en interne ou d'autoformation à leurs personnels respectifs. Les organisations établissent le type de formation qui répond à leurs besoins et peuvent demander divers types de formation selon les fonctions, les contrôles ou les mécanismes de sécurité et de protection de la vie privée visés.

SA-17 — Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte produise des spécifications de conception et une architecture de sécurité et de protection de la vie privée qui :
a. est conforme à l'architecture de sécurité et de protection de la vie privée de l'organisation qui fait partie intégrante de l'architecture d'entreprise de l'organisation
b. décrit intégralement et précisément les fonctions de sécurité et de protection de la vie privée requises ainsi que l'attribution des contrôles de sécurité parmi les composants physiques et logiques
c. expose comment les fonctions de sécurité et de protection de la vie privée, les mécanismes et les services fonctionnent ensemble pour fournir les capacités de sécurité requises et favoriser une approche coordonnée en matière de protection

Responsable : Aucun

Discussion :

L'architecture de sécurité et de protection de la vie privée et la conception des développeuses et développeurs concernent les développeuses et développeurs externes, mais elles pourraient également être appliquées au développement interne. Par opposition, le contrôle PL-08 vise d'abord les développeuses et développeurs internes de façon à ce que les organisations puissent développer une architecture de sécurité et de protection de la vie privée qui s'intègre à l'architecture d'entreprise. La distinction entre les contrôles SA-17 et PL-08 est particulièrement importante lorsque les organisations externalisent le développement des systèmes, des composants de système ou des services qui s'y rapportent et lorsqu'il est impératif de démontrer l'uniformité de l'architecture d'entreprise et celle de sécurité et de protection de la vie privée de l'organisation. Les documents 15408-2 et 15408-3 de l'ISO/IEC, et l'ITSP.10.037, Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes du CCC, fournissent de l'information sur l'architecture et la conception de la sécurité, notamment des modèles de stratégies officiels, des composants relatifs à la sécurité, de la correspondance formelle et informelle, une conception simple et la façon de structurer le droit d'accès minimal et la mise à l'essai.

SA-17(01) — Modèle formel de stratégie (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de :
a. produire, en parfaite intégration avec le processus de développement, un modèle formel de stratégie décrivant [Affectation : éléments de stratégie organisationnelle de sécurité désignés par l'organisme] à mettre en œuvre
b. démontrer que le modèle formel de stratégie est cohérent et suffisant pour appliquer les dispositions de la stratégie organisationnelle de sécurité dès lors que celle-ci est en vigueur

Responsable : Aucun

Discussion :

Les modèles formels décrivent des comportements particuliers ou des stratégies de sécurité et de protection de la vie privée en langage formel, ce qui permet de prouver l'adéquation de ces comportements et de ces stratégies de façon formelle. Tous les composants de systèmes ne peuvent pas forcément être modélisés. En règle générale, les spécifications formelles concernent des stratégies ou des comportements particuliers qui revêtent un certain intérêt, comme des stratégies de contrôles d'accès non discrétionnaires. Pour ce qui est du modèle formel de stratégie, les organisations choisissent un langage et une approche en se fondant sur la nature des stratégies et des comportements devant être décrits et sur les outils disponibles.

SA-17(02) — Composants servant à la sécurité (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de :
a. définir le matériel, les logiciels et les micrologiciels servant à la sécurité
b. fournir un argumentaire démontrant l'exhaustivité de la définition du matériel, des logiciels et des micrologiciels de sécurité

Responsable : Aucun

Discussion :

Dans le cas d'un système, d'un composant de système ou d'un service qui s'y rapporte, le matériel, les logiciels et les micrologiciels servant à la sécurité forment la partie dont le fonctionnement adéquat sera garant des propriétés de sécurité qui sont exigées.

SA-17(03) — Correspondance formelle (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de :
a. produire, en parfaite intégration avec le processus de développement, des spécifications formelles de haut niveau qui décrivent les interfaces du matériel, des logiciels et des micrologiciels servant à la sécurité sur le plan des exceptions, des messages d'erreur et des effets
b. montrer – par des preuves accessibles et, s'il y a lieu, par des démonstrations informelles – que les spécifications de haut niveau sont conformes au modèle formel de stratégie
c. montrer, par des démonstrations informelles, que les spécifications formelles de haut niveau prennent en compte toutes les interfaces du matériel, des logiciels et des micrologiciels servant à la sécurité
d. montrer que les spécifications formelles de haut niveau décrivent précisément le matériel, les logiciels et les micrologiciels utilisés à des fins de sécurité
e. décrire les mécanismes liés au matériel, aux logiciels et aux micrologiciels servant à la sécurité qui ne sont pas explicitement pris en compte dans les spécifications formelles de haut niveau, mais qui sont inhérents à ce matériel, à ces logiciels et à ces micrologiciels servant à la sécurité

Responsable : Aucun

Discussion :

La correspondance est un élément important de l'assurance gagnée en cours de modélisation. Elle démontre que la mise en œuvre constitue une transformation précise du modèle, et que tout code ou détail de mise en œuvre additionnel n'aura aucune incidence sur les comportements ou sur les stratégies en cours de modélisation. Les méthodes formelles peuvent être utilisées pour montrer que la description formelle d'un système est conforme aux propriétés de sécurité de haut niveau, et que la description formelle de système est adéquatement mise en œuvre, et ce, par la description d'un niveau inférieur, notamment la description des composants matériels. La cohérence entre les spécifications formelles de haut niveau et les modèles formels de stratégies est généralement impossible à prouver hors de tout doute. Par conséquent, une combinaison de méthodes formelles et informelles pourrait être requise pour démontrer la cohérence. La cohérence entre les spécifications de haut niveau et la mise en œuvre pourraient nécessiter l'utilisation de démonstrations informelles en raison des contraintes liées à l'applicabilité des méthodes formelles dans le but de prouver que les spécifications sont intégralement conformes à la mise en œuvre. Les mécanismes liés au matériel, aux logiciels et aux micrologiciels, qui sont strictement inhérents aux composants servant à la sécurité, comprennent les registres de mappage, ainsi que les entrées et sorties directes liées à la mémoire.

SA-17(04) — Correspondance informelle (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de :
a. produire, en parfaite intégration avec le processus de développement, des spécifications descriptives informelles de haut niveau qui décrivent les interfaces du matériel, des logiciels et des micrologiciels servant à la sécurité sur le plan des exceptions, des messages d'erreur et des effets
b. montrer par [Sélection (un choix) : démonstration informelle; arguments convaincants fournis, si possible, par des méthodes formelles] que les spécifications descriptives de haut niveau sont conformes au modèle formel de stratégie
c. montrer, par des démonstrations informelles, que les spécifications descriptives de haut niveau prennent en compte toutes les interfaces du matériel, des logiciels et des micrologiciels servant à la sécurité
d. montrer que les spécifications descriptives de haut niveau décrivent précisément les interfaces du matériel, des logiciels et des micrologiciels servant à la sécurité
e. décrire les mécanismes liés au matériel, aux logiciels et aux micrologiciels servant à la sécurité qui ne sont pas explicitement pris en compte dans les spécifications descriptives de haut niveau, mais qui sont strictement inhérents à ce matériel, à ces logiciels et à ces micrologiciels servant à la sécurité

Responsable : Aucun

Discussion :

La correspondance est un élément important de l'assurance gagnée en cours de modélisation. Elle démontre que la mise en œuvre constitue une transformation précise du modèle, et que le code ou le détail de mise en œuvre additionnel n'aura aucune incidence sur les comportements ou les stratégies en cours de modélisation. La cohérence entre les spécifications descriptives de haut niveau (par exemple, une conception de haut niveau ou de bas niveau) et le modèle formel de stratégie est généralement impossible à prouver hors de tout doute. Par conséquent, une combinaison de méthodes formelles et informelles pourrait être requise pour démontrer la cohérence. Les mécanismes liés au matériel, aux logiciels et aux micrologiciels, qui sont strictement inhérents au matériel, aux logiciels et aux micrologiciels servant à la sécurité, comprennent les registres de mappage, ainsi que les entrées et sorties directes liées à la mémoire.

SA-17(05) — Conception simple (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de :
a. concevoir et structurer le matériel, les logiciels et les micrologiciels servant à la sécurité de façon à créer un mécanisme de protection complet, de conception simple et doté d'une sémantique précisément définie
b. structurer en interne le matériel, les logiciels et les micrologiciels servant à la sécurité, en portant une attention particulière au mécanisme en question

Responsable : Aucun

Discussion :

Le principe de complexité réduite repose sur le fait que la conception du système est aussi simple et petite que possible (voir le contrôle SA-08(07)). Une conception petite et simple est plus facile à comprendre et à analyser, en plus d'être moins vulnérable aux erreurs (voir les contrôles AC-25 et SA-08(13)). Le principe de complexité réduite s'applique à tous les aspects d'un système, mais il est particulièrement important pour la sécurité en raison des diverses analyses réalisées pour obtenir des preuves de la propriété de sécurité émergente du système. Pour assurer la réussite de telles analyses, il est essentiel de faire appel à une conception simple et de petite taille. L'application du principe de complexité réduite aide les développeuses et développeurs de système à comprendre l'exactitude et l'exhaustivité des fonctions de sécurité du système et à faciliter la détermination des vulnérabilités potentielles. La conséquence de la complexité réduite veut que la simplicité du système soit directement liée au nombre de vulnérabilités qu'il contiendr
a. En d'autres mots, les systèmes plus simples contiennent moins de vulnérabilités. Deux avantages importants de la complexité réduite font en sorte qu'il soit plus facile de comprendre si la stratégie de sécurité a bien été intégrée dans la conception du système et qu'il y ait moins de vulnérabilités susceptibles d'être introduites lors du processus de développement technique. Ce principe permet également de rendre des conclusions par rapport à l'exactitude, à l'exhaustivité et à l'existence des vulnérabilités avec un degré élevé d'assurance comparativement aux conclusions formulées dans des situations où la conception du système est fondamentalement plus complexe.

SA-17(06) — Structure de mise à l'essai (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant de système ou du service qui s'y rapporte structure le matériel, les logiciels et les micrologiciels servant à la sécurité de manière à faciliter la mise à l'essai.

Responsable : Aucun

Discussion :

L'application des principes du développement sécurisé abordés dans le document SP 800-160 Volume 1 Revision 1 du NIST (en anglais seulement) et dans le cadre de développement mentionné dans l'ITSP.10.037, Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes du CCC permet de favoriser une mise à l'essai et une évaluation complètes, uniformes et exhaustives des systèmes, des composants de systèmes et des services. L'exhaustivité d'une telle mise à l'essai contribue aux preuves produites pour créer un cas ou un argument d'assurance efficace par rapport à la robustesse du système, du composant du système ou du service.

SA-17(07) — Structure relative au droit d’accès minimal (---)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant de système ou du service qui s’y rapporte structure le matériel, les logiciels et les micrologiciels servant à la sécurité de manière à faciliter le contrôle de l’accès avec le droit d’accès minimal.

Responsable : Aucun

Discussion :

Le principe de droit d’accès minimal repose sur le fait que l’on doit affecter suffisamment de privilèges à chaque composant pour lui permettre d’accomplir ses fonctions, mais sans plus (voir le contrôle SA-08(14)). L’application du principe de droit d’accès minimal limite la portée des actions du composant, ce qui a deux effets désirables. Dans un premier temps, l’incidence sur la sécurité advenant la défaillance, la corruption ou une mauvaise utilisation du composant du système est limitée. Dans un second temps, l’analyse de la sécurité du composant est simplifiée. Le principe de droit d’accès minimal est un principe omniprésent qui se reflète dans tous les aspects de la conception d’un système sécurisé. Les interfaces utilisées pour appeler les capacités du composant ne sont accessibles que par certains sous-ensembles de la population d’utilisatrices et utilisateurs, et la conception du composant prend en charge un degré de granularité suffisamment précis pour assurer la décomposition des privilèges. Par exemple, dans le cas d’un mécanisme de vérification, on pourrait retrouver une interface pour la ou le gestionnaire des vérifications qui configure les paramètres des vérifications, une interface pour l’exploitante ou exploitant des vérifications qui s’assure que les données de vérification sont collectées et stockées en toute sécurité et, pour finir, une autre interface pour la vérificatrice ou le vérificateur des vérifications qui doit afficher les données de vérification collectées sans toutefois effectuer d’opérations à partir de ces données. En plus de ses manifestations dans l’interface du système, le principe de droit d’accès minimal peut être utilisé comme principe directeur pour la structure interne du système en tant que tel. Un aspect du droit d’accès minimal interne est de construire des modules de manière à ce que seules les fonctions d’un module puissent effectuer des opérations directes sur les éléments encapsulés par ce module. Il est possible d’accéder indirectement aux éléments externes à un module susceptibles d’être touchés par l’exploitation de ce module dans le cadre d’une interaction (par exemple, lors d’un appel de fonction) avec le module qui contient ces éléments. Un autre aspect du droit d’accès minimal interne veut que la portée d’un module ou d’un composant donné comprenne uniquement les éléments du système qui sont nécessaires pour son fonctionnement et que les modes d’accès des éléments (par exemple, lecture, écriture) soient minimaux.

SA-17(08) — Orchestration (---)

Énoncés :

Concevoir [Affectation : systèmes ou composants de systèmes critiques désignés par l'organisation] avec un comportement coordonné pour mettre en œuvre les capacités suivantes : [Affectation : capacités définies par l'organisation, par système ou composant].

Responsable : Aucun

Discussion :

Les ressources de sécurité distribuées qui se trouvent à différentes couches ou dans différents éléments des systèmes peuvent interagir de façon imprévue ou inappropriée. Les conséquences négatives peuvent comprendre des défaillances en cascade, des interférences ou des lacunes dans la couverture. La coordination du comportement des ressources de sécurité (par exemple, en s'assurant qu'un correctif est appliqué à toutes les ressources avant d'apporter un changement dans la configuration qui suppose que le correctif a été installé) peut éviter de telles interactions négatives.

SA-17(09) — Diversité de la conception (---)

Énoncés :

Utiliser les différentes conceptions de [Affectation : systèmes ou composants de systèmes critiques désignés par l'organisation] pour satisfaire à un ensemble commun d'exigences ou fournir une fonctionnalité équivalente.

Responsable : Aucun

Discussion :

La diversité de conception repose sur l'imposition des mêmes exigences à plusieurs développeuses et développeurs, chacun étant responsable de développer une variante du système ou du composant du système qui répond à ces exigences. Les variantes peuvent se trouver dans la conception du logiciel, dans la conception du matériel ou dans la conception du logiciel et du matériel. Les différences dans les conceptions des variantes peuvent découler de l'expérience des développeuses et développeurs (par exemple, avant l'utilisation d'un schéma de conception), du style de conception (par exemple, au moment de décomposer une fonction obligatoire en plus petites tâches, déterminer ce qui constitue une tâche distincte et jusqu'où il convient de décomposer les tâches en sous-tâches), de la sélection des bibliothèques à intégrer dans la variante et de l'environnement de développement (par exemple, différents outils de conception facilitent la visualisation des schémas de conception). La diversité de la conception du matériel consiste notamment à prendre différentes décisions concernant l'information qu'il convient de conserver sous forme analogique et de convertir sous forme numérique, à transmettre la même information à différents moments et à introduire des délais dans l'échantillonnage (diversité temporelle). La diversité de la conception est souvent utilisée pour prendre en charge la tolérance aux anomalies.

SA-18 — Résistance au trafiquage et détection (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-09.

Responsable : Aucun

SA-18(01) — Multiples phases du cycle de développement de systèmes (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-09(01).

Responsable : Aucun

SA-18(02) — Inspection des systèmes ou des composants (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-10.

Responsable : Aucun

SA-19 — Authenticité des composants (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-11.

Responsable : Aucun

SA-19(01) — Formation anticontrefaçon (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-11(01).

Responsable : Aucun

SA-19(02) — Contrôle des configurations pour l'entretien et la réparation des composants (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-11(02).

Responsable : Aucun

SA-19(03) — Mise hors service des composants (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-12.

Responsable : Aucun

SA-19(04) — Analyse anticontrefaçon (---)

Énoncés :

Annulé : Transféré sous le contrôle SR-11(03).

Responsable : Aucun

SA-20 — Développement sur mesure des composants essentiels (---)

Énoncés :

Procéder à une nouvelle mise en œuvre ou au développement sur mesure des composants de systèmes essentiels suivants : [Affectation : composants essentiels désignés par l'organisation].

Responsable : Aucun

Discussion :

Les organisations déterminent que certains composants de systèmes ne peuvent vraisemblablement pas être considérés comme fiables en raison de certaines menaces ou de vulnérabilités inhérentes, et que ces mêmes composants ne disposent pas de contrôles de sécurité aptes à atténuer raisonnablement les risques. La remise en œuvre ou le développement sur mesure de tels composants peut satisfaire aux exigences d'assurance élevée et être accompli en apportant des changements aux composants de systèmes (y compris le matériel, les logiciels et les micrologiciels) pour faire en sorte que les attaques courantes des adversaires aient peu de chances de réussir. Dans les cas où aucune autre source n'est disponible et que les organisations décident de ne pas procéder à la remise en œuvre ou au développement sur mesure des composants de systèmes essentiels, des contrôles additionnels peuvent être employés. Les contrôles comprennent une vérification accrue, des restrictions d'accès au code source et aux utilitaires du système et la protection contre la suppression des fichiers système et d'application.

SA-21 — Filtrage de sécurité des développeuses et développeurs (---)

Énoncés :

Exiger que la développeuse ou le développeur de [Affectation : système, composant de système ou service qui s'y rapporte désigné par l'organisation] :
a. dispose des autorisations d'accès requises en fonction des [Affectation : responsabilités gouvernementales officielles définies par l'organisation] qui ont été attribuées
b. satisfasse aux critères additionnels de filtrage de sécurité du personnel définis par l'organisation : [Affectation : critères additionnels de sélection du personnel définis par l'organisation]

Responsable : Aucun

Discussion :

Le filtrage de sécurité des développeuses et développeurs concerne les développeurs externes. Le filtrage de sécurité des développeuses et développeurs internes est abordé dans le contrôle PS-

> **03.** Puisque les systèmes, les composants de systèmes ou les services qui s'y rapportent peuvent être employés dans le cadre d'activités de nature critique qui s'avèrent essentielles à la protection des intérêts du Québec en matière de sécurité ou économique, il est primordial que les organisations s'assurent que les développeuses et développeurs soient dignes de confiance. Il se pourrait que le niveau de fiabilité des développeuses et développeurs doive correspondre à celui des autres personnes ayant accès aux systèmes, aux composants ou aux services après le déploiement. Les habilitations de sécurité, les vérifications des antécédents, la citoyenneté et la nationalité sont des exemples de critères d'autorisation d'accès ou de filtrage de sécurité du personnel. La vérification de la fiabilité des développeuses et développeurs peut également nécessiter l'examen et l'analyse des titres de propriété ainsi que des relations que l'entreprise entretient avec des entités pouvant interférer avec la qualité ou la fiabilité des systèmes, des composants ou des services en cours de développement. Le fait de respecter les critères visant les autorisations d'accès et le filtrage de sécurité du personnel se manifeste par la production de listes des personnes autorisées à mener des activités de développement sur les divers systèmes, composants de systèmes et/ou services qui s'y rapportent, de façon à permettre aux organisations d'établir si une développeuse ou un développeur répond aux exigences relatives aux autorisations d'accès et au filtrage de sécurité.

SA-21(01) — Validation du filtrage de sécurité (---)

Énoncés :

Annulé : Intégré au contrôle SA-21.

Responsable : Aucun

SA-22 — Composants de systèmes non pris en charge (Nc--)

Énoncés :

a. Remplacer les composants des systèmes lorsqu'ils ne sont plus pris en charge par les développeuses, les développeurs, les fournisseurs ou les fabricants
b. Offrir les options suivantes pour les solutions de rechange visant à assurer la continuité du soutien des composants non pris en charge faisant l'objet d'un [Sélection (un choix ou plus) : soutien interne; {Affectation : soutien offert par des fournisseurs externes défini par l'organisation}]

Responsable : Aucun

Discussion :

La prise en charge (ou le soutien) des composants de systèmes comprend les correctifs logiciels, les mises à jour de micrologiciels, les remplacements de pièces et les contrats de maintenance. Les exemples de composants non pris en charge comprennent les circonstances où les fournisseurs ne produisent plus de correctifs logiciels critiques ou de mises à jour pour les produits, ce qui peut mener à des possibilités pour les adversaires d'exploiter les faiblesses des composants installés. Les exceptions au remplacement des composants de systèmes non pris en charge comprennent les systèmes qui fournissent des capacités essentielles à la mission ou aux activités lorsque des technologies plus récentes ne sont pas disponibles ou lorsque les systèmes sont tellement isolés qu'il est impossible d'installer des composants de remplacement. Les autres sources de soutien permettent de répondre au besoin de fournir un soutien continu pour les composants de systèmes qui ne sont plus pris en charge par les fabricants d'origine, les développeuses, les développeurs ou les fournisseurs lorsque ces composants sont essentiels à la mission et aux activités de l'organisation. Au besoin, les organisations peuvent établir un soutien interne en développant des correctifs sur mesure pour les composants logiciels critiques ou avoir recours à des services de fournisseurs externes capables de fournir, au moyen de relations contractuelles, du soutien continu pour les composants non pris en charge qui ont été désignés. Ces relations contractuelles peuvent comprendre des fournisseurs de logiciels libres à valeur ajoutée. Le risque accru d'utilisation de composants de systèmes non pris en charge peut être atténué, par exemple, en empêchant la connexion de ces composants aux réseaux publics ou non contrôlés ou en mettant en oeuvre d'autres formes d'isolation.

SA-22(01) — Solution de rechange visant à assurer la continuité du soutien (---)

Énoncés :

Annulé : Intégré au contrôle SA-22.

Responsable : Aucun

SA-23 — Spécialisation (---)

Énoncés :

Avoir recours [Sélection (un choix ou plus) : à la conception; à la modification; au renforcement; à la reconfiguration] des [Affectation : systèmes ou composants de systèmes désignés par l'organisation] prenant en charge des services ou des fonctions essentiels à la mission pour renforcer la robustesse de ces systèmes ou composants.

Responsable : Aucun

Discussion :

Il est souvent nécessaire d'améliorer un système ou un composant de système qui prend en charge des fonctions ou des services essentiels à la mission pour maximiser la robustesse de la ressource. Parfois, cette amélioration est effectuée au niveau de la conception. Dans d'autres cas, elle est réalisée au cours de la phase postconception, que ce soit en modifiant le système concerné ou en renforçant le système au moyen de composants additionnels. Par exemple, des fonctions supplémentaires d'authentification ou de non-répudiation peuvent être ajoutées au système pour renforcer l'identité des ressources critiques selon les autres ressources qui dépendent de ressources définies par l'organisation.

SA-24 — Conception aux fins de cyberrésilience (---)

Énoncés :

a. Concevoir les systèmes organisationnels, les composants de systèmes ou les systèmes qui s'y rapportent de manière à renforcer leur cyberrésilience en définissant :

1. les buts suivants en matière de cyberrésilience : [Affectation : buts en matière de cyberrésilience définis par l'organisation]

2. les objectifs suivants en matière de cyberrésilience : [Affectation : objectifs en matière de cyberrésilience définis par l'organisation]

3. les techniques de cyberrésilience suivantes : [Affectation : techniques de cyberrésilience définies par l'organisation]

4. les approches de mise en oeuvre de la cyberrésilience suivantes : [Affectation : approches de mise en oeuvre de la cyberrésilience définies par l'organisation]

5. les principes de conception de la cyberrésilience suivants : [Affectation : principes de conception de la cyberrésilience définis par l'organisation]

b. Mettre en oeuvre et passer en revue les buts, les objectifs, les techniques, les approches de mise en oeuvre et les principes de conception dans le cadre du processus de gestion des risques organisationnels ou du processus d'ingénierie de la sécurité des systèmes

Responsable : Aucun

Discussion :

La cyberrésilience est essentielle pour assurer la survivance des systèmes essentiels à la mission et des biens de grande valeur. La cyberrésilience met l'accent sur la limitation des dommages causés par l'adversité ou des conditions susceptibles de mener à la perte des biens. Les dommages peuvent toucher (1) les organisations (par exemple, une atteinte à la réputation, de plus grands risques existentiels), (2) les fonctions liées à la mission ou aux activités de l'organisation (par exemple, une capacité réduite de mener à bien les missions en cours et celles à venir), (3) la sécurité (par exemple, une capacité réduite d'atteindre les objectifs en matière de sécurité ou de prévenir les cyberincidents, de les détecter et d'y réagir), (4) les systèmes (par exemple, l'utilisation non autorisée des ressources du système ou une capacité réduite de se conformer aux exigences système) ou (5) les éléments propres au système (par exemple, la destruction physique, la corruption, la modification ou la fabrication d'informations). La cyberrésilience vise à aider les organisations à maintenir un état de préparation éclairé face à l'adversité, à mener à bien les fonctions essentielles liées à la mission ou aux activités en dépit d'incidents négatifs, à rétablir les fonctions liées à la mission ou aux activités durant et après ces incidents et à modifier les fonctions liées à la mission ou aux activités et leurs capacités de soutien advenant des changements prévus dans les environnements techniques, opérationnels et de menace. Le document SP 800-160 Volume 2 Revision 1 du NIST fournit de l'information additionnelle sur le cadre d'ingénierie de la cyberrésilience, dont des descriptions détaillées des buts, des objectifs, des techniques, des approches de mise en oeuvre et des principes de conception de la cyberrésilience. Le document SP 800-160 Volume 1 Revision 1 du NIST fournit de l'information additionnelle sur l'atteinte de la cyberrésilience en tant que propriété émergente d'un système en cours de conception.

SA-400 — Souveraineté et juridiction (---)

Énoncés :

Exiger que les fonctions opérationnelles de l'organisation respectent un processus d'évaluation des menaces et des risques en matière de souveraineté et de juridiction au [Sélection (un choix ou plus) : niveau de l'organisation; niveau de la mission et des activités; niveau du système] qui consiste à :
a. procéder à l'évaluation des préjudices pour déterminer les préjudices potentiels maximaux qui pourraient être causés par une contrainte légale externe imposée aux fonctions organisationnelles ou aux ressources informationnelles en :
    1. considérant les besoins opérationnels en matière de sécurité, y compris les lois ou la réglementation qui exigent que les données ne soient pas divulguées ou compromises
    2. mettant à jour la catégorisation de la sécurité des fonctions organisationnelles ou des ressources informationnelles
    3. documentant les conséquences négatives de la contrainte légale
b. procéder à l'évaluation des menaces propres à la juridiction pour établir la probabilité d'être pris pour cible
c. effectuer une évaluation des vulnérabilités pour déterminer les moyens potentiels que la juridiction externe pourrait utiliser pour exploiter les fonctions organisationnelles ou les ressources informationnelles
d. procéder à l'évaluation des risques propres à la juridiction

Responsable : Aucun

Discussion :

La souveraineté des données concerne le droit du Québec de contrôler l'accès à l'information numérique qui est assujetti à un contrôle prévu par la loi et la divulgation d'une telle information. Par résidence des données, on entend l'emplacement physique ou géographique des données au repos d'une organisation. Par juridiction, on entend le domaine d'autorité qui, dans ce contexte, fait référence à la capacité d'imposer la conformité des entités dans ce domaine comme menace principale. L'hébergement de données dans une juridiction étrangère suscite des préoccupations dans la mesure où ces données pourraient être observées, modifiées ou refusées dans le cadre d'une contrainte légale, alors que ça ne devrait pas être le cas lorsqu'une organisation jouit de la souveraineté de ses données. L'exposition d'une fonction organisationnelle à une compétence juridique différente peut en fait éliminer les barrières juridiques souveraines qui protègent contre la compromission dans la juridiction d'origine. Par exemple, la protection de la vie privée des citoyennes et citoyens n'est souvent pas accordée aux non-citoyennes et non-citoyens, et les fournisseurs de services peuvent être légalement tenus de fournir l'accès à des données ou à des services qui seraient protégés par la loi dans la juridiction d'origine. Dans le cas des fonctions organisationnelles, on peut donner en exemple la technologie opérationnelle qui contrôle les infrastructures essentielles hébergées dans un nuage qui est modifié ou mis hors service par une juridiction étrangère hostile. Les techniques employées peuvent être très sophistiquées et seront généralement exécutées avec tous les privilèges d'administrateur des initiées et initiés. La contrainte légale imposée par des juridictions dotées de moyens sophistiqués est extrêmement efficace pour ce qui est de contourner les autres contrôles. Plusieurs juridictions peuvent s'appliquer, par exemple une administration municipale, une ville, un comté, une réserve, un district, une région, une province, un État, un canton, un territoire ou une nation. Tous les niveaux doivent être identifiés pour évaluer les capacités d'imposer des contraintes. D'autres juridictions peuvent forcer la compromission des fonctions opérationnelles en matière de confidentialité, d'intégrité ou de disponibilité. Une évaluation des préjudices doit documenter les conséquences négatives de la contrainte légale, notamment tout besoin opérationnel en matière de sécurité (par exemple, les lois ou la réglementation qui exigent que les données ne soient pas compromises). Une organisation pourrait ne pas être en mesure d'adopter une approche à la gestion des risques (notamment en raison d'un mandat prescrit par la loi ou de la souveraineté des données nationales) et devoir éviter d'emblée tout scénario de risque.

SA-400(01) — Évaluation des menaces et des risques (---)

Énoncés :

Exiger que l'organisation effectue des évaluations des menaces et des risques qui pèsent sur la souveraineté des données en tenant compte de sa juridiction et des aspects pour lesquels des contraintes légales pourraient être efficaces.

Responsable : Aucun

Discussion :

L'organisation détermine la valeur du préjudice causé par les fonctions opérationnelles proposées pour occuper d'autres juridictions. Les quatre surfaces (logique, physique, personnel et cycle de vie) abordées dans le document Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes (ITSP.10.037) peuvent être vulnérables.

SA-400(02) — Évaluation d'ordre juridique et contractuel (---)

Énoncés :

Évaluer l'assurance de la sécurité des processus opérationnels au moyen de mécanismes juridiques ou de passation de marché.

Responsable : Aucun

Discussion :

Plusieurs juridictions offrent différentes possibilités pour protéger les fonctions opérationnelles contre la contrainte légale à divers niveaux d'assurance. Des accords internationaux et multilatéraux peuvent aider à accroître la protection. Les modalités des marchés conclus avec les fournisseurs peuvent aider à réduire l'exposition à de telles contraintes ou en faire le signalement (il importe de souligner que certaines formes de contrainte peuvent également interdire toute forme de non-divulgation). Dans la mesure où la prestation de service comporte des fournisseurs de tierces parties, s'assurer que les documents contractuels font mention de la souveraineté des données et des obligations en matière de juridiction. Si les organisations décident d'aborder les obligations en matière de souveraineté et de juridiction au niveau de l'organisation ou du projet, cette obligation devrait être incluse dans les obligations contractuelles connexes. Les organisations devraient obtenir les conseils de spécialistes dans la juridiction cible si des mécanismes juridiques et contractuels sont employés pour prévenir toute contrainte légale étrangère, puisqu'il est probable que toute législation à caractère obligatoire ait préséance sur les mesures législatives ou les contrats de protection. Ce qui constitue une application régulière de la loi dans d'autres juridictions peut être insatisfaisant d'un point de vue fédéral ou provincial.

SA-400(03) — Marquage des attributs liés aux processus opérationnels (---)

Énoncés :

S'assurer que les processus opérationnels fassent l'objet du traitement prévu selon la compétence juridique.

Responsable : Aucun

Discussion :

Les attributs des métadonnées peuvent être définis et liés aux processus opérationnels ou aux données pour aider les processus de gestion à traiter correctement la compétence juridique prévue. Par exemple, la mention « Réservé aux juridictions canadiennes » ou « Données nationales souveraines » peut être apposée sur les documents comme attribut. Le traitement automatisé des attributs de métadonnées peut être d'une grande aide pour les fournisseurs d'infrastructures partagées qui doivent respecter une multiplicité d'exigences en matière de compétences.

SA-400(04) — Protection des données au repos (---)

Énoncés :

Éviter que les données résident dans des territoires qui relèvent d'autres compétences juridiques.

Responsable : Aucun

Discussion :

Permettre aux données au repos de résider dans d'autres juridictions fournit la plus grande occasion d'imposer à tout moment une contrainte sur les données. Héberger les données au repos dans des juridictions canadiennes augmentera le facteur travail et pourrait éliminer certaines capacités. Le chiffrement des données au repos offre une valeur limitée, mais pourrait permettre de prévenir la récupération physique des données avec une certaine efficacité. Il n'y a aucun délai minimum après lequel les données sont considérées « au repos ». Si les données doivent être écrites, même momentanément, sur un support non volatile, elles doivent être considérées comme étant au repos. Cela peut notamment avoir une incidence sur les situations d'urgence ou imprévues, comme des vidages de la mémoire, la mise en cache ou la permutation de la mémoire, ainsi que sur les opérations de reprise après sinistre. Les considérations relatives aux données au repos doivent également tenir compte de la façon dont les données stockées seront éventuellement mises hors service et éliminées afin de s'assurer que les données ne fassent pas l'objet d'une contrainte étrangère à la fin de la durée de vie du système.

SA-400(05) — Protection des données en transit (---)

Énoncés :

Éviter que les données transitent par des territoires qui relèvent d'autres compétences juridiques.

Responsable : Aucun

Discussion :

Permettre aux données en transit de traverser d'autres juridictions fournit de nombreuses occasions de contraindre les données. Le fait d'acheminer les données dans des juridictions canadiennes uniquement élimine plusieurs capacités de contrainte. Le chiffrement des données en transit peut également s'avérer utile.

SA-400(06) — Protection des données en cours d'utilisation (---)

Énoncés :

Éviter que les données soient utilisées dans des territoires qui relèvent d'autres compétences juridiques.

Responsable : Aucun

Discussion :

Permettre aux données en cours d'utilisation de résider dans d'autres juridictions fournit une occasion de contraindre les données. Le fait de traiter les données dans des juridictions canadiennes uniquement élimine plusieurs capacités de contrainte. Aucune méthode de chiffrement n'a encore été approuvée pour protéger les données en cours d'utilisation. En principe, une forme de chiffrement connue sous le nom de « chiffrement homomorphique » pourrait permettre certains types de traitement alors que les données restent chiffrées, mais le Centre pour la cybersécurité ne considère pas pour l'instant que le chiffrement homomorphique est suffisant pour assurer le chiffrement conformément à son document Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111). Par conséquent, si le chiffrement homomorphique est employé pour protéger les données en cours d'utilisation, il convient actuellement de l'évaluer en tant que texte en clair (c'est-à-dire n'offrant aucune protection cryptographique selon le contrôle SC-13). Il n'y a aucun délai minimum après lequel les données sont considérées en cours d'utilisation. Leur présence dans un système pour un seul cycle d'UCT devrait suffire pour l'imposition d'une contrainte.

SA-400(07) — Protection contre les contraintes extraterritoriales (---)

Énoncés :

Prévenir la compromission des fonctions opérationnelles par des personnes ou des sociétés assujetties à une autre compétence juridique.

Responsable : Aucun

Discussion :

Les adversaires peuvent avoir des moyens de forcer les personnes et/ou les sociétés à compromettre les fonctions opérationnelles même si l'intégralité de ces fonctions est conservée à l'extérieur de la juridiction de l'adversaire. Il convient de tenir compte de la loyauté des personnes ou des sociétés, des liens directs entre les entités (comme les sociétés affiliées, les membres de la famille, les biens étrangers) et des liens indirects (comme les partenariats et les relations). Les personnes résidant au Canada qui détiennent une citoyenneté canadienne et une citoyenneté étrangère peuvent être contraintes par leur autre pays, même si elles sont assujetties aux lois canadiennes, et pourraient être tenues de choisir entre les conséquences juridiques imposées dans l'une ou l'autre des juridictions.

SA-400(08) — Protection du cycle de vie des activités (---)

Énoncés :

Prévenir la compromission des fonctions opérationnelles dans le cadre d'attaques du cycle de vie découlant d'une contrainte légale ou menées depuis une autre compétence juridique.

Responsable : Aucun

Discussion :

L'utilisation de produits ou de services (par exemple, des logiciels, des micrologiciels, du matériel, des services de conception, des services de consultations, etc.) qui ont déjà fait l'objet d'une contrainte peut exposer les fonctions opérationnelles aux compromissions inhérentes à ces produits ou services. La plupart des systèmes actuels comportent des éléments tirés de multiples compétences juridiques et une approche basée sur le risque sera nécessaire pour sélectionner les solutions qui permettent d'atténuer les menaces relevées selon les besoins opérationnels en matière de sécurité. Un contrôle compensatoire à mettre en place pour prévenir toute compromission inhérente consiste à assurer une isolation rigoureuse du réseau.

SA-400(09) — Propriété publique (---)

Énoncés :

Prévenir la compromission des fonctions opérationnelles lors d'un transfert de propriété des fonctions du cycle de vie à une autre compétence juridique.

Responsable : Aucun

Discussion :

Bien que les dépendances du système puissent être sécurisées contre une contrainte étrangère dès le début de la mise en œuvre, si un transfert de propriété survient au cours de la durée de vie du système, ce dernier pourrait faire l'objet d'attaques du cycle de vie découlant d'une contrainte étrangère. Pour éviter une telle possibilité, les organisations sélectionnent un soutien au cycle de vie et des arrangements en matière d'approvisionnement qui seront régis par une propriété publique canadienne pour toute la durée de vie du système.

SC

Sécurité des communications et des systèmes

System and Communications Protection

SC-01 — Politique et procédures de protection des systèmes et des communications (---)

Énoncés :

a. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :

1. une politique de protection des systèmes et des communications [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables

2. des procédures pour faciliter la mise en oeuvre de la politique de protection des systèmes et des communications ainsi que des contrôles connexes

c. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures de protection des systèmes et des communications

c. Passer en revue et mettre à jour, par rapport à la protection des systèmes et des communications actuels :

1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La politique et les procédures de protection des systèmes et des communications abordent les contrôles de la famille SC qui ont été mis en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à l'élaboration de la politique et des procédures de protection des systèmes et des communications. En règle générale, les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin de politiques et de procédures propres à la mission ou au système. La politique peut être intégrée à la politique générale de sécurité et de protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures de protection des systèmes et des communications comprennent les conclusions d'une évaluation ou d'une vérification, des incidents touchant à la sécurité ou des violations, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.

SC-02 — Séparation des fonctionnalités d'utilisateur et du système (---)

Énoncés :

Séparer la fonctionnalité d'utilisateur, dont les services d'interface utilisateur, de la fonctionnalité de gestion du système.

Responsable : Aucun

Discussion :

La fonctionnalité de gestion des systèmes comprend les fonctions nécessaires pour administrer les bases de données, les composantes réseau, les stations de travail ou le serveur. Ces fonctions exigent généralement un accès utilisateur privilégié. Les fonctions d'utilisateur sont distinctes des fonctions de gestion des systèmes tant physiquement que logiquement. Les organisations peuvent séparer les fonctions de gestion des systèmes des fonctions d'utilisateur en faisant appel à des ordinateurs différents ou à différentes instances de systèmes d'exploitation, d'unités centrales de traitement ou d'adresses réseau, en employant des techniques de virtualisation ou au moyen d'une combinaison de ces méthodes ou d'autres méthodes. Les interfaces administratives Web, qui utilisent des méthodes d'authentification distinctes pour les utilisatrices et utilisateurs de toute autre ressource du système sont un exemple de séparation des fonctions de gestion des systèmes des fonctions d'utilisateur. La séparation des fonctions d'utilisateur de celles du système peut prévoir l'isolation des interfaces administratives pour certains domaines et l'ajout de contrôles d'accès. On peut réaliser la séparation des fonctionnalités d'utilisateur de celles du système en appliquant les principes de conception technique de la sécurité des systèmes mentionnés au contrôle SA-08, ainsi qu'aux contrôles SA-08(01), SA-08(03), SA-08(04), SA-08(10), SA-08(12), SA-08(13), SA-08(14) et SA-08(18).

SC-02(01) — Interfaces pour les utilisatrices et utilisateurs non privilégiés (---)

Énoncés :

Éviter de présenter la fonctionnalité de gestion des systèmes sur les interfaces destinées aux utilisatrices et utilisateurs non privilégiés.

Responsable : Aucun

Discussion :

Éviter de présenter la fonctionnalité de gestion des systèmes sur les interfaces destinées aux utilisatrices et utilisateurs non privilégiés permet de s'assurer que les options d'administration de systèmes, dont les privilèges d'administrateur, ne sont pas accessibles aux utilisatrices et utilisateurs réguliers. La restriction de l'accès des utilisatrices et utilisateurs interdit le recours aux options grisées communément utilisées pour empêcher l'accès à une telle information. Une solution potentielle consiste à ne pas afficher les options d'administration jusqu'à ce que les utilisatrices et utilisateurs ouvrent une session avec des privilèges d'administrateur.

SC-02(02) — Dissociabilité (---)

Énoncés :

Stocker l'information d'état séparément des applications et des logiciels.

Responsable : Aucun

Discussion :

Advenant la compromission d'un système, le fait de stocker les applications et les logiciels séparément de l'information d'état relative aux interactions des utilisatrices et utilisateurs avec une application permettra de mieux protéger la vie privée des individus.

SC-03 — Isolation des fonctions de sécurité (---)

Énoncés :

Isoler les fonctions de sécurité des autres fonctions.

Responsable : Aucun

Discussion :

Le système isole les fonctions de sécurité des autres fonctions au moyen d'un périmètre d'isolation mis en œuvre à l'aide de partitions et de domaines. Le périmètre d'isolation contrôle l'accès aux composants matériels, logiciels et micrologiciels qui accomplissent les fonctions de sécurité, tout en en assurant leur intégrité. Les systèmes mettent en œuvre la séparation du code de diverses façons, notamment par des noyaux de sécurité qui ont recours à des anneaux de processeurs ou à des modes de processeurs. En ce qui concerne le code hors noyau, l'isolation de la fonction de sécurité est souvent réalisée par des mesures de protection du système de fichiers qui protègent le code sur disque et tiennent compte de la protection des espaces d'adressage, ce qui permet de préserver l'exécution du code. Les systèmes peuvent restreindre l'accès aux fonctions de sécurité en ayant recours à des mécanismes de contrôle des accès et à la mise en œuvre de capacités fondées sur le principe du droit d'accès minimal. Même s'il est largement préférable que l'espace réservé à la fonction de sécurité (isolation) ne contienne que l'intégralité du code ayant trait à la sécurité, il arrive exceptionnellement qu'il soit nécessaire d'ajouter d'autres fonctions. L'isolation des fonctions de sécurité des autres fonctions peut être réalisée en appliquant les principes de conception technique de la sécurité des systèmes mentionnés au contrôle SA-08, ainsi qu'aux contrôles SA-08(01), SA-08(03), SA-08(04), SA-08(10), SA-08(12), SA-08(13), SA-08(14) et SA-08(18).

SC-03(01) — Séparation du matériel (---)

Énoncés :

Avoir recours à des mécanismes de séparation du matériel pour mettre en œuvre l'isolation des fonctions de sécurité.

Responsable : Aucun

Discussion :

Les mécanismes de séparation du matériel comprennent les architectures matérielles en anneau, qui sont mises en œuvre pour les microprocesseurs, ainsi que la segmentation physique des adresses, qui est employée pour assurer le soutien des objets de stockage logiquement différents qui possèdent leurs propres attributs (par exemple, lisible, modifiable).

SC-03(02) — Accès et fonctions de contrôle des flux (---)

Énoncés :

Isoler les fonctions de sécurité appliquant le contrôle de l'accès et du flux d'information des autres fonctions de sécurité et des fonctions non liées à la sécurité.

Responsable : Aucun

Discussion :

L'isolation des fonctions de sécurité est le résultat de la mise en œuvre. Il est toujours possible d'analyser et de surveiller les fonctions. Les fonctions de sécurité qui sont potentiellement isolées des fonctions d'application du contrôle des accès et des flux comprennent les vérifications, la détection des intrusions et les fonctions de protection contre le code malveillant.

SC-03(03) — Réduction des fonctionnalités n'ayant pas trait à la sécurité (---)

Énoncés :

Réduire à son minimum le nombre des fonctions non liées à la sécurité appelées à intégrer le périmètre isolé qui comprend les fonctions de sécurité.

Responsable : Aucun

Discussion :

Dans les cas où il s'avère impossible de procéder à une isolation stricte des fonctions de sécurité et des autres fonctions, il importera d'adopter des mesures visant à réduire, au sein du périmètre d'isolation de la fonction de sécurité, le nombre des fonctions n'ayant pas trait à la sécurité. En raison de leur proximité, les fonctions non liées à la sécurité qui sont comprises dans le périmètre d'isolation sont considérées comme pertinentes à la sécurité, puisque les erreurs ou le code malveillant dans le logiciel peuvent avoir des répercussions directes sur les fonctions de sécurité des systèmes. Sur le plan fondamental de la conception, il est donc important que les parties de systèmes qui assurent la protection de l'information soient aussi modestes que possible, tant sur le plan du volume que de la complexité. La réduction du nombre de fonctions non liées à la sécurité au sein des composants servant à la sécurité dans les systèmes permet aux ingénieures, aux ingénieurs et aux responsables de la mise en œuvre de se concentrer exclusivement sur les fonctions qui sont essentielles à l'exécution des capacités de sécurité requises (typiquement les mesures de contrôle des accès). En réduisant le nombre des fonctions non liées à la sécurité dans le périmètre d'isolation, on observe une réduction importante du volume de code devant être jugé fiable sur le plan de l'application des stratégies de sécurité, ce qui accroît l'intelligibilité.

SC-03(04) — Jumelage et cohésion des modules (---)

Énoncés :

Appliquer les fonctions de sécurité sous forme de modules essentiellement indépendants qui maximisent la cohésion interne des modules et réduisent les jumelages entre modules.

Responsable : Aucun

Discussion :

Réduire les interactions entre les modules aide à limiter les fonctions de sécurité et à en gérer la complexité. Les concepts de jumelage et de cohésion sont importants sur le plan de la modularité de la conception logicielle. Le jumelage renvoie aux dépendances qu'un module peut avoir avec d'autres modules. La cohésion, quant à elle, fait référence à la relation entre les fonctions d'un module. Les pratiques exemplaires en matière de génie logiciel et d'ingénierie en sécurité des systèmes misent sur la structuration en couches, la minimisation et la décomposition modulaire pour diminuer et gérer la complexité. Il est ainsi possible de produire des modules logiciels hautement cohésifs et à couplage lâche.

SC-03(05) — Structures en couches (---)

Énoncés :

Appliquer les fonctions de sécurité dans une structure en couches qui permet de réduire les interactions entre les couches de la conception et d'éviter que les couches inférieures soient assujetties au bon fonctionnement des couches supérieures ou de leurs fonctions.

Responsable : Aucun

Discussion :

L'adoption de structures en couches nécessitant peu d'interaction entre les fonctions de sécurité et les couches libres [non looping] (par exemple, les fonctions des couches inférieures ne dépendent pas des fonctions des couches supérieures) accentue l'isolation des fonctions de sécurité et facilite la gestion de la complexité.

SC-04 — Information dans les ressources système partagées (---)

Énoncés :

Empêcher les transferts d'information non autorisés ou non prévus au moyen de ressources système partagées.

Responsable : Aucun

Discussion :

Empêcher les transferts d'information non autorisés ou non prévus au moyen de ressources système partagées permet d'éviter que l'information découlant des actions effectuées par des utilisatrices et utilisateurs ou des rôles antérieurs (ou les opérations de processus agissant en leur nom) soit accessible aux utilisatrices et utilisateurs ou aux rôles actuels (ou les processus actuels agissant en leur nom) qui accèdent aux ressources système partagées après que les ressources ont été retournées au système. L'information dans les ressources système partagées s'applique également aux représentations chiffrées de l'information. Dans d'autres contextes, le contrôle de l'information dans les ressources système partagées est appelé la réutilisation d'objets et la protection d'information résiduelle. L'information dans les ressources système partagées ne s'applique pas à la persistance d'information, qui fait référence à la représentation résiduelle des données qui ont été nominalement supprimées, ni aux voies clandestines (y compris celles de réglage et de stockage) où les ressources système partagées sont manipulées de façon à enfreindre les restrictions relatives aux flux d'information, ni aux composants des systèmes qui sont associés à une seule utilisatrice, à un seul utilisateur ou à un seul rôle.

SC-04(01) — Niveaux de sécurité (---)

Énoncés :

Annulé : Intégré au contrôle SC-04.

Responsable : Aucun

SC-04(02) — Traitement multiniveau ou des périodes (---)

Énoncés :

Prévenir le transfert non autorisé d'information par l'intermédiaire de ressources partagées conformément à [Affectation : procédures définies par l'organisation] lorsque le traitement exécuté par le système alterne explicitement entre divers niveaux de classification de l'information ou différentes catégories de sécurité.

Responsable : Aucun

Discussion :

Les changements apportés aux niveaux de traitement peuvent survenir au cours du traitement multiniveau ou des périodes avec l'information aux différents niveaux de classification ou aux différentes catégories de sécurité. Ils peuvent également avoir lieu durant la réutilisation en série des composants matériels à différents niveaux de classification. Les procédures définies par l'organisme peuvent inclure des processus de nettoyage approuvés et destinés à l'information stockée électroniquement.

SC-05 — Protection contre les dénis de service (Nc--)

Énoncés :

a. [Sélection (un choix) : Protéger contre; Limiter] les effets des types d'attaques par déni de service suivants : [Affectation : types d'attaque par déni de service définis par l'organisation]
b. Employer les contrôles suivants pour atteindre l'objectif de déni de service : [Affectation : contrôles définis par l'organisation par types d'attaque par déni de service]

Responsable : Aucun

Discussion :

Les événements liés à des dénis de service peuvent survenir en raison de plusieurs causes internes et externes, comme une attaque menée par un adversaire ou le manque de planification pour soutenir les besoins organisationnels en matière de capacité et de bande passante. De telles attaques peuvent survenir par l'intermédiaire d'une vaste gamme de protocoles réseau (par exemple, IPv4, IPv6). Il existe une variété de technologies pour limiter ou éliminer l'origine et les effets des événements liés à des dénis de service. Par exemple, les mécanismes de protection des frontières peuvent filtrer certains types de paquets pour empêcher les composants d'un système faisant partie de l'un des réseaux internes d'être directement visés par des attaques par déni de service ou d'en être la source. Combinée à la redondance des services, l'utilisation d'une capacité réseau et d'une bande passante accrues peut également réduire la sensibilité à certaines attaques par déni de service.

SC-05(01) — Restreindre la capacité de mener des attaques sur d'autres systèmes (---)

Énoncés :

Restreindre la capacité des individus à lancer les attaques par déni de service suivantes sur d'autres systèmes : [Affectation : attaques par déni de service définies par l'organisation].

Responsable : Aucun

Discussion :

Restreindre la capacité des individus à lancer des attaques par déni de service exige que les mécanismes communément utilisés pour de telles attaques ne soient pas disponibles. Les individus concernés comprennent les initiées et initiés internes ou les adversaires externes qui ont compromis le système ou s'y sont introduits afin de l'utiliser pour lancer une attaque par déni de service. Les organisations peuvent restreindre la capacité des individus à se connecter et à transmettre de l'information aléatoire par un support de transport (par exemple, des réseaux câblés ou sans fil, des paquets de données mystifiés). Les organisations peuvent également restreindre la capacité des individus à utiliser les ressources du système de façon excessive. La protection contre la capacité de certains individus à lancer des attaques par déni de service peut être mise en œuvre sur certains systèmes ou sur des dispositifs de périmètres de façon à prévenir les atteintes aux systèmes pouvant constituer une cible.

SC-05(02) — Capacité, bande passante et redondance (---)

Énoncés :

Gérer l'excédent de capacité et de largeur de bande, ou toute autre redondance, afin de limiter les effets d'attaques par déni de service avec inondation d'information.

Responsable : Aucun

Discussion :

La gestion de la capacité garantit que cette dernière est suffisante pour contrer les attaques par inondation. La gestion de la capacité comprend l'établissement de priorités relatives à certaines utilisations, les quotas, le partitionnement et l'équilibrage de charge.

SC-05(03) — Détection et surveillance (---)

Énoncés :

a. Utiliser les outils de surveillance suivants pour détecter les indicateurs d'attaques par déni de service visant le système ou lancées à partir de celui-ci : [Affectation : outils de surveillance définis par l'organisation]
b. Surveiller les ressources système suivantes pour déterminer si elles sont suffisantes pour prévenir les attaques par déni de service fructueuses : [Affectation : ressources du système définies par l'organisation]

Responsable : Aucun

Discussion :

Les organisations examinent l'utilisation et l'importance des ressources de systèmes, lorsqu'elles gèrent les risques liés à des attaques par déni de service pouvant résulter d'attaques malveillantes. Les attaques par déni de service peuvent provenir de sources internes ou externes. Les ressources sensibles aux attaques par déni de service sont les fonctions de stockage sur disque matériel, la mémoire et les cycles des unités centrales de traitement (UCT). Au nombre des techniques qui permettent de prévenir les attaques par déni de service visant les fonctions et la capacité de stockage, on retrouve l'imposition d'une limite pour les disques, une configuration des systèmes qui permet d'alerter automatiquement les administratrices et administrateurs lorsque la limite d'une capacité de stockage est atteinte, l'utilisation de technologies de compression de fichiers dans le but de maximiser l'espace de stockage, et l'imposition de partitions distinctes pour les données système et les données d'utilisateur.

SC-06 — Disponibilité des ressources (---)

Énoncés :

Garantir la disponibilité des ressources en attribuant [Affectation : ressources définies par l'organisation] en fonction de [Sélection (un choix ou plus) : priorité; quota; {Affectation : contrôles définis par l'organisation}].

Responsable : Aucun

Discussion :

La protection des priorités permet d'éviter que des processus retardent ou empêchent l'exécution de processus de priorité supérieure par le système. Les quotas empêchent que des utilisatrices, des utilisateurs ou des processus disposent de plus de ressources que prévu.

SC-07 — Protection des frontières (---)

Énoncés :

a. Surveiller et contrôler les communications des interfaces externes gérées vers le système et celles des principales interfaces internes gérées au sein du système
b. Mettre en oeuvre des sous-réseaux pour les composants de systèmes à accès public qui sont séparés [Sélection (un choix) : physiquement; logiquement] des réseaux internes de l'organisation
c. Se connecter aux réseaux ou aux systèmes externes uniquement par des interfaces gérées qui sont dotées de mécanismes de protection des frontières répartis conformément à l'architecture de sécurité et de protection de la vie privée de l'organisation

Responsable : Aucun

Discussion :

Les interfaces gérées incluent les passerelles, les routeurs, les pare-feu, les mécanismes de protection, les analyseurs réseau de code malveillant, les systèmes de virtualisation et les tunnels chiffrés mis en oeuvre au sein d'une architecture de sécurité. Les sous-réseaux qui sont séparés physiquement ou logiquement des réseaux internes sont appelés communément des zones démilitarisées (ZD) ou, en anglais, DMZ (Demilitarized Zones). La restriction ou l'interdiction relative aux interfaces des systèmes organisationnels peut inclure le fait de diriger le trafic Web externe vers les serveurs Web désignés en utilisant des interfaces gérées, le fait d'interdire tout trafic externe qui semble usurper une adresse interne ou le fait d'interdire tout trafic interne qui semble usurper une adresse externe. Le document SP 800-189 du NIST donne plus d'information sur les techniques de validation des adresses sources pour prévenir l'entrée et la sortie du trafic utilisant les adresses usurpées. Les services de télécommunications commerciaux sont fournis par des composants réseau et des systèmes de gestion consolidés utilisés conjointement par les clientes et clients. Ces services peuvent également inclure des lignes d'accès et d'autres éléments de service fournis par des tiers. Ils peuvent représenter des sources de risque supplémentaire, malgré les dispositions du contrat en matière de sécurité. La protection de la frontière peut être mise en oeuvre comme contrôle commun sur l'ensemble ou une partie d'un réseau organisationnel de manière à ce que la frontière à protéger soit plus grande que la frontière du système (c'est-à-dire une limite d'autorisation).

SC-07(01) — Sous-réseaux séparés physiquement (---)

Énoncés :

Annulé : Intégré au contrôle SC-07.

Responsable : Aucun

SC-07(02) — Accès public (---)

Énoncés :

Annulé : Intégré au contrôle SC-07.

Responsable : Aucun

SC-07(03) — Points d’accès (---)

Énoncés :

Limiter le nombre de connexions réseau externes au système.

Responsable : Aucun

Discussion :

La limitation du nombre de connexions réseau externes permet d’exercer une surveillance du trafic de communications entrant et sortant. Il est important de limiter le nombre de connexions réseau externes au système lorsque les organisations passent des anciennes aux nouvelles technologies (par exemple, la transition des protocoles réseau IPv4 à IPv6). De telles transitions peuvent exiger la mise en œuvre simultanée des anciennes et nouvelles technologies pendant cette période, ce qui augmente le nombre de points d’accès au système.

SC-07(04) — Services de télécommunications externes (---)

Énoncés :

a. Appliquer une interface gérée à chaque service de télécommunications externe
b. Établir une stratégie de flux de trafic pour chaque interface gérée
c. Protéger la confidentialité et l'intégrité de l'information transmise par l'intermédiaire des interfaces
d. Documenter chaque exception à la stratégie de flux de trafic en précisant le besoin de la mission ou de l'activité donnant lieu à l'exception et la durée de ce besoin
e. Examiner les exceptions à la stratégie relative aux flux de trafic [Affectation : fréquence définie par l'organisation] et retrancher les exceptions qui ne sont plus justifiées par un besoin lié à la mission ou aux activités
f. Prévenir l'échange non autorisé du trafic du plan de contrôle avec des réseaux externes
g. Publier de l'information pour permettre aux réseaux distants de détecter le trafic du plan de contrôle non autorisé depuis les réseaux internes
h. Filtrer le trafic du plan de contrôle en provenance des réseaux externes

Responsable : Aucun

Discussion :

Les services de télécommunications externes peuvent fournir des services de communications de voix et/ou de données. Les exemples de trafic du plan de contrôle comprennent le routage par protocole BGP (Border Gateway Protocol), le système d'adressage par domaines (DNS pour Domain Name System) et les protocoles de gestion. Prière de consulter le document NIST SP 800-189 pour de l'information supplémentaire sur l'utilisation de l'infrastructure à clé publique de ressources (ICPR) pour protéger les itinéraires BGP et détecter les annonces BGP non autorisées.

SC-07(05) — Refus par défaut – Autorisation par exception (---)

Énoncés :

Refuser par défaut le trafic de communications réseau et permettre le trafic de communications réseau au moyen d'exceptions [Sélection (un choix ou plus) : à proximité des interfaces gérées; pour {Affectation : systèmes définis par l'organisation}].

Responsable : Aucun

Discussion :

Le refus par défaut et la permission par exception s'appliquent au trafic de communication réseau entrant et sortant. Une stratégie relative au trafic de communication réseau qui interdit tout trafic et ne permet le passage qu'à titre exceptionnel garantit que seules les connexions aux systèmes essentielles et approuvées sont permises. Le refus par défaut – autorisation par exception s'applique également à un système qui est connecté à un système externe.

SC-07(06) — Réponse aux échecs reconnus (---)

Énoncés :

Annulé : Intégré au contrôle SC-07(18).

Responsable : Aucun

SC-07(07) — Tunnellisation partagée pour les appareils distants (---)

Énoncés :

Prévenir la tunnellisation partagée pour les dispositifs distants qui se connectent à des systèmes organisationnels à moins que le tunnel partagé soit fourni de façon sécurisée au moyen de [Affectation : mesures de protection définies par l'organisation].

Responsable : Aucun

Discussion :

La tunnellisation partagée est un processus qui consiste à permettre à une utilisatrice, un utilisateur ou un dispositif distant d'établir une connexion non distante à un système et de communiquer simultanément par l'entremise d'une autre connexion à une ressource située dans un réseau interne. Cette méthode d'accès réseau permet à une utilisatrice ou un utilisateur d'accéder à des dispositifs distants et, simultanément, d'accéder à des réseaux non contrôlés. La tunnellisation partagée peut s'avérer désirable par les utilisatrices et utilisateurs distants qui veulent communiquer avec les ressources du système local, notamment les imprimantes et les serveurs de fichiers. La tunnellisation partagée pourrait toutefois donner libre cours aux connexions externes non autorisées, rendant ainsi le système plus vulnérable aux attaques et aux exfiltrations d'information organisationnelle. On peut prévenir la tunnellisation partagée en désactivant les paramètres de configuration qui permettent une telle capacité dans des dispositifs distants et en empêchant ces paramètres de configuration d'être configurés par les utilisatrices et utilisateurs. La prévention peut également être réalisée par la détection de la tunnellisation partagée (ou des paramètres de configuration qui permettent la tunnellisation partagée) dans le dispositif distant, ainsi que par l'interdiction des connexions lorsque le dispositif distant utilise la tunnellisation partagée. Un RPV peut être utilisé pour fournir un tunnel partagé de manière sécurisée. Un RPV fourni de manière sécurisée comprend le verrouillage de la connectivité à des environnements exclusifs, gérés et nommés ou à un ensemble particulier d'adresses préapprouvées, sans l'intervention d'une utilisatrice ou un utilisateur.

SC-07(08) — Acheminement du trafic vers des serveurs mandataires authentifiés (---)

Énoncés :

Acheminer [Affectation : trafic de communications internes défini par l'organisation] vers [Affectation : réseaux externes désignés par l'organisation] par l'intermédiaire de serveurs mandataires authentifiés à proximité des interfaces gérées.

Responsable : Aucun

Discussion :

Les réseaux externes sont des réseaux qui échappent au contrôle de l'organisation. Un serveur mandataire est un serveur (par exemple, un système ou une application) qui sert d'intermédiaire auprès des clients qui veulent accéder aux ressources d'un système depuis des serveurs à l'extérieur de l'organisation ou d'autres serveurs organisationnels. Les ressources système qui peuvent être demandées comprennent les fichiers, les connexions, les pages Web ou les services. Par une connexion au serveur mandataire, les clients soumettent des requêtes qui sont évaluées de façon à gérer la complexité et à fournir une protection additionnelle en limitant les connexions directes. Les dispositifs de filtrage de contenus Web constituent les serveurs mandataires les plus couramment utilisés pour fournir un accès Internet. Les serveurs mandataires peuvent prendre en charge la journalisation des sessions TCP (Transmission Control Protocol) et le blocage d'adresses URL, d'adresses IP et de noms de domaine en particulier. Les serveurs mandataires Web peuvent également être configurés à partir de listes de sites Web autorisés et non autorisés définies par l'organisation. Il convient de mentionner que les serveurs mandataires peuvent restreindre l'utilisation des RPV et ouvrir la porte à de potentielles attaques de type adversaire au milieu (selon la mise en oeuvre).

SC-07(09) — Restriction du trafic de communications malveillant sortant (---)

Énoncés :

a. Détecter et bloquer le trafic de communications sortant susceptible de constituer une menace pour les systèmes externes
b. Vérifier l'identité des utilisatrices et utilisateurs internes associés aux communications bloquées

Responsable : Aucun

Discussion :

La détection du trafic de communications sortant provenant d'activités internes et susceptible de poser une menace pour les systèmes externes est désignée sous le nom de détection d'extrusion. La détection d'extrusion est effectuée dans le système des interfaces gérées. Elle comprend une analyse du trafic de communications entrant et sortant qui vise à trouver des indications de menaces internes ciblant la sécurité des systèmes externes. Les menaces internes visant les systèmes externes comprennent le trafic annonciateur d'attaques par déni de service, du trafic utilisant des adresses sources usurpées et du trafic contenant du code malveillant. Les organisations devraient définir les critères pour déterminer, mettre à jour et gérer les menaces relevées par rapport à la détection d'extrusion.

SC-07(10) — Prévention de l'exfiltration (---)

Énoncés :

a. Prévenir l'exfiltration de l'information
b. Procéder à des tests d'exfiltration [Affectation : fréquence définie par l'organisation]

Responsable : Aucun

Discussion :

La prévention de l'exfiltration s'applique à l'exfiltration d'information intentionnelle et accidentelle. Les techniques utilisées pour prévenir l'exfiltration d'information des systèmes peuvent être mises en oeuvre aux points d'extrémité internes, aux frontières externes et à travers les interfaces gérées. Elles comprennent également l'adhésion aux formats de protocoles, la surveillance du balisage malveillant en provenance des systèmes, la déconnexion des interfaces réseau externes, sauf lorsqu'elles sont explicitement requises, l'analyse des profils de trafic visant à détecter tout écart par rapport au volume et aux types de trafic attendus au sein des organisations, les procédures de rappel vers les centres de commande et de contrôle, la réalisation de tests d'intrusion, la surveillance de la stéganographie, le désassemblage et le réassemblage d'en-têtes de paquet, et l'utilisation d'outils de prévention de la perte et de la fuite de données. Parmi les dispositifs servant à imposer le respect rigoureux des formats de protocole, on retrouve les pare-feu d'inspection approfondie des paquets et les passerelles d'interface XML (Extensible Markup Language). Les dispositifs vérifient le respect des spécifications et des formats de protocoles au niveau de la couche application et permettent de relever les vulnérabilités indétectables au moyen de dispositifs fonctionnant au niveau des couches réseau ou transport. La prévention de l'exfiltration est similaire à la prévention de la perte ou de la fuite de données et est étroitement liée aux solutions interdomaines et aux mécanismes de protection de systèmes qui appliquent les exigences relatives aux flux d'information.

SC-07(11) — Restrictions du trafic de communications entrant (---)

Énoncés :

Faire en sorte que seules les communications entrantes provenant de [Affectation : sources autorisées désignées par l'organisation] puissent être acheminées vers [Affectation : destinations autorisées désignées par l'organisation].

Responsable : Aucun

Discussion :

Des techniques générales de validation des adresses sources sont employées pour restreindre l'utilisation d'adresses sources illégitimes et non attribuées, ainsi que celle d'adresses sources qui ne devraient être utilisées que dans le système. La restriction du trafic de communications entrant fournit des indices que les paires d'adresses (source et destination) représentent des communications autorisées ou permises. Ces indices peuvent être fondés sur divers facteurs, notamment la présence de paires d'adresses dans les listes de communications autorisées ou permises, l'absence de paires d'adresses dans les listes de paires non autorisées ou interdites, ou le respect de règles plus générales de paires (sources et destination) autorisées ou permises. L'authentification robuste d'adresses réseau est impossible sans le recours à des protocoles de sécurité explicites, ce qui fait en sorte que les adresses peuvent souvent être usurpées. De plus, il est possible d'utiliser des méthodes de restriction du trafic entrant basé sur les identités, comme les listes de contrôle d'accès aux routeurs et les règles de pare-feu.

SC-07(12) — Protection au niveau de l'hôte (---)

Énoncés :

Mettre en oeuvre [Affectation : mécanismes de protection de la frontière au niveau de l'hôte définis par l'organisation] à [Affectation : composants des systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Les mécanismes de protection des frontières intégrés à l'hôte peuvent être des ordinateurs pare-feu. Les composants de systèmes qui appliquent des mécanismes de protection des frontières intégrés à l'hôte peuvent être des serveurs, des stations de travail, des ordinateurs blocs-notes et des appareils mobiles.

SC-07(13) — Isolation des outils de sécurité, des mécanismes et des composants de soutien (---)

Énoncés :

Isoler les [Affectation : principaux outils, mécanismes et composants de soutien de la sécurité de l'information désignés par l'organisation] des autres composants internes du système au moyen de sous-réseaux physiques distincts dotés d'interfaces gérées tournées vers les autres parties du système.

Responsable : Aucun

Discussion :

La distinction physique des sous-réseaux dotés d'interfaces gérées est utile lorsqu'il s'agit d'isoler les défenses d'un réseau informatique des réseaux de traitement opérationnel essentiel, dans le but d'empêcher les parties adverses de découvrir les techniques d'analyse et d'investigation informatique employées par les organisations.

SC-07(14) — Protection contre les connexions physiques non autorisées (---)

Énoncés :

Assurer une protection contre les connexions physiques non autorisées à [Affectation : interfaces gérées désignées par l'organisation].

Responsable : Aucun

Discussion :

Les systèmes qui fonctionnent selon diverses catégories de sécurité ou divers niveaux de classification pourraient partager des contrôles physiques et environnementaux communs, puisqu'ils peuvent se trouver dans les mêmes locaux d'une installation. En pratique, ces systèmes distincts peuvent également partager les mêmes salles d'équipement, armoires de câblage et trajets de distribution des câbles. La protection contre les connexions physiques non autorisées peut être assurée par l'utilisation de chemins de câbles, de boîtiers de raccordement et de tableaux de connexions physiquement distincts et clairement identifiés à chaque extrémité des interfaces gérées qui limitent l'accès au moyen de contrôles d'accès physique.

SC-07(15) — Accès privilégiés aux réseaux (---)

Énoncés :

Acheminer tous les accès réseau privilégiés par l'intermédiaire d'une interface gérée spécialisée aux fins de contrôle des accès et de vérification.

Responsable : Aucun

Discussion :

L'accès privilégié offre une plus grande accessibilité aux fonctions du système, dont les fonctions de sécurité. Les adversaires tentent d'obtenir un accès privilégié aux systèmes au moyen d'un accès distant pour causer des répercussions négatives sur la mission ou les activités, comme exfiltrer l'information ou mettre hors fonction une capacité de système essentielle. Acheminer toutes les requêtes d'accès réseau privilégiés par l'intermédiaire d'une interface gérée spécialisée permet de limiter davantage l'accès privilégié à de plus amples contrôles d'accès et de vérification.

SC-07(16) — Prévention de la découverte de composants de systèmes (---)

Énoncés :

Prévenir la découverte des composants de systèmes particuliers qui représentent une interface gérée.

Responsable : Aucun

Discussion :

Prévenir la découverte des composants de systèmes représentant une interface gérée aide à éviter que les adresses réseau de ces composants soient découvertes au moyen de techniques et d'outils couramment utilisés pour trouver les dispositifs sur les réseaux. Les adresses réseau ne sont pas disponibles aux fins de découverte et doivent être connues au préalable pour qu'on puisse y accéder. Pour prévenir la découverte des composants et des dispositifs, on peut ne pas diffuser les adresses réseau, avoir recours à la traduction d'adresses de réseau ou ne pas saisir les adresses dans les systèmes d'adressage par domaines. Une autre technique de prévention consiste à changer les adresses réseau périodiquement.

SC-07(17) — Application automatisée des formats de protocoles (---)

Énoncés :

Appliquer la stricte adhésion aux formats de protocoles.

Responsable : Aucun

Discussion :

Les composants de systèmes qui servent à appliquer les formats de protocole comprennent les pare-feu d'inspection approfondie des paquets et les passerelles XML. Les composants vérifient le respect de la spécification et du format de protocole au niveau de la couche application et permettent d'identifier les vulnérabilités indétectables au moyen de dispositifs fonctionnant au niveau des couches réseau ou transport.

SC-07(18) — Fonctionnement à sécurité intégrée (---)

Énoncés :

Éviter que les systèmes passent en mode non sécurisé dans l'éventualité de la défaillance opérationnelle d'un dispositif de protection des frontières.

Responsable : Aucun

Discussion :

Le fonctionnement à sécurité intégrée est une condition réalisée au moyen de mécanismes visant à s'assurer qu'advenant la défaillance opérationnelle de dispositifs de protection des frontières sur des interfaces gérées, les systèmes ne passent pas à des états non sécurisés lorsque les propriétés de sécurité prévues n'ont plus aucun effet. Les interfaces gérées comprennent les routeurs, les pare-feu et les passerelles d'application qui résident sur des sous-réseaux protégés (communément appelés des ZD). Les défaillances de dispositifs de protection des frontières ne doivent pas permettre à l'information qui est extérieure aux dispositifs d'entrer dans ce dernier ni permettre la diffusion non autorisée d'information.

SC-07(19) — Blocage des communications provenant d'hôtes non configurés par l'organisme (---)

Énoncés :

Bloquer le trafic de communications entrant et sortant entre [Affectation : clients en communication désignés par l'organisation] qui est configuré indépendamment par les utilisatrices, les utilisateurs et les fournisseurs de services externes.

Responsable : Aucun

Discussion :

Les clients de communications qui ont été configurés indépendamment par les utilisatrices ou utilisateurs finaux et les fournisseurs de services externes comprennent les clients de messagerie instantanée, ainsi que les logiciels et les applications de vidéoconférence. Le blocage de trafic ne s'applique pas aux clients des communications qui sont configurés par des organisations dans le but d'exécuter des fonctions autorisées.

SC-07(20) — Isolation dynamique et séparation (---)

Énoncés :

Fournir la capacité d'isoler dynamiquement [Affectation : composants de systèmes désignés par l'organisation] des autres composants de systèmes.

Responsable : Aucun

Discussion :

La capacité d'isoler dynamiquement certains composants de systèmes internes s'avère utile lorsqu'il est nécessaire de partitionner ou de séparer certains composants de systèmes d'origine douteuse des composants jugés fiables. L'isolation des composants réduit la surface d'attaque des systèmes organisationnels. L'isolation de certains composants de systèmes représente également un moyen de limiter les dommages causés par les attaques fructueuses.

SC-07(21) — Isolation des composants de systèmes (---)

Énoncés :

Avoir recours à des mécanismes de protection de la frontière dans le but de séparer [Affectation : composants du système désignés par l'organisation] assurant le soutien aux [Affectation : fonctions liées à la mission et aux activités définies par l'organisation].

Responsable : Aucun

Discussion :

Les organisations peuvent isoler des composants de systèmes qui exécutent diverses fonctions liées à la mission ou aux activités. Ce type d'isolation limite les flux d'information non autorisés parmi les composants de systèmes et fournit l'occasion de mettre en œuvre des niveaux de sécurité accrus pour certains composants de systèmes. La séparation des composants de systèmes par des mécanismes de protection frontalière permet d'accroître la protection de chacun des composants de systèmes et d'intensifier le contrôle des flux d'information entre ces mêmes composants. Isoler les composants de systèmes offre une protection accrue qui limite les dommages que les cyberattaques et les erreurs malveillantes pourraient causer. Le degré de séparation varie selon les mécanismes choisis. Les mécanismes de protection des frontières comprennent les routeurs, les passerelles et les pare-feu qui séparent les composants de systèmes en réseaux et sous-réseaux distincts; les dispositifs interdomaines qui séparent les sous-réseaux; les techniques de virtualisation; le chiffrement des flux d'information entre les composants de systèmes au moyen de clés de chiffrement distinctes et l'isolation physique et électrique complète du réseau ou du système concerné par rapport à tous les autres réseaux.

SC-07(22) — Sous-réseaux distincts pour la connexion à des domaines de sécurité différents (---)

Énoncés :

Appliquer des adresses réseau distinctes pour établir une connexion à des systèmes se trouvant dans des domaines de sécurité différents.

Responsable : Aucun

Discussion :

La décomposition des systèmes en sous-réseau aide à fournir le niveau de protection requis pour les connexions réseau à des domaines de sécurité différents qui contiennent de l'information comportant des catégories de sécurité différentes ou des niveaux de sécurité différents.

SC-07(23) — Désactivation de la rétroaction à l'expéditrice ou expéditeur après l'échec de validation d'un protocole (---)

Énoncés :

Désactiver la fonction de rétroaction à l'expéditrice ou expéditeur advenant l'échec de la validation d'un format de protocole.

Responsable : Aucun

Discussion :

La désactivation de la rétroaction à l'expéditrice ou expéditeur en cas d'échec de la validation du format d'un protocole empêche les adversaires d'obtenir de l'information qui, en d'autres circonstances, serait non disponible.

SC-07(24) — Renseignements personnels (---)

Énoncés :

Pour les systèmes qui traitent des renseignements personnels
a. appliquer les règles de traitement suivantes aux éléments de données des renseignements personnels : [Affectation : règles de traitement définies par l'organisation]
b. surveiller le traitement autorisé dans les interfaces externes du système et à ses principales frontières internes
c. documenter chaque exception à la règle de traitement
d. examiner et supprimer les exceptions qui ne sont plus prises en charge

Responsable : Aucun

Discussion :

Gérer le traitement des renseignements personnels est un aspect important de la protection de la vie privée des individus. L'application des exceptions aux règles de traitement, leur surveillance et leur documentation permet de s'assurer que les renseignements personnels sont traités conformément aux exigences établies en matière de respect de la vie privée.

SC-07(25) — Connexions à des systèmes de sécurité nationaux non classifiés (---)

Énoncés :

Interdire toute connexion directe de [Affectation : système de sécurité national non classifié désigné par l'organisation] à un réseau externe sans utiliser [Affectation : dispositif de protection des frontières désigné par l'organisation].

Responsable : Aucun

SC-07(26) — Connexions à des systèmes de sécurité nationaux classifiés (---)

Énoncés :

Interdire toute connexion directe de [Affectation : système de sécurité national classifié désigné par l'organisation] à un réseau externe sans utiliser [Affectation : dispositif de protection des frontières désigné par l'organisation].

Responsable : Aucun

SC-07(27) — Connexions à des systèmes de sécurité non nationaux non classifiés (---)

Énoncés :

Interdire toute connexion directe de [Affectation : système de sécurité non national non classifié désigné par l'organisation] à un réseau externe sans utiliser [Affectation : dispositif de protection des frontières désigné par l'organisation].

Responsable : Aucun

SC-07(28) — Connexions aux réseaux publics (---)

Énoncés :

Interdire toute connexion directe de [Affectation : système désigné par l'organisation] à un réseau public.

Responsable : Aucun

Discussion :

Une connexion directe est une connexion physique ou virtuelle dédiée entre deux systèmes ou plus. Par réseau public, on entend tout réseau auquel peut accéder le public, comme Internet et les réseaux extranet d'accès public d'une organisation.

SC-07(29) — Séparation des sous-réseaux pour l'isolation des fonctions (Nc--)

Énoncés :

Mettre en oeuvre [Sélection (un choix) : physiquement; logiquement] des sous-réseaux distincts pour isoler les fonctions et les composants de systèmes critiques suivants : [Affectation : composants et fonctions de systèmes essentiels définis par l'organisation].

Responsable : Aucun

Discussion :

Il pourrait être nécessaire de séparer les composants et les fonctions des composants de systèmes critiques des autres composants et fonctions des composants de systèmes non critiques au moyen de sous-réseaux distincts pour faire en sorte qu'ils soient moins susceptibles de faire l'objet d'une violation ou d'une compromission catastrophique ou débilitante donnant lieu à la défaillance des systèmes. Par exemple, séparer physiquement la fonction de commande et de contrôle du système de divertissements en vol en séparant les sous-réseaux d'un avion commercial permet d'offrir un niveau accru d'assurance dans la fiabilité et la robustesse des fonctions de système critiques.

SC-08 — Confidentialité et intégrité des transmissions (Nc--)

Énoncés :

Protéger [Sélection (un choix ou plus) : la confidentialité; l'intégrité] de l'information transmise.

Responsable : Aucun

Discussion :

La protection de la confidentialité et de l'intégrité de l'information transmise s'applique aux réseaux internes et externes ainsi qu'à tous les composants du système qui peuvent transmettre de l'information, y compris les serveurs, les ordinateurs blocs-notes, les ordinateurs de bureau, les appareils mobiles, les imprimantes, les photocopieurs, les numériseurs, les télécopieurs et les radios. Les chemins de communication non protégés sont vulnérables à l'interception et à la modification. On peut assurer la protection de la confidentialité et de l'intégrité de l'information en faisant appel à des moyens physiques ou logiques. La protection physique peut être réalisée au moyen de systèmes de distribution protégés. Un système de distribution protégé est un système de télécommunications à fibre optique qui comprend des points terminaux et les contrôles électromagnétiques, acoustiques, électriques et physiques adéquats pour permettre une transmission non chiffrée de l'information classifiée. Le recours à des techniques de chiffrement permet d'assurer une protection logique. Les organisations qui misent sur des fournisseurs commerciaux offrant des fonctions de transmission qui sont des services accessoires plutôt que des services nominaux peuvent avoir de la difficulté à obtenir les assurances nécessaires pour la mise en oeuvre des contrôles exigés pour garantir la confidentialité et l'intégrité des transmissions. Dans de telles situations, les organisations établissent les types de services de confidentialité ou d'intégrité qui sont disponibles dans les ensembles de services de télécommunications commerciaux standard. S'il est impossible d'obtenir les contrôles nécessaires et l'assurance qu'ils sont appliqués de manière efficace par la voie contractuelle appropriée, les organisations peuvent mettre en place des contrôles compensatoires appropriés.

SC-08(01) — Protection cryptographique (Nc--)

Énoncés :

Mettre en oeuvre des mécanismes de chiffrement pour [Sélection (un choix ou plus) : prévenir la divulgation non autorisée d'information; détecter les modifications apportées à l'information] durant la transmission.

Responsable : Aucun

Discussion :

Le chiffrement protège l'information contre toute divulgation ou modification non autorisée durant la transmission. Les mécanismes cryptographiques qui protègent la confidentialité et l'intégrité de l'information durant la transmission incluent les protocoles TLS et Internet Protocol Security (IPsec). Les mécanismes de chiffrement utilisés pour protéger l'intégrité de l'information comprennent les fonctions de hachage cryptographique qui ont des applications semblables en ce qui a trait aux signatures numériques, les sommes de contrôle et les codes d'authentification des messages.

SC-08(02) — Traitement pré-transmission et post-transmission (---)

Énoncés :

Maintenir [Sélection (un choix ou plus) : la confidentialité; l'intégrité] de l'information au cours de la préparation à la transmission et pendant la réception.

Responsable : Aucun

Discussion :

L'information est divulguée ou modifiée de façon accidentelle ou malveillante en cours de transmission ou au moment de sa réception, notamment pendant l'agrégation, aux points de transformation de protocole et pendant le groupage et le dégroupage. Ces divulgations ou modifications non autorisées compromettent la confidentialité ou l'intégrité de l'information.

SC-08(03) — Protection cryptographique pour les éléments complémentaires des messages (---)

Énoncés :

Appliquer des mécanismes visant à protéger les éléments complémentaires des messages, sauf si l'information est protégée par [Affectation : autres mesures de protection physique définies par l'organisation].

Responsable : Aucun

Discussion :

La protection cryptographique des éléments complémentaires des messages porte sur la protection contre la divulgation non autorisée de l'information. Les éléments complémentaires des messages comprennent l'en-tête des messages et l'information relative au routage. La protection cryptographique prévient l'exploitation des éléments complémentaires et s'applique aux réseaux internes et externes ou encore aux liens pouvant être visibles à celles et ceux qui ne sont pas des utilisatrices et utilisateurs autorisés. L'information relative aux en têtes et au routage est parfois transmise en texte clair (c'est-à-dire non chiffrée) en raison du fait que l'information n'est pas identifiée comme étant pertinente par les organisations ou parce que le chiffrement de l'information pourrait réduire les performances du réseau ou accroître les coûts. Les autres contrôles physiques comprennent, par exemple, les systèmes de diffusion protégée.

SC-08(04) — Dissimulation et distribution aléatoire des communications (---)

Énoncés :

Appliquer des mécanismes cryptographiques visant à protéger ou à distribuer aléatoirement les schémas de communication, sauf si l'information est protégée par [Affectation : autres contrôles physiques définis par l'organisation].

Responsable : Aucun

Discussion :

La dissimulation ou la distribution aléatoire des schémas de communication vise à offrir une protection contre la divulgation non autorisée de l'information. Les schémas de communication comprennent la fréquence, les périodes, la prévisibilité et la quantité. La modification des schémas de communication peut révéler de l'information ayant une valeur de renseignement, particulièrement lorsque celle-ci est combinée à d'autres informations disponibles sur les fonctions liées à la mission et aux activités de l'organisation. Dissimuler et distribuer aléatoirement les communications prévient le dévoilement indirect de renseignements fondé sur les schémas de communications et s'applique aux réseaux internes et externes ou encore aux liens pouvant être visibles à celles et ceux qui ne sont pas des utilisatrices et utilisateurs autorisés. Le chiffrement des liens et la transmission selon des schémas continus, fixes ou aléatoires permettent d'éviter que des renseignements soient déduits à partir des schémas de communication du système. Les autres contrôles physiques comprennent, par exemple, les systèmes de diffusion protégée.

SC-08(05) — Système de distribution protégé (---)

Énoncés :

Mettre en œuvre [Affectation : système de distribution protégé désigné par l'organisation] pour [Sélection (un choix ou plus) : prévenir la divulgation non autorisée d'information; détecter les modifications apportées à l'information] durant la transmission.

Responsable : Aucun

Discussion :

L'objectif d'un système de distribution protégé est de prévenir l'accès physique aux lignes de communication qui transportent l'information de sécurité nationale, de détecter un tel accès et de faire en sorte qu'il soit difficile.

SC-09 — Confidentialité des transmissions (---)

Énoncés :

Annulé : Intégré au contrôle SC-08.

Responsable : Aucun

SC-10 — Déconnexion du réseau (---)

Énoncés :

Mettre fin à la connexion réseau associée à la session de communication à la fin de la session ou après [Affectation : période définie par l'organisation] d'inactivité.

Responsable : Aucun

Discussion :

La déconnexion réseau s'applique aux réseaux internes et externes. L'interruption des connexions réseau associées aux sessions de communication comprend la désaffectation des adresses TCP/IP ou des paires de ports au niveau du système d'exploitation ou la désaffectation des attributions réseau au niveau de l'application si plusieurs sessions d'application utilisent une seule connexion réseau au niveau du système d'exploitation. Les périodes d'inactivité peuvent être établies par les organisations et comprennent des périodes par type d'accès réseau ou pour des accès réseau particuliers.

SC-11 — Chemin de confiance (---)

Énoncés :

a. Fournir un chemin de communication de confiance isolé [Sélection (un choix) : physiquement; logiquement] pour établir les communications entre les utilisatrices et utilisateurs et les composants fiables du système
b. Permettre aux utilisatrices et utilisateurs d'invoquer le chemin de communication de confiance pour les communications entre l'utilisatrice ou utilisateur et les fonctions de sécurité suivantes du système qui incluent, au minimum, l'authentification et la réauthentification : [Affectation : fonctions de sécurité définies par l'organisation]

Responsable : Aucun

Discussion :

Les chemins de confiance sont des mécanismes par l'intermédiaire desquels les utilisatrices et utilisateurs peuvent communiquer (au moyen de dispositifs de saisie, comme des pavés numériques ou des lecteurs de cartes à puce dotés d'un clavier de NIP intégré) directement avec les fonctions de sécurité des systèmes tout en ayant l'assurance requise pour soutenir les stratégies de sécurité. Les mécanismes des chemins de confiance ne peuvent être activés que par les utilisatrices et utilisateurs ou par les fonctions de sécurité des systèmes organisationnels. Les réponses de l'utilisatrice ou utilisateur qui sont acheminées par les chemins de confiance sont protégées contre les divulgations et les modifications non autorisées provoquées par des applications non fiables. Les organisations emploient des chemins de confiance pour les connexions d'assurance élevée entre les fonctions de sécurité des systèmes et les utilisatrices et utilisateurs, notamment pendant les connexions au système. Les mises en œuvre initiales des chemins de confiance employaient un signal hors bande pour amorcer le chemin, comme utiliser la touche <BREAK>, qui ne transmet aucun caractère susceptible d'être usurpé. Dans les mises en œuvre plus récentes, une combinaison de touches impossibles à détourner a été utilisée (par exemple, les touches <CTRL>+<ALT>+<DEL>). De telles combinaisons de clés, par contre, sont propres aux plateformes et ne peuvent pas assurer la mise en œuvre d'un chemin de confiance dans tous les cas. L'application des chemins de communication de confiance est généralement fournie dans le cadre d'une mise en œuvre qui répond au concept de contrôleur de référence.

SC-11(01) — Chemin de communication irréfutable (---)

Énoncés :

a. Fournir un chemin de communication de confiance qui est irréfutablement distinct des autres chemins de communication
b. Amorcer le chemin de communication de confiance pour les communications entre les [Affectation : fonctions de sécurité définies par l'organisation] du système et l'utilisatrice ou utilisateur

Responsable : Aucun

Discussion :

Un chemin de communication irréfutable permet au système d'instaurer un chemin de confiance, lequel exige que l'utilisatrice ou utilisateur reconnaisse de façon non équivoque la source de la communication comme étant un composant fiable du système. Par exemple, le chemin de confiance peut apparaître dans une zone de l'écran qui est inaccessible aux autres applications ou être basé sur la présence d'un identifiant qui ne peut être usurpé.

SC-12 — Établissement et gestion des clés cryptographiques (Nc--)

Énoncés :

Établir et gérer les clés cryptographiques lorsque la cryptographie est utilisée dans le système conformément aux exigences de gestion de clés suivantes : [Affectation : exigences définies par l'organisation liées à la génération, à la distribution, au stockage, à l'accès et à la destruction des clés].

Responsable : Aucun

Discussion :

L'établissement et la gestion des clés cryptographiques peuvent être effectués au moyen de procédures manuelles ou de mécanismes automatisés soutenus par des procédures manuelles. Les organisations définissent les exigences liées à la gestion des clés conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables, et elles précisent les options, les paramètres et les niveaux appropriés. Les organisations gèrent les magasins de confiance en veillant à ce que seuls les ancrages de confiance préalablement approuvés se trouvent dans de tels magasins. Cela inclut les certificats disposant d'une visibilité à l'extérieur des systèmes organisationnels et les certificats ayant trait aux systèmes opérationnels internes. Le PVMC conjoint du NIST et du CST fournit de l'information additionnelle sur les modules et les algorithmes cryptographiques validés qui peuvent être utilisés pour gérer et établir les clés cryptographiques.

SC-12(01) — Disponibilité (---)

Énoncés :

Maintenir la disponibilité de l'information dans l'éventualité où les utilisatrices et utilisateurs perdent leurs clés cryptographiques.

Responsable : Aucun

Discussion :

Le séquestre des clés de chiffrement constitue une pratique courante visant à assurer une certaine disponibilité en cas de perte de clés. L'oubli d'une phrase de passe est un exemple de perte de clé cryptographique.

SC-12(02) — Clés symétriques (---)

Énoncés :

Produire, contrôler et distribuer les clés cryptographiques symétriques en faisant appel à une technologie et à des processus de gestion des clés [Sélection (un choix) : validés par le PVMC; approuvés par le Centre pour la cybersécurité; avec matériel de chiffrement préplacé].

Responsable : Aucun

Discussion :

La publication ITSP.40.111 du Centre pour la cybersécurité propose des recommandations sur les mécanismes d'établissement de clés cryptographiques et les fonctions de dérivation de clés pouvant servir à produire des clés symétriques partagées entre deux parties. Ces mécanismes doivent être utilisés dans un protocole de sécurité réseau, comme ceux mentionnés dans l'ITSP.40.062 du Centre pour la cybersécurité avec de plus amples conseils sur la configuration.

SC-12(03) — Clés asymétriques (---)

Énoncés :

Produire, contrôler et distribuer les clés cryptographiques asymétriques en faisant appel à [Sélection (un choix) : des processus de gestion des clés approuvés par le Centre pour la cybersécurité; du matériel de chiffrement préplacé; des certificats d'ICAP à assurance moyenne approuvés ou émis par le Centre pour la cybersécurité; des certificats d'ICP et des jetons de sécurité matériels qui protègent la clé privée de l'utilisatrice ou utilisateur; des certificats émis conformément aux exigences définies par l'organisation].

Responsable : Aucun

Discussion :

L'ITSP.40.111 fournit des recommandations pour les spécifications approuvées de la cryptographie asymétrique et recommande que les mises en œuvre, y compris la génération de clés, soient effectuées dans des modules cryptographiques validés selon le PVMC. L'ITSP.40.062 offre des conseils sur la gestion des clés asymétriques dans une ICP.

SC-12(04) — Certificats d’ICP (---)

Énoncés :

Annulé : Intégré au contrôle SC-12(03).

Responsable : Aucun

SC-12(05) — Certificats d'ICP et jetons matériels (---)

Énoncés :

Annulé : Intégré au contrôle SC-12(03).

Responsable : Aucun

SC-12(06) — Contrôle physique des clés (---)

Énoncés :

Assurer le contrôle physique des clés cryptographiques lorsque l'information stockée est chiffrée par des fournisseurs de services externes.

Responsable : Aucun

Discussion :

Pour les organisations qui ont recours à des fournisseurs de services externes (par exemple, des fournisseurs de services infonuagiques ou de centre de données), le contrôle physique des clés cryptographiques offre une assurance additionnelle que l'information stockée par de tels fournisseurs externes n'est pas sujette à une divulgation ou à une modification non autorisée.

SC-13 — Protection cryptographique (Nc--)

Énoncés :

a. Déterminer les [Affectation : utilisations cryptographiques définies par l'organisation]
b. Mettre en place les types de cryptographies nécessaires à chaque utilisation cryptographique indiquée : [Affectation : types de cryptographies définis par l'organisation pour chaque utilisation cryptographique indiquée]

Responsable : Aucun

Discussion :

La cryptographie peut être employée pour soutenir une variété de solutions de sécurité, notamment la protection d'information classifiée et d'information protégée, la livraison et la mise en oeuvre de signatures numériques, et l'obligation de séparer l'information, lorsque des personnes autorisées disposent des habilitations requises pour l'information en question sans avoir les approbations formelles d'accès nécessaires. La cryptographie peut également servir à soutenir la génération aléatoire de nombres et la génération de hachage. Parmi les normes généralement appliquées en matière de cryptographie, on retrouve la cryptographie homologuée FIPS (Federal Information Processing Standard) et la cryptographie approuvée par le Centre pour la cybersécurité. Par exemple, les organisations qui doivent protéger l'information classifiée peuvent indiquer l'utilisation d'une cryptographie approuvée par le Centre pour la cybersécurité. Les organisations qui doivent fournir et mettre en oeuvre des signatures numériques peuvent indiquer l'utilisation d'une cryptographie homologuée FIPS. La cryptographie est mise en oeuvre conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables.

SC-13(01) — Cryptographie homologuée FIPS (---)

Énoncés :

Annulé : Intégré au contrôle SC-13.

Responsable : Aucun

SC-13(02) — Cryptographie approuvée par la National Security Agency (NSA) (---)

Énoncés :

Annulé : Intégré au contrôle SC-13.

Responsable : Aucun

SC-13(03) — Personnes ne disposant pas des approbations formelles d'accès (---)

Énoncés :

Annulé : Intégré au contrôle SC-13.

Responsable : Aucun

SC-13(04) — Signatures numériques (---)

Énoncés :

Annulé : Intégré au contrôle SC-13.

Responsable : Aucun

SC-13(400) — Données en transit PROTÉGÉ A (---)

Énoncés :

Annulé : Intégré au contrôle SC-13.

Responsable : Aucun

SC-13(401) — Données en transit PROTÉGÉ B (---)

Énoncés :

Annulé : Intégré au contrôle SC-13.

Responsable : Aucun

SC-13(402) — Données en transit PROTÉGÉ C (---)

Énoncés :

Annulé : Intégré au contrôle SC-13.

Responsable : Aucun

SC-14 — Protection de l’accès public (---)

Énoncés :

Annulé : Intégré aux contrôles AC-02, AC-03, AC-05, AC-06, SI-03, SI-04, SI-05, SI-07 et SI-10.

Responsable : Aucun

SC-15 — Applications et dispositifs d'informatique collaborative (---)

Énoncés :

a. Empêcher l'activation à distance des applications et des dispositifs d'informatique collaborative, sauf pour les exceptions suivantes : [Affectation : exceptions définies par l'organisation pour lesquelles l'activation à distance doit être permise]
b. Indiquer de manière explicite l'utilisation permise pour les utilisatrices et utilisateurs qui se trouvent physiquement à proximité des dispositifs

Responsable : Aucun

Discussion :

Les applications et les dispositifs d'informatique collaborative comprennent les dispositifs et applications de rencontres en ligne, les tableaux blancs en réseau, les caméras et les microphones. L'indication explicite de l'utilisation comprend un signal transmis à l'utilisatrice ou utilisateur lorsque l'application ou le dispositif d'informatique coopérative est activé.

SC-15(01) — Déconnexion physique ou logique (---)

Énoncés :

Permettre la déconnexion [Sélection (un choix ou plus) : physique; logique] des dispositifs d'informatique coopérative de manière à assurer la convivialité.

Responsable : Aucun

Discussion :

L'échec de la déconnexion d'un dispositif d'informatique collaborative peut ultérieurement occasionner des compromissions d'information organisationnelle. L'application de méthodes simples de déconnexions par rapport à de tels dispositifs après une séance d'informatique collaborative permet d'assurer que les participantes et participants exécutent la déconnexion sans avoir à suivre des procédures longues et complexes. La déconnexion des dispositifs d'informatique collaborative peut être manuelle ou automatique.

SC-15(02) — Blocage du trafic de communications entrant et sortant (---)

Énoncés :

Annulé : Intégré au contrôle SC-07.

Responsable : Aucun

SC-15(03) — Désactivation et retrait dans les zones de travail sécurisées (---)

Énoncés :

Désactiver ou retirer les applications et dispositifs d'informatique collaborative sur [Affectation : systèmes ou composants de systèmes désignés par l'organisation] dans [Affectation : zones de travail sécurisées désignées par l'organisation].

Responsable : Aucun

Discussion :

La non-désactivation ou le non-retrait d'applications ou de dispositifs d'informatique collaborative des systèmes ou des composants de systèmes peut donner lieu à des compromissions d'information, notamment l'écoute illicite de conversations. Un local isolé pour l'information sensible cloisonnée (LIISC) est un exemple de zone de travail sécurisée.

SC-15(04) — Indication explicite des participantes et participants (---)

Énoncés :

Fournir une indication explicite des participantes et participants actuels de [Affectation : réunions et téléconférences désignées par l'organisation].

Responsable : Aucun

Discussion :

L'indication explicite des participantes et participants actuels permet d'empêcher les personnes non autorisées de participer à des séances d'informatique collaborative à l'insu des autres participants.

SC-16 — Transmission des attributs de sécurité et de protection de la vie privée (---)

Énoncés :

Associer [Affectation : attributs de sécurité et de protection de la vie privée définis par l'organisation] à l'information échangée entre les systèmes et les composants du système.

Responsable : Aucun

Discussion :

Les attributs de sécurité et de protection de la vie privée peuvent être explicitement ou implicitement associés à l'information contenue dans le système ou les composants de systèmes de l'organisation. Les attributs sont des abstractions qui représentent les propriétés ou caractéristiques de base d'une entité pour ce qui a trait à la protection de l'information ou à la gestion des renseignements personnels. Les attributs sont normalement associés aux structures de données internes, notamment aux dossiers, à la mémoire tampon et aux fichiers dans le système. Les attributs de sécurité et de protection de la vie privée sont utilisés pour mettre en œuvre les stratégies de contrôle de l'accès et du flux d'information pour refléter la diffusion, la gestion ou la distribution spéciales des instructions, ce qui comprend l'utilisation ou la divulgation autorisée de renseignements personnels, et pour soutenir les autres aspects des stratégies de contrôle de l'accès et du flux d'information. Les attributs de protection de la vie privée peuvent être utilisés séparément ou avec les attributs de sécurité.

SC-16(01) — Vérification de l’intégrité (---)

Énoncés :

Vérifier l’intégrité des attributs de sécurité et de protection de la vie privée transmis.

Responsable : Aucun

Discussion :

Une partie du processus de vérification de l’intégrité de l’information transmise consiste à s’assurer que les attributs de sécurité et de protection de la vie privée qui sont associés à une telle information n’ont pas été modifiés d’une manière non autorisée. La modification non autorisée des attributs de sécurité et de protection de la vie privée peut donner lieu à une perte d’intégrité de l’information transmise.

SC-16(02) — Mécanismes anti-usurpation (---)

Énoncés :

Mettre en place des mécanismes anti-usurpation pour empêcher les adversaires de falsifier les attributs de sécurité qui indiquent l'application réussie du processus de sécurité.

Responsable : Aucun

Discussion :

Certains vecteurs d'attaque visent à modifier les attributs de sécurité d'un système d'information de manière à y déployer, de façon intentionnelle et malveillante, un niveau insuffisant de sécurité. La modification des attributs pousse les organisations à croire qu'un plus grand nombre de fonctions de sécurité sont en place et en service que ce qui a vraiment été mis en place.

SC-16(03) — Liaison cryptographique (---)

Énoncés :

Mettre en œuvre [Affectation : mécanismes ou techniques définis par l'organisation] pour lier les attributs de sécurité et de protection de la vie privée à l'information transmise.

Responsable : Aucun

Discussion :

Les mécanismes et les techniques cryptographiques peuvent fournir une liaison robuste des attributs de sécurité et de protection de la vie privée à l'information transmise pour aider à assurer l'intégrité d'une telle information.

SC-17 — Certificats d'infrastructure à clé publique (Nc--)

Énoncés :

a. Émettre des certificats à clé publique en vertu de [Affectation : stratégie de certification définie par l'organisation] ou les obtenir auprès d'un fournisseur de services autorisé
b. Inclure uniquement les ancrages de confiance approuvés dans les magasins de confiance ou les magasins de certificats gérés par l'organisation

Responsable : Aucun

Discussion :

Les certificats d'ICP sont des certificats disposant d'une visibilité à l'extérieur des systèmes organisationnels et des certificats ayant trait aux systèmes opérationnels internes, comme les services de synchronisation horaire propres aux diverses applications. Dans les systèmes cryptographiques dotés d'une structure hiérarchique, un ancrage de confiance est une source faisant autorité (c'est-à-dire une autorité de certification) pour laquelle la confiance est présumée et non dérivée. Le certificat racine d'un système d'ICP est un exemple d'ancrage de confiance. Un magasin de confiance ou de certificats permet de maintenir une liste des certificats racines autorisés.

SC-18 — Code mobile (---)

Énoncés :

a. Définir le code mobile et les technologies de code mobile acceptables et inacceptables
b. Autoriser, surveiller et contrôler l'utilisation de code mobile sur le système

Responsable : Aucun

Discussion :

Le code mobile comprend tout programme, application ou contenu qui peut être transmis par l'intermédiaire d'un réseau (par exemple, intégré dans un courriel, un document ou un site Web) et exécuté sur un système distant. Les décisions concernant le recours à du code mobile dans les systèmes organisationnels reposent sur la possibilité qu'une utilisation malveillante du code cause des dommages aux systèmes. Les technologies de code mobile incluent les applets Java, JavaScript, HTML5, WebGL et VBScript. Les restrictions d'utilisation et les lignes directrices sur la mise en œuvre s'appliquent à la sélection et à l'utilisation de code mobile installé sur les serveurs ainsi que de code mobile téléchargé et exécuté sur des postes de travail et des appareils individuels, dont des ordinateurs blocs-notes et des téléphones intelligents. La stratégie et les procédures liées au code mobile concernent les mesures prises afin d'empêcher le développement, l'acquisition et l'introduction de code mobile non acceptable au sein des systèmes organisationnels, ce qui comprend exiger la signature numérique du code mobile par une source de confiance.

SC-18(01) — Établissement du code inadéquat et application de mesures correctives (---)

Énoncés :

Identifier [Affectation : code mobile inadéquat défini par l'organisation] et prendre [Affectation : mesures correctives définies par l'organisation].

Responsable : Aucun

Discussion :

Les mesures correctives à prendre lorsque du code mobile inadéquat est détecté comprennent le blocage, la mise en quarantaine ou la notification des administratrices et administrateurs. Le blocage sert notamment à empêcher la transmission de fichiers de traitement de texte contenant des macros, dès lors que ces dernières ont été jugées comme étant du code mobile inadéquat.

SC-18(02) — Acquisition, développement et utilisation (---)

Énoncés :

Veiller à ce que l'acquisition, le développement ou l'utilisation du code mobile à déployer dans les systèmes répondent aux [Affectation : exigences relatives au code mobile définies par l'organisation].

Responsable : Aucun

SC-18(03) — Prévention du téléchargement et de l'exécution (---)

Énoncés :

Prévenir le téléchargement et l'exécution de [Affectation : code mobile inadéquat défini par l'organisation].

Responsable : Aucun

SC-18(04) — Prévention de l’exécution automatique (---)

Énoncés :

Empêcher l’exécution automatique de code mobile dans [Affectation : applications logicielles désignées par l’organisation] et exiger que [Affectation : mesures définies par l’organisation] soient prises avant d’exécuter le code.

Responsable : Aucun

Discussion :

Demander aux utilisatrices et utilisateurs de confirmer l’ouverture de pièces jointes dans les courriels ou la consultation de liens sur le Web est une des actions exigées avant l’exécution de code mobile. Prévenir l’exécution automatique de code mobile comprend la désactivation des fonctions d’exécution automatique des composants de systèmes qui ont recours à une technologie de supports amovibles.

SC-18(05) — Autoriser l’exécution dans les environnements clos seulement (---)

Énoncés :

Permettre l’exécution de code mobile autorisé uniquement dans les environnements clos de machines virtuelles.

Responsable : Aucun

Discussion :

Permettre l’exécution de code mobile uniquement dans les environnements clos de machines virtuelles aide à prévenir l’introduction de code malveillant dans d’autres systèmes et composants de systèmes.

SC-19 — Voix sur IP (---)

Énoncés :

a. L'organisation définit les restrictions d'utilisation et donne des conseils sur la mise en œuvre des technologies de voix sur protocole Internet (VoIP pour Voice over Internet Protocol) en tenant compte de la possibilité qu'une utilisation malveillante de ces technologies cause des dommages au système d'information
b. L'organisation autorise, surveille et contrôle l'utilisation de la voix sur IP dans le système d'information

Responsable : Aucun

SC-19(400) — Conversion de protocole (---)

Énoncés :

Il est interdit d'utiliser un service de VoIP non classifié dans des installations classifiées, sauf si ce service est converti en service téléphonique traditionnel (POTS pour Plain Old Telephone Service) avant de sortir des limites de l'installation.

Responsable : Aucun

SC-19(401) — Aucun accès au réseau public (---)

Énoncés :

Dans les installations classifiées, il est interdit d'utiliser un service de VoIP non classifié dans un réseau local ayant accès à un réseau de données public.

Responsable : Aucun

SC-20 — Service sécurisé de résolution de nom ou d'adresse (source faisant autorité) (---)

Énoncés :

a. Fournir des éléments additionnels d'information sur l'authentification de l'origine des données et sur la vérification de leur intégrité, en plus des données de résolution de nom faisant autorité, que le système retourne en réponse aux requêtes externes de résolution de nom ou d'adresse
b. Offrir des moyens d'indiquer l'état de sécurité des zones enfants et (si l'enfant prend en charge des services sécurisés de résolution) de vérifier l'existence d'une chaîne de confiance entre les domaines parents et enfants lorsque le système est utilisé dans un espace de nom hiérarchique distribué

Responsable : Aucun

Discussion :

Fournir de l'information tirée d'une source faisant autorité permet aux clients externes, comme les clients à distance provenant d'Internet, d'obtenir des assurances d'authentification de l'origine ou de vérification de l'intégrité pour l'information de résolution de nom d'hôte ou de service en adresse réseau obtenue par l'intermédiaire du service. Les systèmes qui fournissent les services de résolution de nom et d'adresse comprennent les serveurs DNS. Parmi les artéfacts additionnels, on retrouve les extensions de sécurité DNS (DNSSEC pour Domain Name System Security Extension), les signatures numériques et les clés cryptographiques. Les données faisant autorité comprennent les enregistrements des ressources liées au service DNS. L'utilisation d'enregistrements de ressource de signataire par délégation du service DNS est l'un des moyens permettant d'indiquer l'état de sécurité des zones enfants. Les systèmes qui utilisent des technologies autres que le service DNS pour mettre en correspondance les noms d'hôte ou de service et les adresses réseau offrent d'autres moyens d'assurer l'authenticité et l'intégrité des données des réponses.

SC-20(01) — Zones enfants (---)

Énoncés :

Annulé : Intégré au contrôle SC-20.

Responsable : Aucun

SC-20(02) — Intégrité et origine des données (---)

Énoncés :

Fournir les artéfacts de protection de l'intégrité et de l'origine des données pour les requêtes internes de résolution de nom ou d'adresse.

Responsable : Aucun

SC-21 — Service sécurisé de résolution de nom ou d'adresse (résolveur récursif ou cache) (---)

Énoncés :

Soumettre une requête, puis authentifier l'origine et vérifier l'intégrité des données des réponses de la résolution de nom et d'adresse que le système reçoit de sources faisant autorité.

Responsable : Aucun

Discussion :

Chaque client des services de résolution de nom ou d'adresse effectue cette vérification de façon autonome ou par des voies authentifiées menant à des fournisseurs de validation dignes de confiance. Les systèmes qui fournissent des services de résolution de nom et d'adresse pour les clients locaux incluent les serveurs DNS récursifs de résolution ou de mise en cache. Les résolveurs de clients de DNS exécutent une validation des signatures DNSSEC ou les clients utilisent des voies authentifiées vers des résolveurs récursifs qui se chargent de telles validations. Les systèmes qui utilisent des technologies autres que le DNS pour mettre en correspondance les noms d'hôte et de service et les adresses réseau offrent d'autres moyens d'assurer l'authenticité et l'intégrité des données des réponses.

SC-21(01) — Intégrité et origine des données (---)

Énoncés :

Annulé : Intégré au contrôle SC-21.

Responsable : Aucun

SC-22 — Architecture et prestation de services de résolution de nom ou d'adresse (---)

Énoncés :

S'assurer que les systèmes qui offrent collectivement des services de résolution de nom et d'adresse pour une organisation sont tolérants aux pannes et appliquent une séparation des rôles internes et externes.

Responsable : Aucun

Discussion :

Les systèmes qui fournissent les services de résolution de nom et d'adresse comprennent les serveurs DNS. Pour éliminer les points de défaillance uniques et améliorer la redondance, les organisations emploient au moins deux serveurs DNS faisant autorité dont l'un est configuré comme serveur principal et l'autre, comme serveur secondaire. De plus, les organisations déploient généralement les serveurs dans deux sous-réseaux faisant respectivement partie de réseaux situés dans des régions géographiques distinctes (par exemple, situés dans des installations physiques différentes). Pour ce qui est de la séparation des rôles, les serveurs DNS associés à des rôles internes exécutent uniquement le processus de résolution de nom et d'adresse pour les requêtes provenant de l'intérieur des organisations (c'est-à-dire provenant de clients internes). Les serveurs DNS associés à des rôles externes traitent uniquement les requêtes de résolution des clients à l'extérieur des organisations (c'est-à-dire en provenance de réseaux externes, y compris d'Internet). Les organisations désignent les clients qui peuvent accéder aux serveurs DNS faisant autorité dans certains rôles particuliers (par exemple, par plage d'adresses ou au moyen de listes explicites).

SC-23 — Authenticité des sessions (---)

Énoncés :

Protéger l'authenticité des sessions de communication.

Responsable : Aucun

Discussion :

La protection de l'authenticité des sessions vise à protéger les communications au niveau de la session plutôt qu'au niveau des paquets. Cette protection permet d'instaurer un niveau de confiance adéquat aux deux extrémités des sessions de communication quant à l'identité des autres parties et à la validité de l'information transmise. La protection de l'authenticité vise à protéger contre les attaques par interception, le détournement de session et l'insertion d'information erronée dans les sessions.

SC-23(01) — Annulation de la validation des identificateurs de session lors de la fermeture de session (---)

Énoncés :

Invalider les identificateurs de session lorsque l'utilisatrice ou utilisateur ferme sa session ou lorsque la session est terminée autrement.

Responsable : Aucun

Discussion :

L'invalidation des identificateurs de session lors de la fermeture de session réduit la capacité des adversaires à saisir et à poursuivre l'emploi d'identificateurs de session antérieurement valides.

SC-23(02) — Fermetures de session exécutées par les utilisatrices et utilisateurs et affichage de messages (---)

Énoncés :

Annulé : Intégré au contrôle AC-12(01).

Responsable : Aucun

SC-23(03) — Identificateurs de session uniques générés par le système (---)

Énoncés :

Générer un identificateur de session unique pour chaque session avec [Affectation : exigences relatives à la randomisation définies par l'organisation] et reconnaître uniquement les identificateurs générés par le système.

Responsable : Aucun

Discussion :

Générer des identificateurs de session uniques réduit la capacité des adversaires à réutiliser les identificateurs de session antérieurement valides. L'utilisation du concept aléatoire pour la génération d'identificateurs de session uniques permet de protéger le système contre les attaques par force brute visant à déterminer les futurs identificateurs de session.

SC-23(04) — Identificateurs de session uniques avec randomisation (---)

Énoncés :

Annulé : Intégré au contrôle SC-23(03).

Responsable : Aucun

SC-23(05) — Autorités de certification homologuées (---)

Énoncés :

Permettre uniquement l'utilisation de [Affectation : autorités de certification désignées par l'organisation] à des fins de vérification de l'établissement de sessions protégées.

Responsable : Aucun

Discussion :

Le fait de s'en remettre aux autorités de certification pour l'établissement de sessions sécurisées entraîne l'utilisation de certificats TLS. Après vérification auprès des autorités respectives, ces certificats facilitent l'établissement de sessions protégées entre les clients Web et les serveurs Web.

SC-24 — Défaillance dans un état connu (---)

Énoncés :

Échec de [Affectation : état connu du système défini par l'organisation] pour les défaillances suivantes des composants indiqués tout en préservant [Affectation : information relative à l'état du système définie par l'organisation] en défaillance : [Affectation : liste des types de défaillances du système définis par l'organisation sur les composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

La défaillance du système dans un état connu met en relief les questions de sécurité conformément à la mission ou aux besoins opérationnels des organisations. La défaillance dans un état connu prévient les pertes sur le plan de la confidentialité, de l'intégrité ou de la disponibilité dans les cas de défaillance des systèmes organisationnels ou de composants de systèmes. Elle permet également d'empêcher les systèmes de tomber en panne dans un état susceptible de causer des préjudices aux individus ou la destruction des biens. La protection de l'information relative à l'état du système facilite le redémarrage du système et le retour au mode opérationnel tout en perturbant le moins possible les processus liés à la mission ou aux activités.

SC-25 — Nœuds légers (---)

Énoncés :

Employer un minimum de fonctionnalités et de stockage d'information sur les composants de systèmes suivants : [Affectation : composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Le déploiement de composants de systèmes ayant une fonctionnalité minimale réduit la nécessité de sécuriser chaque point d'extrémité et peut atténuer les risques d'exposition de l'information, des systèmes et des services à des attaques. Une fonctionnalité réduite ou minimale comprend les nœuds sans disque et les technologies de client léger.

SC-26 — Leurres (---)

Énoncés :

Inclure des composants dans les systèmes organisationnels conçus spécifiquement pour servir de cibles aux attaques malveillantes dans le but de les détecter, de les repousser et de les analyser.

Responsable : Aucun

Discussion :

Les leurres (par exemple, les pièges à pirates, les réseaux leurres ou les faux réseaux) sont mis en place pour attirer les adversaires et détourner les attaques des systèmes d'exploitation qui soutiennent les fonctions liées à la mission et aux activités de l'organisation. L'utilisation de leurres exige le recours à certaines mesures d'isolation pour s'assurer que le code malveillant détourné n'a aucune incidence sur les systèmes organisationnels. Tout dépendant de l'usage particulier du leurre, une discussion préalable avec l'équipe des services juridiques du ministère pourrait être requise.

SC-26(01) — Détection de code malveillant (---)

Énoncés :

Annulé : Intégré au contrôle SC-35.

Responsable : Aucun

SC-27 — Applications indépendantes des plateformes (---)

Énoncés :

Inclure dans les systèmes organisationnels les applications qui sont indépendantes des plateformes suivantes : [Affectation : applications définies par l'organisation qui sont indépendantes des plateformes].

Responsable : Aucun

Discussion :

Les plateformes sont des combinaisons du matériel, des micrologiciels et de composants logiciels utilisés pour exécuter les logiciels d'application. Les plateformes comprennent les systèmes d'exploitation, les architectures d'ordinateur sous-jacentes, ou les deux. Les applications indépendantes des plateformes peuvent s'exécuter sur diverses plateformes. De telles applications favorisent la portabilité et la reconstitution sur des plateformes différentes, augmentant ainsi la disponibilité des fonctions essentielles au sein des organisations, lorsque des attaques sont lancées contre des systèmes s'exécutant sur des systèmes d'exploitation particuliers.

SC-28 — Protection de l'information au repos (Nc--)

Énoncés :

Protéger [Sélection (un choix ou plus) : la confidentialité; l'intégrité] de l'information au repos suivante : [Affectation : information au repos définie par l'organisation].

Responsable : Aucun

Discussion :

Par information au repos, on entend l'état de l'information lorsqu'elle n'est pas en cours de traitement, en transit ou stockée dans des composants du système. De tels composants comprennent les disques durs internes ou externes, les dispositifs réseau de stockage ou les bases de données. La protection de l'information au repos ne met toutefois pas l'accent sur le type de dispositif de stockage ou la fréquence d'accès, mais plutôt sur l'état de l'information. L'information au repos porte sur la confidentialité et l'intégrité de l'information, et concerne l'information relative aux utilisatrices et utilisateurs ainsi que celle relative aux systèmes. L'information relative aux systèmes nécessitant une protection comprend les configurations ou les ensembles de règles pour les pare-feu, les systèmes de détection et de prévention des intrusions, les routeurs de filtrage et le contenu d'authentification. Les organisations pourraient employer divers mécanismes pour assurer la protection de la confidentialité et de l'intégrité, y compris des mécanismes cryptographiques et l'analyse des échanges de fichiers. La protection de l'intégrité peut être assurée, par exemple, par la mise en oeuvre de technologies WORM (Write Once Read Many). S'il est impossible d'assurer une protection adéquate de l'information au repos d'une manière quelconque, les organisations peuvent utiliser d'autres contrôles, comme l'analyse fréquente pour relever le code malveillant au repos et le stockage hors site sécurisé plutôt que le stockage en ligne.

SC-28(01) — Protection cryptographique (Nc--)

Énoncés :

Mettre en place des mécanismes cryptographiques visant à prévenir la divulgation et la modification non autorisées de l'information au repos suivante sur [Affectation : composants de systèmes ou supports désignés par l'organisation] : [Affectation : information définie par l'organisation].

Responsable : Aucun

Discussion :

La sélection des mécanismes cryptographiques se fonde sur le besoin de protéger la confidentialité et l'intégrité de l'information organisationnelle. La robustesse d'un mécanisme correspond à la catégorie de sécurité et à la classification de l'information. Les organisations ont la souplesse nécessaire pour chiffrer l'information sur des composants de systèmes ou des supports, ou pour chiffrer les structures de données, y compris des fichiers, des dossiers ou des champs.

SC-28(02) — Stockage hors ligne (---)

Énoncés :

Supprimer l'information suivante des dispositifs de stockage en ligne et la stocker hors ligne dans des lieux sécurisés : [Affectation : information définie par l'organisation].

Responsable : Aucun

Discussion :

Le retrait de l'information organisationnelle des dispositifs de stockage en ligne élimine la possibilité que des individus parviennent à accéder sans autorisation à de l'information par l'intermédiaire d'un réseau. Par conséquent, les organisations peuvent choisir de déplacer leur information vers des dispositifs de stockage hors ligne au lieu de la protéger pendant qu'elle est enregistrée dans du stockage en ligne.

SC-28(03) — Clés cryptographiques (---)

Énoncés :

Protéger le stockage des clés cryptographiques [Sélection (un choix) : [Affectation : mesures de protection définies par l'organisation]; magasin de clés avec protection matérielle].

Responsable : Aucun

Discussion :

Un module de plateforme sécurisée (TPM pour Trusted Platform Module) est un exemple de magasin de données avec protection matérielle pouvant être utilisé pour protéger les clés cryptographiques.

SC-29 — Hétérogénéité (---)

Énoncés :

Employer un ensemble diversifié de technologies de l'information pour les composants de systèmes pendant la mise en œuvre du système : [Affectation : composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Accroître la diversité des technologies de l'information utilisées dans les systèmes organisationnels réduit les répercussions de l'exploitation potentielle d'une technologie en particulier. Une telle diversité offre une protection contre les défaillances de modes communs, dont les défaillances découlant d'attaques contre la chaîne d'approvisionnement. La diversité sur le plan des technologies de l'information réduit considérablement la probabilité que les moyens employés par les adversaires pour compromettre un composant de système soient efficaces contre d'autres composants de systèmes, exigeant du coup plus d'efforts de la part des adversaires pour mener à bien les attaques prévues. Un accroissement de la diversité peut ajouter en complexité et en charge de gestion, ce qui pourrait ultimement mener à des erreurs ou à des configurations non autorisées.

SC-29(01) — Techniques de virtualisation (---)

Énoncés :

Utiliser des techniques de virtualisation pour faciliter le déploiement de divers systèmes d'exploitation et de diverses applications faisant l'objet de changements [Affectation : fréquence définie par l'organisation].

Responsable : Aucun

Discussion :

Les changements fréquents apportés aux systèmes d'exploitation et aux applications peuvent poser des défis importants sur le plan de la gestion des configurations, mais ils ont l'avantage de compliquer la tâche des adversaires qui mènent des attaques. Les changements d'applications ou de systèmes d'exploitation virtuels, par opposition aux changements de véritables applications ou systèmes d'exploitation, engendrent des changements virtuels qui endiguent l'efficacité des attaques tout en réduisant les efforts de gestion des configurations. Les techniques de virtualisation peuvent aider à isoler les logiciels non fiables ou de provenance douteuse dans des environnements d'exécution clos.

SC-30 — Dissimulation et détournement (---)

Énoncés :

Employer les techniques de dissimulation et de détournement suivantes pour [Affectation : systèmes désignés par l'organisation] à [Affectation : périodes définies par l'organisation] : [Affectation : techniques de dissimulation et de détournement définies par l'organisation].

Responsable : Aucun

Discussion :

Les techniques de dissimulation et de détournement permettent de réduire considérablement la capacité de ciblage des adversaires (comme les créneaux et la surface d'attaque) qui préparent et lancent des cyberattaques. Par exemple, les techniques de virtualisation permettent aux organisations de dissimuler les systèmes et, éventuellement, de réduire la probabilité de réussite des attaques tout en évitant les coûts importants associés à la mise en place de plateformes multiples. L'usage accru des techniques de dissimulation et de détournement – notamment le facteur aléatoire, le facteur d'incertitude et la virtualisation – peut suffisamment confondre et désorienter les adversaires et, ultérieurement, accroître le risque de découverte ou d'exposition de leur savoir-faire. Les techniques de dissimulation et de détournement peuvent accroître le temps dont les organisations disposent pour effectuer les fonctions liées à la mission et aux activités de l'organisation. La mise en œuvre des techniques de dissimulation et de détournement sur un système peut ajouter en complexité et en charge de gestion.

SC-30(01) — Techniques de virtualisation (---)

Énoncés :

Annulé : Intégré au contrôle SC-29(01).

Responsable : Aucun

SC-30(02) — Facteur aléatoire (---)

Énoncés :

Employer [Affectation : techniques définies par l'organisation] pour introduire le facteur aléatoire dans la gestion des activités et des biens organisationnels.

Responsable : Aucun

Discussion :

Le facteur aléatoire introduit un niveau accru d'incertitude dans l'esprit des adversaires relativement aux mesures que les organisations prennent pour protéger leurs systèmes contre les attaques. En effet, de telles mesures peuvent freiner la capacité des adversaires à cibler correctement les ressources informationnelles des organisations qui assurent le soutien de fonctions essentielles liées à leurs missions et à leurs activités. L'incertitude peut également faire hésiter les adversaires avant de lancer ou de poursuivre des cyberattaques. Les techniques de détournement qui recourent au facteur aléatoire comprennent la prise de mesures de routine à divers moments de la journée, l'emploi de diverses technologies de l'information, le recours à différents fournisseurs et la rotation des rôles et des responsabilités au sein du personnel organisationnel.

SC-30(03) — Changement des lieux de traitement et de stockage (---)

Énoncés :

Changer l'emplacement du [Affectation : traitement et/ou stockage défini par l'organisation] [Sélection (un choix) : {Affectation : fréquence définie par l'organisation}; à intervalles irréguliers].

Responsable : Aucun

Discussion :

Les adversaires ciblent les fonctions liées à la mission et aux activités de l'organisation, ainsi que les systèmes qui soutiennent ces fonctions, tout en essayant de minimiser l'exposition de leurs activités et de leur savoir-faire. Les systèmes organisationnels qui sont par nature statiques, homogènes et prévisibles sont plus vulnérables aux attaques qui nécessitent peu d'efforts et de coûts de la part des adversaires pour être fructueuses. La modification des lieux de traitement et de stockage (également appelée défense par déplacement des cibles) prend en compte les menaces persistantes avancées qui font appel à diverses techniques, comme la virtualisation, le traitement distribué et la réplication. Cette approche permet aux organisations de relocaliser les composants de systèmes (c'est-à-dire le traitement ou le stockage) qui prennent en charge les fonctions essentielles liées aux missions et aux activités. Les changements de sites de traitement et de stockage sèment l'incertitude chez les adversaires pour ce qui est des cibles à préconiser lors d'éventuelles attaques. Cette incertitude accroît la somme de travail que les adversaires doivent investir et rend la compromission et la violation des systèmes organisationnels plus difficiles et chronophages. Elle accroît également les chances que ces mêmes adversaires dévoilent accidentellement certains aspects du savoir-faire qu'ils utilisent pour tenter de repérer les ressources organisationnelles essentielles.

SC-30(04) — Information trompeuse (---)

Énoncés :

Employer de l'information en apparence réelle, mais en définitive trompeuse, dans [Affectation : composants de systèmes désignés par l'organisation] au sujet de leur posture et de leurs mesures de sécurité.

Responsable : Aucun

Discussion :

Utiliser de l'information trompeuse vise à confondre les adversaires potentiels par rapport à la nature et à la portée des contrôles déployés par l'organisation. Les adversaires risquent ainsi d'employer des techniques d'attaque inadéquates et, par conséquent, inefficaces. Une technique dont les organisations disposent pour tromper les adversaires consiste à placer de l'information trompeuse au sujet de certains contrôles dans les systèmes externes connus pour être ciblés par les adversaires. Une autre technique consiste à recourir aux faux réseaux qui imitent certains aspects des vrais systèmes organisationnels, mais qui utilisent, par exemple, des configurations logicielles périmées.

SC-30(05) — Dissimulation des composants de systèmes (---)

Énoncés :

Employer les techniques suivantes pour cacher ou dissimuler [Affectation : composants de systèmes désignés par l'organisation] : [Affectation : techniques définies par l'organisation].

Responsable : Aucun

Discussion :

Par les mesures visant à cacher, à déguiser ou à dissimuler les composants de systèmes essentiels, les organisations se donnent les moyens de réduire la probabilité que les adversaires ciblent les biens organisationnels ou parviennent à les compromettre. Parmi les moyens de dissimulation des composants de systèmes, les organisations pourront recourir à la configuration de routeurs ou à l'utilisation du chiffrement ou de techniques de virtualisation.

SC-31 — Analyse des voies clandestines (---)

Énoncés :

a. Procéder à une analyse des voies clandestines dans le but d'identifier les éléments du système qui pourraient éventuellement constituer des voies clandestines de [Sélection (un choix ou plus) : stockage; synchronisation temporelle]
b. Évaluer la bande passante maximale de ces voies

Responsable : Aucun

Discussion :

Les développeuses et développeurs sont les mieux placés pour déterminer les parties des systèmes qui sont susceptibles d'être converties en voies clandestines. L'analyse des voies clandestines est une activité importante, lorsqu'il y a possibilité que des flux d'information non autorisés traversent des domaines de sécurité, comme dans le cas des systèmes qui contiennent de l'information à exportation contrôlée et qui sont connectés à des réseaux externes (c'est-à-dire les réseaux qui ne sont pas contrôlés par les organisations). L'analyse des voies clandestines est également utile pour les systèmes sécurisés multiniveaux, les systèmes à sécurité multiniveau et les systèmes interdomaines.

SC-31(01) — Test d’exploitabilité des voies clandestines (---)

Énoncés :

Tester un sous-ensemble de voies clandestines identifiées afin de savoir quelles voies s’avèrent exploitables.

Responsable : Aucun

SC-31(02) — Bande passante maximale (---)

Énoncés :

Réduire la bande passante maximale pour certaines voies clandestines de [Sélection (un choix ou plus) : stockage; synchronisation temporelle] à [Affectation : valeurs définies par l'organisation].

Responsable : Aucun

Discussion :

Il est généralement impossible d'éliminer entièrement les voies clandestines, en particulier celles de réglage, sans avoir une incidence importante sur les performances.

SC-31(03) — Mesure de la bande passante dans les environnements opérationnels (---)

Énoncés :

Mesurer la bande passante [Affectation : sous-ensemble de voies clandestines particulières défini par l'organisation] dans l'environnement opérationnel du système.

Responsable : Aucun

Discussion :

La mesure de la bande passante des voies clandestines dans des environnements opérationnels particuliers aide les organisations à établir les quantités d'information qui peuvent fuir clandestinement avant que la fuite ait une incidence sur les fonctions liées à la mission et aux activités de l'organisation. La bande passante des voies clandestines peut varier considérablement lorsqu'elle est mesurée selon des réglages qui sont indépendants des environnements opérationnels particuliers, ce qui comprend les laboratoires ou les environnements de développement de systèmes.

SC-32 — Partitionnement des systèmes (---)

Énoncés :

Partitionner le système en [Affectation : composants de systèmes désignés par l'organisation] résidant dans des domaines ou des environnements [Sélection (un choix) : physiques; logiques] basés sur [Affectation : circonstances propices à la séparation physique ou logique des composants définies par l'organisation].

Responsable : Aucun

Discussion :

Le partitionnement du système fait partie de la stratégie de protection en profondeur. Les organisations déterminent le degré de séparation physique des composants de système. Les options de séparation physique comprennent des composants physiquement distincts dans des bâtis séparés d'une même pièce, des composants critiques dans des pièces distinctes et la séparation géographique de composants critiques. La catégorisation de sécurité peut également guider la sélection des composants qui se prêtent le mieux au partitionnement de domaine. Les interfaces gérées limitent ou interdisent l'accès réseau et les flux d'information entre les composants partitionnés du système.

SC-32(01) — Séparation des domaines physiques pour les fonctions privilégiées (---)

Énoncés :

Partitionner les fonctions privilégiées dans des domaines physiques distincts.

Responsable : Aucun

Discussion :

Les fonctions privilégiées qui s'effectuent dans un seul domaine physique peuvent représenter un point de défaillance unique si ce domaine en venait à être compromis ou à faire l'objet d'un déni de service.

SC-33 — Intégrité de la préparation des transmissions (---)

Énoncés :

Annulé : Intégré au contrôle SC-08.

Responsable : Aucun

SC-34 — Programmes exécutables non modifiables (---)

Énoncés :

Pour les [Affectation:composants de systèmes désignés par l'organisation], charger et exécuter :
a. l'environnement d'exploitation à partir de supports matériels non inscriptibles
b. les applications suivantes à partir de supports matériels non inscriptibles : [Affectation : applications désignées par l'organisation]

Responsable : Aucun

Discussion :

L'environnement d'exploitation d'un système contient le code qui héberge les applications, comme les systèmes d'exploitation, les outils de gestion ou les moniteurs de machines virtuelles (c'est-à-dire les hyperviseurs). Il peut également renvoyer à certaines applications s'exécutant directement sur des plateformes matérielles. Les supports matériels non inscriptibles et les supports matériels non réinscriptibles comprennent les lecteurs de disques compacts inscriptibles (CD-R pour Compact Disc-Recordable), de disques numériques universels enregistrables (DVD-R pour Digital Versatile Disk-Recordable) et de disques Blu-Ray (BD-R), ainsi que la mémoire morte programmable (PROM pour Programmable Read-Only Memory) à utilisation unique. L'utilisation du stockage non modifiable garantit l'intégrité de l'aspect logiciel à partir du point de création de l'image en lecture seule. L'utilisation de mémoire morte reprogrammable peut être acceptée comme support non inscriptible dans la mesure où l'intégrité peut être adéquatement protégée depuis le point de l'inscription initiale jusqu'à l'insertion de la mémoire dans le système; et qu'il y a des mécanismes fiables de protection du matériel contre la reprogrammation de la mémoire tant que celle-ci est installée dans les systèmes organisationnels.

SC-34(01) — Dispositif de stockage non inscriptible (---)

Énoncés :

Utiliser [Affectation : composants de systèmes désignés par l'organisation] avec des dispositifs de stockage qui demeurent non inscriptibles à chaque redémarrage du composant ou lors des mises sous tension et hors tension.

Responsable : Aucun

Discussion :

Interdire le recours à des dispositifs de stockage inscriptibles élimine la possibilité d'insertion de code malveillant par une mémoire inscriptible persistante dans le composant de système désigné. La restriction s'applique aux mémoires de stockage fixes et amovibles, celles-ci étant utilisées directement ou selon les restrictions imposées par les contrôles d'accès des appareils mobiles.

SC-34(02) — Protection de l’intégrité et des supports non inscriptibles (---)

Énoncés :

Protéger l’intégrité de l’information avant son enregistrement dans les supports non inscriptibles et contrôler ces supports après l’enregistrement de l’information.

Responsable : Aucun

Discussion :

Les mécanismes de protection préviennent la substitution de supports dans les systèmes d’information ou empêchent la reprogrammation de supports non inscriptibles programmables avant leur installation dans les systèmes. Les mécanismes de protection comprennent, par exemple, une combinaison de prévention, de détection et de mesures d’intervention.

SC-34(03) — Protection matérielle (---)

Énoncés :

Annulé : Transféré sous le contrôle SC-51.

Responsable : Aucun

SC-35 — Identification des programmes malveillants externes (---)

Énoncés :

Inclure les composants de systèmes qui tentent proactivement d'identifier les programmes malveillants en provenance du réseau ou les sites Web malveillants.

Responsable : Aucun

Discussion :

L'identification des programmes malveillants externes diffère des leurres mentionnés dans le contrôle SC-26 dans la mesure où les composants analysent activement les réseaux, y compris Internet, à la recherche de code malveillant contenu sur les sites Web externes. Comme pour les leurres, le recours à des techniques d'identification des programmes malveillants externes exige la prise de mesures d'isolation pour s'assurer que tout code malveillant découvert lors de la recherche et exécuté par la suite n'a aucune incidence sur les systèmes organisationnels. La virtualisation est une technique courante qui permet de réaliser une telle isolation.

SC-36 — Traitement et stockage répartis (---)

Énoncés :

Répartir les composants de traitement et de stockage suivants dans plusieurs [Sélection (un choix) : lieux physiques; domaines logiques] : [Affectation : composants de traitement et de stockage désignés par l'organisation].

Responsable : Aucun

Discussion :

La répartition du traitement et du stockage dans plusieurs lieux physiques offre un certain degré de redondance ou de chevauchement pour les organisations. Par conséquent, la redondance et le chevauchement accroissent la somme de travail des adversaires qui cherchent à produire un effet négatif sur les activités, les biens ou le personnel de l'organisation. Le recours au traitement et au stockage répartis ne se fonde pas sur un lien central de traitement ou de stockage. Il permet plutôt un traitement et un stockage parallèles.

SC-36(01) — Techniques de scrutation (---)

Énoncés :

a. Avoir recours à des techniques de scrutation pour relever les anomalies, les erreurs et les compromissions dans les composants de traitement et stockage suivants : [Affectation : composants de traitement et de stockage répartis désignés par l'organisation]
b. Prendre les mesures suivantes lorsque des anomalies, des erreurs ou des compromissions sont identifiées : [Affectation : actions définies par l'organisation]

Responsable : Aucun

Discussion :

Le traitement et le stockage répartis peuvent servir à réduire la possibilité que des adversaires arrivent à compromettre la confidentialité, l'intégrité ou la disponibilité de l'information et des systèmes organisationnels. Cependant, les composants de traitement et de stockage répartis ne peuvent empêcher que des adversaires compromettent un ou plusieurs des composants. La scrutation permet de comparer les résultats de traitement au contenu de stockage des divers composants répartis. La scrutation permet d'identifier les anomalies, les erreurs ou les compromissions dans les composants de traitement et de stockage répartis.

SC-36(02) — Synchronisation (---)

Énoncés :

Synchroniser les systèmes ou les composants de systèmes suivants : [Affectation : systèmes ou composants de systèmes dupliqués désignés par l'organisation].

Responsable : Aucun

Discussion :

Les contrôles SC-36 et CP-09(06) exigent la duplication des systèmes ou des composants de systèmes dans des lieux répartis. La synchronisation de données et de services dupliqués et redondants aide à assurer que l'information contenue dans les lieux répartis peut être utilisée dans le cadre des fonctions liées à la mission ou aux activités de l'organisation, le cas échéant.

SC-37 — Voies d’acheminement hors bande (---)

Énoncés :

Employer les voies d’acheminement hors bande suivantes pour la distribution physique ou la transmission électronique de [Affectation : information, composants de systèmes ou dispositifs désignés par l’organisation] à [Affectation : personnel ou systèmes désignés par l’organisation] : [Affectation : voies d’acheminement hors bande définies par l’organisation].

Responsable : Aucun

Discussion :

Les voies d’acheminement hors bande comprennent les accès non réseau aux systèmes, les chemins réseaux qui sont physiquement séparés des chemins réseaux utilisés pour le trafic opérationnel ou les chemins non électroniques, comme Postes Canad
a. L’utilisation de voies d’acheminement hors bande contraste avec l’utilisation de voies intrabandes (c’est-à-dire les mêmes voies) qui servent au transport du trafic opérationnel courant. Les voies d’acheminement hors bande ne sont pas sujettes aux mêmes vulnérabilités ou expositions que les voies intrabandes. Par conséquent, les atteintes à la confidentialité, à l’intégrité ou à la disponibilité des voies intrabandes n’entraîneront pas la compromission des voies d’acheminement hors bande ni n’auront d’incidence négative sur celles-ci. Les organisations peuvent employer les voies d’acheminement hors bande pour la distribution ou la transmission de nombreux éléments organisationnels, notamment les identifiants et authentifiants; l’information sur la gestion des clés cryptographiques; les sauvegardes de systèmes et de données; les changements apportés à la gestion des configurations du matériel, des micrologiciels ou des logiciels; les mises à jour de sécurité; l’information sur la maintenance; et les mises à jour concernant la protection contre les programmes malveillants. Par exemple, les clés cryptographiques des fichiers chiffrés sont distribuées au moyen d’une voie différente que celle employée pour le fichier.

SC-37(01) — Assurance de la distribution et de la transmission (---)

Énoncés :

Employer [Affectation : contrôles définis par l'organisation] pour garantir que seuls [Affectation : personnel ou systèmes désignés par l'organisation] reçoivent l'information, les composants de systèmes ou les dispositifs suivants : [Affectation : systèmes, composants de systèmes ou dispositifs désignés par l'organisation].

Responsable : Aucun

Discussion :

Parmi les techniques qui permettent aux organisations de veiller à ce que seuls certains systèmes ou certaines personnes reçoivent de l'information, des composants de systèmes ou des dispositifs particuliers, on retrouve l'envoi d'authentifiants par l'entremise d'un service de messagerie approuvé tout en exigeant que la ou le destinataire produise une pièce d'identité avec photo délivrée par le gouvernement en guise de condition à la réception.

SC-38 — Sécurité des opérations (---)

Énoncés :

Employer les contrôles de sécurité des opérations suivants pour protéger l'information organisationnelle tout au long du cycle de vie de développement des systèmes : [Affectation : contrôles de sécurité des opérations définis par l'organisation].

Responsable : Aucun

Discussion :

La sécurité des opérations (OPSEC pour Operations Security) est un processus systématique par lequel il est possible d'empêcher d'éventuels adversaires d'accéder à l'information concernant les capacités et les intentions des organisations, et ce, par l'identification, le contrôle et la protection d'information généralement non classifiée portant spécifiquement sur la planification et l'exécution des activités organisationnelles de nature sensible. Le processus OPSEC en question comporte cinq étapes : identification de l'information essentielle, analyse des menaces, analyse des vulnérabilités, évaluation des risques et application des mesures de prévention appropriées. Les contrôles OPSEC s'appliquent aux systèmes organisationnels et aux environnements dans lesquels les systèmes sont utilisés. Les contrôles OPSEC protègent la confidentialité de l'information et visent, notamment, à limiter l'échange d'information avec les fournisseurs, les fournisseurs potentiels et d'autres intervenantes et intervenants non organisationnels. Parmi les exemples de fonctions essentielles à la mission ou aux activités de l'organisation, on retrouve les identités des utilisatrices et utilisateurs, l'utilisation de certains éléments, les fournisseurs, les processus relatifs à la chaîne d'approvisionnement, les exigences concernant les fonctions et la sécurité, les spécifications de conception des systèmes, les protocoles de tests et d'évaluation, ainsi que les détails concernant la mise en œuvre de contrôles de sécurité.

SC-39 — Isolation des processus (---)

Énoncés :

Maintenir un domaine d'exécution distinct pour chaque processus exécuté sur le système.

Responsable : Aucun

Discussion :

Les systèmes peuvent conserver des domaines d'exécution distincts pour chacun des processus d'exécution en attribuant un espace d'adressage à chacun de ces processus. Chaque processus de système dispose de son espace d'adressage de sorte que la communication entre les processus s'effectue de manière contrôlée par l'intermédiaire des fonctions de sécurité, ce qui empêche également qu'un processus en vienne à modifier le code d'exécution d'un autre processus. La conservation de domaines distincts pour l'exécution des processus est rendue possible grâce, notamment, à l'application d'espaces d'adressage distincts. Les technologies d'isolation des processus, comme la mise en bac à sable ou la virtualisation, séparent logiquement les logiciels et micrologiciels des autres logiciels, micrologiciels et données. L'isolation des processus permet de limiter l'accès des logiciels potentiellement non fiables aux autres ressources du système. La capacité de maintenir des domaines d'exécution distincts est offerte dans les systèmes d'exploitation commerciaux qui font appel aux technologies à processeurs multiétats.

SC-39(01) — Séparation du matériel (---)

Énoncés :

Mettre en place des mécanismes de séparation du matériel pour faciliter l'isolation des processus.

Responsable : Aucun

Discussion :

La séparation matérielle des processus de systèmes est généralement moins sujette à la compromission que la séparation logicielle, ce qui donne l'assurance que la séparation sera efficace. Les mécanismes de séparation du matériel comprennent la gestion matérielle de la mémoire.

SC-39(02) — Domaine d’exécution distinct pour chaque fil d’exécution (---)

Énoncés :

Conserver un domaine d’exécution distinct pour chacun des fils d’exécution dans [Affectation : traitement multifil défini par l’organisation].

Responsable : Aucun

SC-40 — Protection des liaisons sans fil (---)

Énoncés :

Protéger les [Affectation : liaisons sans fil définies par l'organisation] externes et internes contre les attaques suivantes qui visent les paramètres de signaux : [Affectation : types de paramètres de signaux définis par l'organisation ou références aux sources de telles attaques].

Responsable : Aucun

Discussion :

La protection des liaisons sans fil s'applique aux liaisons de communication internes et externes qui pourraient être visibles pour les personnes qui ne sont pas des utilisatrices et utilisateurs autorisés des systèmes. Les adversaires peuvent exploiter les paramètres de signaux des liaisons sans fil lorsque ceux-ci ne sont pas adéquatement protégés. Il existe de nombreuses façons d'exploiter les paramètres de signaux de liaisons sans fil dans le but de soutirer du renseignement, d'interrompre des services ou d'usurper l'identité d'utilisatrices et utilisateurs des systèmes. La protection des liaisons sans fil atténue l'incidence des attaques qui ciblent principalement les systèmes sans fil. Il pourrait être impossible d'appliquer les mesures de protection des liaisons sans fil de manière à satisfaire aux exigences de l'organisation en matière de sécurité, lorsque les organisations comptent sur des fournisseurs de services commerciaux pour des services de transmission considérés comme étant auxiliaires plutôt que des services dédiés.

SC-40(01) — Interférence électromagnétique (---)

Énoncés :

Mettre en œuvre des mécanismes cryptographiques visant à appliquer [Affectation : niveau de protection défini par l'organisation] dans le but de contrer les effets de l'interférence électromagnétique internationale.

Responsable : Aucun

Discussion :

La mise en œuvre de mécanismes cryptographiques visant à atténuer l'interférence électromagnétique permet de protéger les systèmes contre le brouillage intentionnel qui pourrait entraver ou gêner les communications, de sorte que les formes d'onde à spectre étalé qui servent à la protection antibrouillage du sans-fil soient impossibles à prévoir pour les personnes autorisées. La mise en œuvre de mécanismes cryptographiques pourrait incidemment contribuer à l'atténuation du brouillage accidentel causé par les émetteurs légitimes qui partagent le même spectre. Les exigences liées à la mission, les menaces prévues, les concepts d'opérations, de même que les lois, les décrets, les directives, la réglementation, les politiques et les normes, déterminent les niveaux de disponibilité des liaisons sans fil, la cryptographie requise et les performances.

SC-40(02) — Atténuation du potentiel de détection (---)

Énoncés :

Appliquer des mécanismes cryptographiques visant à réduire le potentiel de détection des liaisons sans fil [Affectation : niveau de réduction défini par l'organisation].

Responsable : Aucun

Discussion :

La mise en œuvre de mécanismes cryptographiques visant à réduire le potentiel de détection permet de masquer les communications et de protéger les émetteurs sans fil contre la géolocalisation. Elle veille également à ce que les formes d'ondes à spectre étalé, qui sont utilisées pour garantir une faible probabilité de détection, soient impossibles à prévoir pour les personnes non autorisées. Les exigences liées à la mission, les menaces prévues, les concepts d'opérations, de même que les lois, les décrets, les directives, la réglementation, les politiques et les normes applicables, déterminent les niveaux de disponibilité auxquels les liaisons sans fil seront indétectables.

SC-40(03) — Déception des communications par imitation ou par manipulation (---)

Énoncés :

Mettre en œuvre des mécanismes cryptographiques visant à identifier et à rejeter les transmissions sans fil qui constituent des tentatives délibérées de communications trompeuses par imitation ou par manipulation, qui sont fondées sur des paramètres de signaux.

Responsable : Aucun

Discussion :

La mise en œuvre de mécanismes cryptographiques visant à identifier et à rejeter les communications trompeuses par imitation ou par manipulation permet de garantir que les paramètres de signaux de transmissions sans fil sont impossibles à prévoir pour les personnes non autorisées. L'imprévisibilité réduit les risques d'occurrence des communications trompeuses par imitation ou par manipulation fondées sur les seuls paramètres de signaux.

SC-40(04) — Identification des paramètres de signaux (---)

Énoncés :

Mettre en œuvre des mécanismes cryptographiques visant à prévenir l'identification des [Affectation : émetteurs sans fil désignés par l'organisation] par l'utilisation des paramètres de signaux d'un émetteur.

Responsable : Aucun

Discussion :

La mise en œuvre de mécanismes cryptographiques visant à prévenir l'identification des émetteurs sans fil permet d'assurer une protection contre l'identification de l'unicité des émetteurs sans fil à des fins d'exploitation du renseignement ainsi que de veiller à ce que les modifications « anti-signature » apportées aux paramètres de signaux soient impossibles à prévoir pour les personnes non autorisées. Elle offre aussi l'anonymat, le cas échéant. Les techniques de signature d'émetteurs radioélectriques permettent d'identifier les paramètres propres à un signal d'émetteur dans le but d'établir la signature de ces émetteurs à des fins de surveillance et d'identification des missions ou des utilisatrices et utilisateurs.

SC-400 — Authentification de la source de l’entité (Nc--)

Énoncés :

Le système d’information permet à la ou au destinataire d’un message de vérifier l’identificateur présumé de la source dans un message.

Responsable : Aucun

Discussion :

L’authentification de la source empêche toute entité non autorisée d’envoyer un message en usurpant l’identité d’une autre entité. Ce contrôle s’applique aux communications non liées à une session et peut être appliqué aux protocoles de n’importe quelle couche, des paquets IP au courrier électronique. Par message, on entend toute communication entre deux entités.

SC-400(01) — Authentification de l’identifiant présumé (Nc--)

Énoncés :

L’authentification de l’identifiant présumé du message repose sur la cryptographie.

Responsable : Aucun

SC-400(02) — Signature numérique (---)

Énoncés :

L'organisation utilise la cryptographie validée selon le Programme de validation des modules cryptographiques (PVMC) pour la génération et la vérification des signatures numériques.

Responsable : Aucun

SC-400(03) — Mise en œuvre de l’authentification (---)

Énoncés :

L’organisation utilise la cryptographie et les protocoles approuvés par le Centre pour la cybersécurité pour effectuer l’authentification.

Responsable : Aucun

SC-401 — Systèmes de télécommunications non classifiés dans les installations sécurisées (---)

Énoncés :

a. Les systèmes de télécommunications non classifiés dans les installations sécurisées ne doivent ni laisser passer ni transmettre de discussions audio sensibles lorsqu'ils sont au repos et non utilisés. De plus, ils doivent être configurés de manière à en empêcher le contrôle ou l'activation externes. Les concepts de protection audio de type « combiné raccroché » mentionnés dans les publications 5002 et 5006 du CNSSI doivent être intégrés aux systèmes de télécommunications des installations sécurisées
b. Les systèmes et services téléphoniques non classifiés doivent être configurés de manière à empêcher les exploits techniques ou l'intrusion. De plus, ils doivent intégrer des contrôles d'accès physique et logiciels pour empêcher la divulgation ou la manipulation de la programmation système et des données stockées
c. L'organisation doit veiller à appliquer aux systèmes de télécommunications non classifiés les exigences particulières suivantes

1. assurer la protection audio de type « combiné raccroché » par l'utilisation d'équipement CNSSI 5006, de dispositifs de déconnexion approuvés CNSSI 5006, ou d'une configuration système CNSSI 5002 équivalente
2. assurer l'isolation par l'utilisation d'un système téléphonique informatisé doté d'un contrôle de configuration logicielle et matérielle, et d'un contrôle des rapports de vérification (enregistrement détaillé des données d'appel, rapports sur les données d'appel, etc.). La programmation système n'offre pas la capacité de placer ou de maintenir le combiné en position non raccrochée. La configuration du système doit faire en sorte d'identifier et d'atténuer toutes les vulnérabilités associées à l'état du combiné (raccroché ou non)
3. veiller à ce que l'équipement utilisé pour administrer les systèmes téléphoniques soit installé dans une zone dont l'accès est réservé au personnel autorisé. Lorsque les terminaux d'administration locaux (d'un système téléphonique informatisé) ne sont pas ou ne peuvent pas être hébergés dans la zone contrôlée, ni protégés contre les manipulations non autorisées, alors l'utilisation d'un équipement téléphonique approuvé CNSSI 5006 doit être exigée, quelle que soit la configuration du système téléphonique informatisé
4. veiller à ne pas utiliser la maintenance à distance à l'extérieur des installations sécurisées
5. veiller à ne pas utiliser de téléphones à haut-parleur ni de systèmes d'audioconférences avec les systèmes de télécommunications non classifiés dans les installations sécurisées.
6. veiller à ce que les fonctions utilisées pour la messagerie vocale ou les systèmes unifiés de messagerie soient configurées de manière à empêcher l'accès non autorisé aux ports de diagnostic distants ou à la tonalité d'invitation à numéroter interne
7. veiller à ce que les répondeurs téléphoniques (TAD) et les télécopieurs ne comportent pas de fonctions qui présentent des vulnérabilités sur le plan de la sécurité, comme la surveillance des locaux à distance, la programmation à distance ou autres fonctions similaires qui peuvent permettre un accès à distance aux sons de la pièce.

d. Tous les systèmes de télécommunications non classifiés et leurs infrastructures doivent être isolés physiquement et électriquement de tout système d'information ou de télécommunications classifié, conformément aux exigences du CNSS ou de toute autre norme de séparation appliquée au système d'information classifié en place
e. Il faut respecter les exigences de sécurité et les lignes directrices en matière d'installation formulées dans la publication CNSSI 5000 pour les systèmes de VoIP installés dans toute zone de sécurité physique où est traitée de l'information classifiée

Responsable : Aucun

SC-41 — Accès des ports et des périphériques d'entrée et de sortie (---)

Énoncés :

Procéder à une désactivation ou à un retrait [Sélection (un choix) : physique; logique] de [Affectation : ports de connexion ou périphériques d'entrée et de sortie désignés par l'organisation] sur les systèmes ou les composants de systèmes suivants : [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Désactiver ou retirer les ports de connexion et les périphériques d'entrée et de sortie (E/S) aide à prévenir l'exfiltration des renseignements contenus dans les systèmes et à empêcher l'introduction de code malveillant depuis ces ports ou périphériques. La désactivation ou le retrait physique des ports ou des périphériques est une mesure plus robuste que les approches logiques. Les exemples de ports de connexion comprennent les ports USB (Universal Serial Bus), Thunderbold et FireWire (IEEE 1394). Les exemples de périphériques d'E/S comprennent les lecteurs de disques optiques, les clés USB, les écrans et les souris.

SC-42 — Capacité des capteurs et données (---)

Énoncés :

a. Interdire [Sélection (un choix ou plus) : l'utilisation de dispositifs dotés de {Affectation : capacités de captation environnementale définies par l'organisation} dans {Affectation : installations, secteurs ou systèmes désignés par l'organisation}; l'activation à distance des capacités de captation environnementale sur les systèmes ou les composants de systèmes organisationnels, sauf pour les exceptions suivantes : {Affectation : exceptions définies par l'organisation pour lesquelles l'activation à distance de capteurs est permise}]
b. Indiquer explicitement l'utilisation de capteurs pour [Affectation : groupes d'utilisatrices et utilisateurs désignés par l'organisation]

Responsable : Aucun

Discussion :

La capacité de captation et les données connexes s'appliquent aux types de systèmes ou de composants de systèmes qui appartiennent à la catégorie des appareils mobiles, comme les téléphones cellulaires, les téléphones intelligents et les tablettes. Les appareils mobiles sont souvent dotés des capteurs capables de collecter et d'enregistrer des données relatives à l'environnement où les systèmes sont utilisés. Des capteurs sont souvent intégrés aux appareils mobiles, comme des microphones, des appareils photo, des récepteurs du système mondial de localisation (GPS pour Global Positioning System) et des accéléromètres. Même si les capteurs des appareils mobiles fournissent d'importantes fonctionnalités, ils peuvent être exploités par les adversaires pour obtenir de précieuses informations sur les personnes et sur les organisations s'ils sont activés furtivement. Par exemple, l'activation à distance de la fonction de GPS d'un appareil mobile pourrait permettre à un adversaire de surveiller les mouvements d'une personne. Les organisations pourraient interdire à quiconque d'apporter des téléphones cellulaires ou des appareils photo numériques dans l'enceinte de certaines installations ou dans certains secteurs contrôlés qui font partie d'installations servant au stockage d'information classifiée ou qui sont le lieu de conversation de données de nature sensible.

SC-42(01) — Signalement auprès du personnel ou des rôles autorisés (---)

Énoncés :

Veiller à ce que le système soit configuré de telle sorte que l'information ou les données collectées par [Affectation : capteurs désignés par l'organisation] ne soit signalées qu'au personnel ou aux rôles autorisés à cette fin.

Responsable : Aucun

Discussion :

Dans les situations où les capteurs sont activés par des personnes autorisées, il demeure malgré tout possible que l'information ou les données collectées par les capteurs soient acheminées à des entités non autorisées. Les organisations devraient s'assurer de mettre en place les contrôles nécessaires pour protéger les données des capteurs.

SC-42(02) — Utilisation autorisée (---)

Énoncés :

Employer les mesures suivantes pour que l'information ou les données collectées par [Affectation : capteurs désignés par l'organisation] ne soient utilisées qu'aux fins autorisées : [Affectation : mesures définies par l'organisation].

Responsable : Aucun

Discussion :

Les organisations devraient s'assurer de posséder l'autorité légitime pour toute utilisation ou divulgation des données des capteurs. L'information collectée par les capteurs pour une fin particulière pourrait être utilisée à des fins non autorisées. Par exemple, les capteurs GPS qui servent normalement à assurer le soutien à l'orientation du trafic pourraient être exploités par des adversaires qui cherchent à surveiller les déplacements d'individus. Parmi les mesures visant à atténuer de telles activités, on retrouve la formation permettant d'assurer que les personnes autorisées n'abusent pas de leurs pouvoirs et, dans les cas où les données des capteurs sont maintenues par des entités externes, que des restrictions contractuelles concernant l'utilisation de telles données sont en place.

SC-42(03) — Dispositifs interdits d'utilisation (---)

Énoncés :

Annulé : Intégré au contrôle SC-42.

Responsable : Aucun

SC-42(04) — Avis de collecte (---)

Énoncés :

Appliquer les mesures suivantes pour informer plus facilement les individus que leurs renseignements personnels ont été collectés par [Affectation : capteurs désignés par l'organisation] : [Affectation : mesures définies par l'organisation].

Responsable : Aucun

Discussion :

Il convient d'obtenir des conseils juridiques avant de procéder à la collecte de données de capteur sur des dispositifs fournis par l'employeur. Lorsque les personnes sont mises au courant que les capteurs organisationnels collectent des données, elles peuvent assurer une gestion plus efficace de leur vie privée. Les mesures peuvent comprendre des avis écrits traditionnels ou des configurations de capteur qui informent directement ou indirectement les utilisatrices et utilisateurs par l'entremise d'autres dispositifs que le capteur collecte de l'information. Il est important de considérer la clarté de l'avis.

SC-42(05) — Minimisation de la collecte (---)

Énoncés :

Employer des [Affectation : capteurs désignés par l'organisation] qui sont configurés pour minimiser la collecte de renseignements non nécessaires sur les individus.

Responsable : Aucun

Discussion :

Bien que les stratégies qui limitent l'utilisation autorisée puissent s'appliquer aux renseignements après leur collecte, le fait de réduire la collecte de renseignements non nécessaires permet d'atténuer les risques liés au respect de la vie privée et de la Charte, ainsi que le risque d'échec des contrôles découlant de ces stratégies.

SC-42(400) — Désactivation des zones de sécurité et de haute sécurité (---)

Énoncés :

S'assurer que l'organisation désactive tous les capteurs sur tous les dispositifs si ces derniers ne sont pas autorisés à traiter de l'information au plus haut niveau de classification dans la zone de sécurité ou de haute sécurité dans laquelle ils se trouvent.

Responsable : Aucun

SC-43 — Restrictions relatives à l'utilisation (---)

Énoncés :

a. Établir des restrictions concernant l'utilisation et les directives en matière de mise en œuvre pour les composants de système suivants : [Affectation : composants de systèmes désignés par l'organisation]
b. Autoriser, surveiller et contrôler l'utilisation de tels composants sur le système

Responsable : Aucun

Discussion :

Les restrictions concernant l'utilisation s'appliquent à tous les composants de système, y compris, mais sans s'y limiter, le code mobile, les appareils mobiles, l'accès sans fil et les périphériques câblés et sans fil (par exemple, photocopieurs, imprimantes, numériseurs, dispositifs optiques et autres technologies similaires). Les restrictions concernant l'utilisation et les directives en matière de mise en œuvre sont basées sur le potentiel des composants du système à causer des dommages au système et aident à s'assurer que seul le système autorisé est utilisé.

SC-44 — Chambres de détonation (---)

Énoncés :

Employer une chambre de détonation dans [Affectation : système, composant de système ou lieu désigné par l'organisation].

Responsable : Aucun

Discussion :

Les chambres de détonation, aussi appelées « environnements d'exécution dynamiques », permettent aux organisations d'ouvrir des fichiers joints à des courriels, d'exécuter des applications douteuses ou suspectes, ou d'exécuter des requêtes URL dans un environnement sûr et isolé ou dans des bacs à sable virtuels. Les environnements d'exécution protégés et isolés offrent les moyens d'établir si les fichiers joints ou les applications en question contiennent du code malveillant. Bien que les chambres de détonation soient liées au concept des faux réseaux, elles ne sont pas destinées à maintenir un environnement à long terme dans lequel des adversaires peuvent mener leurs activités tout en étant surveillés. Les chambres de détonation visent plutôt à identifier rapidement le code malveillant et à réduire la probabilité que le code en question se propage aux environnements opérationnels voire à empêcher radicalement de telles propagations.

SC-45 — Synchronisation temporelle des systèmes (Nc--)

Énoncés :

Synchroniser les horloges des systèmes et des composants de systèmes.

Responsable : Aucun

Discussion :

La synchronisation temporelle des horloges du système est essentielle à l'exécution appropriée de plusieurs services du système, comme les processus d'identification et d'authentification dont le contrôle de l'accès exige des certificats et des restrictions selon l'heure de la journée. Un déni de service ou l'impossibilité de refuser des certificats expirés peut survenir si les horloges ne sont pas correctement synchronisées entre les systèmes et les composants de systèmes. L'heure est souvent exprimée selon le temps universel coordonné (UTC pour Universal Time Coordinated) ou selon l'heure locale qui est un décalage par rapport à l'UTC. La granularité des mesures temporelles fait référence au degré de synchronisation entre les horloges du système et des horloges de référence, comme la synchronisation des horloges avec une précision à des centaines ou à des dizaines de millisecondes. Les organisations peuvent définir des granularités temporelles différentes pour les divers composants du système. Le service lié au temps peut s'avérer essentiel dans le cas d'autres capacités de sécurité comme le contrôle d'accès ainsi que l'identification et l'authentification, selon la nature des mécanismes employés pour soutenir ces capacités.

SC-45(01) — Synchronisation avec une source de temps faisant autorité (Nc--)

Énoncés :

a. Comparer les horloges système internes [Affectation : fréquence définie par l'organisation] en utilisant [Affectation : source de temps faisant autorité définie par l'organisation]
b. Synchroniser les horloges systèmes internes avec la source de temps faisant autorité si la différence temporelle est supérieure à [Affectation : période définie par l'organisation]

Responsable : Aucun

Discussion :

La synchronisation des horloges système internes avec la source de temps faisant autorité permet de synchroniser les horodatages des systèmes ayant de multiples horloges système de même que celles des systèmes connectés à un réseau.

SC-45(02) — Deuxième source de temps faisant autorité (---)

Énoncés :

a. Déterminer une deuxième source de temps faisant autorité dans une région géographique différente de la première source de temps faisant autorité
b. Synchroniser les horloges système internes avec la deuxième source de temps faisant autorité si la première n'est pas disponible

Responsable : Aucun

Discussion :

Il pourrait être nécessaire d'utiliser de l'information de géolocalisation pour déterminer que la deuxième source de temps faisant autorité se trouve dans une région géographique différente.

SC-46 — Application des stratégies interdomaines (---)

Énoncés :

Mettre en œuvre un mécanisme d'application des stratégies [Sélection (un choix) : physiquement; logiquement] entre les interfaces physiques et/ou réseau pour la connexion des domaines de sécurité.

Responsable : Aucun

Discussion :

Pour les mécanismes logiques d'application des stratégies, les organisations devraient éviter de créer un chemin logique entre les interfaces pour s'assurer qu'on ne puisse pas contourner le mécanisme d'application des stratégies. Pour les mécanismes physiques d'application des stratégies, il pourrait être nécessaire d'assurer la robustesse de l'isolation physique fournie par la mise en œuvre physique de l'application des stratégies pour prévenir la présence de voies clandestines logiques pénétrant dans le domaine de sécurité.

SC-46(400) — Transfert manuel de données (---)

Énoncés :

Limiter l'utilisation du transfert manuel de données.

Responsable : Aucun

Discussion :

Une SID de transfert permet de transférer automatiquement l'information de façon sécurisée entre différents domaines de sécurité. L'utilisation du transfert manuel de données devrait se limiter à des exigences particulières. Le fait de contourner les procédures de transfert appropriées et de transférer l'information au moyen d'un support amovible est généralement considéré comme étant un comportement inapproprié de la part de l'utilisatrice ou utilisateur. S'il est nécessaire de transférer l'information au moyen d'un support amovible pour satisfaire à un besoin opérationnel, les procédures effectuées doivent se conformer à ce qui est énoncé dans le document ITSB-112 du Centre pour la cybersécurité. Une utilisatrice ou un utilisateur autorisé peut procéder à un transfert manuel de données au moyen d'un support amovible, comme une clé USB. Le cas échéant, une SID hors ligne peut être utilisée pour analyser et nettoyer le support. Un tel transfert peut être utilisé, par exemple, lorsqu'il est nécessaire de transférer le correctif d'un logiciel ou la mise à jour d'un antivirus d'un support amovible à un domaine de sécurité isolé.

SC-47 — Chemins de communications secondaires (---)

Énoncés :

Mettre en place des [Affectation : chemins de communication secondaires définis par l'organisation] pour la fonction organisationnelle de commande et de contrôle et l'exploitation des systèmes.

Responsable : Aucun

Discussion :

Qu'il soit antagoniste ou non, un incident peut perturber les chemins de communications établis qui sont utilisés pour l'exploitation des systèmes et la fonction organisationnelle de commande et de contrôle. Les chemins de communication secondaires réduisent le risque que l'ensemble des chemins de communications soient touchés par le même incident. Par ailleurs, l'incapacité des responsables de l'organisation d'obtenir de l'information opportune sur les interruptions ou de fournir de l'orientation aux éléments opérationnels en temps opportun après un incident touchant un chemin de communication peut avoir une incidence sur la capacité de l'organisation à intervenir rapidement lors de tels incidents. Mettre en place des chemins de communication secondaires aux fins de commande et de contrôle, y compris désigner d'autres décideuses et décideurs si la personne principale n'est pas disponible et déterminer la portée et les limitations de leurs actions, peut grandement aider l'organisation à poursuivre ses activités et à prendre les mesures appropriées lors d'un incident.

SC-48 — Relocalisation des capteurs (---)

Énoncés :

Relocaliser [Affectation : capteurs et capacités de surveillance désignés par l'organisation] à [Affectation : emplacements désignés par l'organisation] dans les circonstances et les situations suivantes : [Affectation : conditions ou circonstances définies par l'organisation].

Responsable : Aucun

Discussion :

Les adversaires peuvent emprunter divers chemins et utiliser différentes approches lorsqu'ils se déplacent latéralement dans l'organisation (y compris ses systèmes) afin d'atteindre leur cible ou de tenter d'exfiltrer l'information organisationnelle. Les organisations disposent souvent d'un ensemble limité de capacités de surveillance et de détection et elles peuvent porter leur attention aux chemins d'infiltration ou d'exfiltration critiques ou probables. En employant les chemins de communication qui ne sont généralement pas surveillés par une organisation, un adversaire peut augmenter ses chances d'atteindre les objectifs qu'il s'est fixés. En relocalisant ses capteurs et ses capacités de surveillance dans de nouveaux emplacements, une organisation peut empêcher un adversaire d'atteindre ses objectifs. Les capteurs ou les capacités de surveillance peuvent être relocalisés selon le renseignement sur les menaces obtenu par l'organisation ou être relocalisés de façon aléatoire pour confondre d'adversaire et rendre son déplacement latéral dans le système ou l'organisation d'autant plus difficile.

SC-48(01) — Relocalisation dynamique des capteurs ou des capacités de surveillance (---)

Énoncés :

Relocaliser dynamiquement [Affectation : capteurs et capacités de surveillance désignés par l'organisation] à [Affectation : emplacements désignés par l'organisation] dans les circonstances et les situations suivantes : [Affectation : conditions ou circonstances définies par l'organisation].

Responsable : Aucun

SC-49 — Application de la séparation et des stratégies matérielles (---)

Énoncés :

Mettre en œuvre des mécanismes pour l'application de la séparation et des stratégies matérielles entre [Affectation : domaines de sécurité définis par l'organisation].

Responsable : Aucun

Discussion :

Les propriétaires de systèmes pourraient exiger des mécanismes plus forts et robustes pour assurer l'application de la séparation des domaines et des stratégies pour certains types de menaces et d'environnements d'exploitation. L'application de la séparation et des stratégies matérielles offre des mécanismes plus robustes que l'application de la sécurité et des stratégies logicielles.

SC-50 — Séparation imposée par logiciel et application de la stratégie (---)

Énoncés :

Mettre en œuvre des mécanismes pour la séparation imposée par logiciel et l'application de la stratégie entre [Affectation : domaines de sécurité définis par l'organisation].

Responsable : Aucun

Discussion :

Les propriétaires de systèmes pourraient exiger des mécanismes plus forts pour assurer l'application de la séparation des domaines et des stratégies pour certains types de menaces et d'environnements d'exploitation.

SC-51 — Protection matérielle (---)

Énoncés :

a. Appliquer la protection d'écriture matérielle pour [Affectation : composants micrologiciels de systèmes désignés par l'organisation]
b. Mettre en œuvre des procédures particulières pour [Affectation : personnes autorisées désignées par l'organisation] à désactiver manuellement la protection d'écriture matérielle contre les modifications des micrologiciels et à réactiver la protection d'écriture avant de revenir au mode opérationnel

Responsable : Aucun

SI

Intégrité des systèmes et des données

System and Information Integrity

SI-01 — Politique et procédures d'intégrité de l'information et des systèmes (---)

Énoncés :

a. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :

1. une politique d'intégrité de l'information et des systèmes [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables

2. des procédures visant à faciliter la mise en oeuvre de la politique d'intégrité de l'information et des systèmes ainsi que des contrôles connexes

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures d'intégrité de l'information et des systèmes

c. Passer en revue et mettre à jour, par rapport à l'intégrité de l'information et des systèmes :

1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La politique et les procédures d'intégrité de l'information et des systèmes abordent les contrôles de la famille SI qui ont été mis en oeuvre dans les systèmes et les organisations. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à l'élaboration de la politique et des procédures d'intégrité de l'information et des systèmes. En règle générale, les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin pour des politiques et des procédures propres à la mission ou au système. La politique peut être intégrée à la politique générale de sécurité et de protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures d'intégrité de l'information et des systèmes comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.

SI-02 — Correction des défauts (Nc--)

Énoncés :

a. Identifier, signaler et corriger les défauts du système
b. Tester les mises à jour logicielles et micrologicielles visant la correction des défauts pour en vérifier l'efficacité et les répercussions potentielles sur les systèmes avant leur application
c. Installer les mises à jour de sécurité appropriées des logiciels et des micrologiciels dans une période de [Affectation : période définie par l'organisation] suivant la date de publication des mises à jour
d. Intégrer la correction des défauts au processus de gestion des configurations de l'organisation

Responsable : Aucun

Discussion :

La nécessité de corriger les défauts du système s'applique à tous les types de logiciels et de micrologiciels. Les organisations identifient les systèmes touchés par les défauts logiciels, y compris les possibles vulnérabilités résultant de ces défauts, et font rapport de cette information au personnel responsable de la sécurité et de la protection de la vie privée de l'information. Les organisations envisagent d'établir un environnement contrôlé d'application de correctifs pour les systèmes essentiels à la mission. Les mises à jour liées à la sécurité incluent les correctifs, les ensembles de modifications provisoires et les signatures de code malveillant. Les organisations corrigent également le plus rapidement possible les défauts relevés durant les évaluations, la surveillance permanente, les activités liées aux interventions en cas d'incident ou le traitement des erreurs du système. En intégrant la correction des défauts aux processus de gestion des configurations, il est possible d'assurer le suivi et la vérification des mesures correctrices requises. Le délai défini par l'organisation pour les mises à jour de sécurité logicielles et micrologicielles peut varier en fonction de divers facteurs de risque, notamment, la catégorie de sécurité du système, la criticité de la mise à jour (c'est-à-dire la gravité de la vulnérabilité liée au défaut découvert), la tolérance au risque de l'organisation, la mission prise en charge par le système ou l'environnement de menace. Certains types de correctifs peuvent nécessiter plus de mises à l'essai que d'autres. Les organisations doivent déterminer le type de mises à l'essai nécessaires pour le type précis de correction des défauts considérés et le type de changements dont la configuration doit être gérée. La mise à l'essai de la correction des défauts permet d'analyser l'efficacité des mesures prises pour corriger des problèmes de sécurité et les effets secondaires possibles sur la fonctionnalité des systèmes et des composants de systèmes, leurs performances et leur exploitation. Au moment de mettre en oeuvre des activités d'atténuation, les organisations considèrent l'ordre et l'horaire des mises à jour pour valider leur exécution appropriée dans l'environnement du système et soutenir les besoins du système et du composant en matière de disponibilité (c'est-à-dire la mise en oeuvre d'une stratégie de déploiement progressive). Les organisations s'assurent que les mises à jour logicielles et micrologicielles proviennent de sources autorisées avant leur téléchargement. Dans le cadre de ces décisions de mise à l'essai, l'organisation détermine si les mises à jour logicielles ou micrologicielles proviennent de sources autorisées ayant les signatures numériques appropriées.

SI-02(01) — Gestion centrale (---)

Énoncés :

Annulé : Intégré au contrôle PL-09.

Responsable : Aucun

SI-02(02) — État automatisé de la correction des défauts (---)

Énoncés :

Déterminer si les mises à jour logicielles et micrologicielles de sécurité pertinentes ont été installées sur les composants de systèmes au moyen de [Affectation : mécanismes automatisés désignés par l'organisation] [Affectation : fréquence définie par l'organisation].

Responsable : Aucun

Discussion :

Les mécanismes automatisés peuvent déterminer l'état des défauts connus des composants de systèmes et en faire le suivi.

SI-02(03) — Délais de correction des défauts et repères liés aux mesures correctives (---)

Énoncés :

a. Mesurer le temps écoulé entre la détection de l'anomalie et sa correction
b. Fixer les repères suivants pour la prise de mesures correctives : [Affectation : repères définis par l'organisation]

Responsable : Aucun

Discussion :

Les organisations déterminent combien de temps est nécessaire pour corriger les défauts des systèmes, une fois que ces défauts ont été identifiés, puis fixent des repères (c'est-à-dire des délais de traitement) pour la prise de mesures correctives. Les repères peuvent être établis en fonction des types de défauts et de la gravité des possibles vulnérabilités si le défaut est exploitable.

SI-02(04) — Outils automatisés de gestion des correctifs (---)

Énoncés :

Avoir recours à des outils automatisés de gestion des correctifs pour faciliter la correction des défauts des composants de systèmes suivants : [Affectation : composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Avoir recours à des outils automatisés pour soutenir la gestion des correctifs aide à assurer l'application opportune et exhaustive des correctifs sur les systèmes.

SI-02(05) — Mises à jour logicielles ou micrologicielles automatiques (---)

Énoncés :

Installer [Affectation : mises à jour logicielles et micrologicielles de sécurité pertinentes définies par l'organisation] automatiquement sur [Affectation : composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Étant donné l'importance de maintenir l'intégrité et la disponibilité des systèmes, l'organisation doit tenir compte de la méthodologie employée pour procéder aux mises à jour automatiques. Les organisations trouvent l'équilibre entre le besoin de s'assurer que les mises à jour sont installées le plus tôt possible et le besoin de maintenir la gestion des configurations, tout en veillant à résoudre les possibles répercussions que pourraient avoir des mises à jour automatiques (c'est-à-dire la mise en œuvre d'une stratégie de déploiement progressive).

SI-02(06) — Retrait des versions antérieures des logiciels et des micrologiciels (---)

Énoncés :

Supprimer les versions antérieures de [Affectation : éléments logiciels et micrologiciels définis par l'organisation] une fois qu'une version mise à jour a été installée.

Responsable : Aucun

Discussion :

Les versions antérieures des logiciels ou des micrologiciels qui ne sont pas supprimées des systèmes après l'installation des mises à jour peuvent être exploitées par des adversaires. Certains produits peuvent supprimer automatiquement les versions antérieures des logiciels et des micrologiciels sur le système.

SI-02(07) — Analyse des causes fondamentales (---)

Énoncés :

a. Procéder à l'analyse des causes fondamentales pour relever les causes sous-jacentes des problèmes ou des défaillances
b. Élaborer les mesures nécessaires pour corriger les causes fondamentales du problème ou de la défaillance
c. Mettre en oeuvre les mesures nécessaires et surveiller leur mise en oeuvre pour en assurer l'efficacité

Responsable : Aucun

Discussion :

L'analyse des causes fondamentales comprend une vaste gamme d'approches, d'outils et de techniques visant à identifier systématiquement les causes sous-jacentes des problèmes ou des défaillances dans les systèmes et les composants de systèmes (c'est-à-dire le matériel, les logiciels et les micrologiciels). Les organisations tiennent compte de la gravité de l'incident pour déterminer la méthode d'analyse des causes fondamentales à utiliser et les délais dans lesquels il convient de mettre en oeuvre les mesures correctives. L'analyse des causes fondamentales comprend un échéancier, les signes précurseurs qui n'ont pas été relevés, les principales décisions, les écarts, les mesures d'atténuation et la vérification de l'efficacité. Les mesures visant à corriger la source du problème sont déployées et intégrées aux stratégies, aux procédures et aux mises en oeuvre des contrôles de l'organisation.

SI-03 — Protection contre les programmes malveillants (Nc--)

Énoncés :

a. Mettre en oeuvre des mécanismes de protection contre les programmes malveillants [Sélection (un choix ou plus) : basés sur les signatures; non basés sur les signatures] aux points d'entrée et de sortie du système afin de détecter et d'éliminer le code malveillant
b. Mettre à jour automatiquement les mécanismes de protection contre les programmes malveillants dès que de nouvelles versions sont disponibles, conformément à la stratégie et aux procédures organisationnelles de gestion des configurations
c. Configurer les mécanismes de protection contre les programmes malveillants de façon à :
  1. effectuer des analyses périodiques du système [Affectation : fréquence définie par l'organisation] et des analyses en temps réel des fichiers de sources externes aux [Sélection (un choix ou plus) : points d'extrémité; point d'entrée ou sortie du réseau] lors de leur téléchargement, de leur ouverture ou de leur exécution, conformément à la stratégie organisationnelle
  2. [Sélection (un choix ou plus) : bloquer le code malveillant; mettre en quarantaine le code malveillant; effectuer {Affectation : action définie par l'organisation}]; et envoyer une alerte à [Affectation : personnel ou rôles définis par l'organisation] suivant la détection de code malveillant
d. Traiter les faux positifs résultant de la détection et de l'élimination de code malveillant et leurs répercussions potentielles sur la disponibilité des systèmes

Responsable : Aucun

Discussion :

Les points d'entrée et de sortie du système comprennent les pare-feu, les serveurs d'accès à distance, les stations de travail, les serveurs de messagerie, les serveurs Web, les serveurs mandataires, les ordinateurs blocs-notes et les appareils mobiles. Le code malveillant comprend les virus, les vers, les chevaux de Troie et les logiciels espions. Le code malveillant peut également être codé sous différents formats, contenu dans des fichiers compressés ou cachés, ou encore dissimulé dans des fichiers en utilisant des techniques comme la stéganographie. Le code malveillant peut être inséré dans les systèmes de différentes façons, notamment par courriel, par Internet et au moyen de dispositifs de stockage portatifs. Les insertions de code malveillant surviennent lors de l'exploitation de vulnérabilités du système. Il existe une variété de technologies et de méthodes pour limiter ou éliminer les effets des attaques de code malveillant. Les mécanismes de protection contre le code malveillant comprennent des technologies basées ou non sur les signatures. Les mécanismes de détection non fondés sur les signatures comprennent des techniques d'IA utilisant des données heuristiques pour détecter, analyser et décrire les caractéristiques ou les comportements de programmes malveillants, et pour trouver des moyens de contrôler ces programmes en l'absence de signature ou si les signatures existantes ne sont pas efficaces. Le code malveillant polymorphique (c'est-à-dire le code pour lequel les signatures sont modifiées lors de la réplication) est un des cas où les signatures actives sont inexistantes ou inefficaces. Les technologies basées sur la réputation sont un exemple de mécanismes qui ne sont pas fondés sur les signatures. En plus des technologies mentionnées précédemment, la gestion omniprésente des configurations, les contrôles complets d'intégrité des logiciels et les logiciels anti-exploitation peuvent être efficaces pour empêcher l'exécution de code non autorisé. Le code malveillant peut être présent dans des logiciels COTS et dans des logiciels conçus sur mesure. Il peut comprendre des bombes logiques, des portes dérobées et d'autres types d'attaques susceptibles d'avoir des répercussions sur les fonctions liées à la mission et aux activités de l'organisation. Dans les situations où le code malveillant ne peut pas être détecté par les méthodes ou les technologies de détection, l'organisation doit miser sur d'autres types de contrôles, comme des pratiques de codage sécurisé, la gestion et le contrôle des configurations, les processus d'approvisionnement fiable et les pratiques de surveillance, pour s'assurer que le logiciel n'effectue que les fonctions prévues. Les organisations peuvent décider de prendre différentes mesures en réponse à la détection de code malveillant. Par exemple, les organisations peuvent définir des mesures à prendre lors de la détection d'un code malveillant dans le cadre d'une analyse périodique, de la détection de téléchargements malveillants ou de la détection d'éléments malveillants lors de l'ouverture ou de l'exécution de fichiers.

SI-03(01) — Gestion centrale (---)

Énoncés :

Annulé : Intégré au contrôle PL-09.

Responsable : Aucun

SI-03(02) — Mises à jour automatiques (---)

Énoncés :

Annulé : Intégré au contrôle SI-03.

Responsable : Aucun

SI-03(03) — Utilisatrices ou utilisateurs non privilégiés (---)

Énoncés :

Annulé : Intégré au contrôle AC-06(10).

Responsable : Aucun

SI-03(04) — Mises à jour effectuées seulement par des utilisatrices et utilisateurs privilégiés (---)

Énoncés :

Mettre à jour les mécanismes de protection contre les programmes malveillants uniquement lorsqu'une utilisatrice ou un utilisateur privilégié le demande.

Responsable : Aucun

Discussion :

Les mécanismes de protection contre les programmes malveillants appartiennent généralement à la catégorie des logiciels de sécurité et, à ce titre, sont mis à jour par le personnel de l'organisation qui possède les privilèges d'accès appropriés.

SI-03(05) — Dispositifs de stockage portatifs (---)

Énoncés :

Annulé : Intégré au contrôle MP-07.

Responsable : Aucun

SI-03(06) — Tests et vérifications (---)

Énoncés :

a. Tester les mécanismes de protection contre les programmes malveillants [Affectation : fréquence définie par l'organisation] en introduisant du code bénin connu dans le système
b. Vérifier que la détection du code et le signalement des incidents qui lui sont associés s'effectuent comme il se doit

Responsable : Aucun

SI-03(07) — Détection non axée sur les signatures (---)

Énoncés :

Annulé : Intégré au contrôle SI-03.

Responsable : Aucun

SI-03(08) — Détection des commandes non autorisées (---)

Énoncés :

a. Détecter les commandes non autorisées du système d'exploitation dans l'interface de programmation d'application du noyau de [Affectation : composants matériels des systèmes désignés par l'organisation] : [Affectation : commandes non autorisées du système d'exploitation définies par l'organisation]
b. [Sélection (un choix ou plus) : Émettre un avertissement; vérifier l'exécution de la commande; empêcher l'exécution de la commande]

Responsable : Aucun

Discussion :

La détection des commandes non autorisées peut être appliquée aux interfaces essentielles autres que les interfaces axées sur le noyau, y compris les interfaces avec machines virtuelles et applications privilégiées. Les commandes non autorisées des systèmes d'exploitation comprennent les commandes pour des fonctions du noyau provenant de processus du système auxquels on n'accorde pas la confiance nécessaire pour initialiser de telles commandes, ainsi que les commandes pour des fonctions du noyau qui semblent suspectes, mêmes si les commandes de ce type pourraient vraisemblablement être initialisées par ces processus. L'organisation peut faire en sorte que la détection des commandes malveillantes soit effectuée à partir d'une combinaison de types de commandes, de classes de commandes ou d'occurrences précises de commandes. L'organisation peut également définir les composants matériels à partir de types de composants, de composants, de leur emplacement dans le réseau ou d'une combinaison de ces éléments. L'organisation peut choisir entre différentes mesures en fonction du type, de la classe ou de l'occurrence des commandes malveillantes.

SI-03(09) — Authentification des commandes à distance (---)

Énoncés :

Annulé : Transféré sous le contrôle AC-17(10).

Responsable : Aucun

SI-03(10) — Analyse des programmes malveillants (---)

Énoncés :

a. Employer des outils et des techniques pour analyser les caractéristiques et les comportements des programmes malveillants : [Affectation : techniques et outils définis par l'organisation]
b. Intégrer les résultats des analyses des programmes malveillants au processus d'intervention en cas d'incident et de correction des défauts de l'organisation

Responsable : Aucun

Discussion :

L'application des outils d'analyse des programmes malveillants offre aux organisations une connaissance plus approfondie du savoir-faire de leurs adversaires (c'est-à-dire leurs tactiques, techniques et procédures) et du fonctionnement et des buts de certains programmes malveillants en particulier. Comprendre les caractéristiques des programmes malveillants facilite les interventions effectuées par l'organisation pour contrer les menaces actuelles et à venir. L'organisation peut effectuer des analyses des programmes malveillants en se servant de techniques de rétro-ingénierie ou en surveillant le comportement du code malveillant que l'on exécute.

SI-04 — Surveillance des systèmes (---)

Énoncés :

a. Surveiller le système afin de détecter :
- **1.** des attaques et des signes indiquant de possibles attaques conformément aux objectifs de surveillance : [Affectation : objectifs de surveillance définis par l'organisation]
- **2.** des connexions locales, réseau ou à distance non autorisées

b. Détecter les utilisations non autorisées du système au moyen des techniques et des méthodes suivantes : [Affectation : techniques et méthodes définies par l'organisation]
c. Évoquer les capacités de surveillance interne ou déployer des dispositifs de surveillance :
- **1.** stratégiquement dans le système pour collecter l'information que l'organisation juge essentielle
- **2.** de manière aléatoire pour faire le suivi des types de transactions qui l'intéressent particulièrement

d. Analyser les anomalies et les événements détectés
e. Ajuster le niveau d'activité de la surveillance du système lorsqu'il y a un changement dans le risque associé aux activités et aux biens organisationnels, aux individus, à d'autres organisations ou au gouvernement
f. Obtenir un avis juridique concernant les activités de surveillance des systèmes
g. Fournir [Affectation : renseignements liés à la surveillance du système définis par l'organisation] à [Affectation : personnel ou rôles définis par l'organisation] [Sélection (un choix ou plus) : au besoin; {Affectation : fréquence définie par l'organisation}]

Responsable : Aucun

Discussion :

La surveillance du système est à la fois interne et externe. La surveillance externe comprend l'observation des événements qui surviennent dans les interfaces externes du système. La surveillance interne comprend l'observation des événements qui se produisent à l'intérieur du système. Les organisations surveillent le système en observant les activités liées à la vérification en temps réel ou en observant d'autres aspects du système, comme les tendances d'accès, les caractéristiques d'accès et d'autres opérations. Les objectifs de la surveillance orientent et éclairent la détermination des événements. La capacité de surveillance du système est possible grâce à une variété d'outils et de techniques, notamment les systèmes de détection et de prévention des intrusions, les logiciels de protection contre le code malveillant, les outils d'analyse, les logiciels de surveillance des enregistrements de vérification et les logiciels de surveillance des réseaux. Selon l'architecture de sécurité, la distribution et la configuration des dispositifs de surveillance peuvent avoir une incidence sur le débit aux principales frontières internes et externes, ainsi qu'à d'autres emplacements du réseau en raison de l'introduction de la latence du débit sur le réseau. S'il est nécessaire de gérer le débit, de tels dispositifs sont stratégiquement placés et déployés dans le cadre d'une infrastructure de sécurité panorganisationnelle établie. Les dispositifs de surveillance sont déployés à des emplacements stratégiques, notamment dans des emplacements du périmètre sélectionnés et près des principaux serveurs et des batteries de serveurs qui prennent en charge les applications essentielles. Les dispositifs de surveillance sont habituellement employés aux interfaces gérées associées aux contrôles SC-07 et AC-
- **17.** L'information collectée est déterminée par les objectifs de surveillance de l'organisation et la capacité des systèmes de prendre en charge de tels objectifs. Des types précis de transactions d'intérêt comprennent, par exemple, le trafic du protocole de transfert hypertexte (HTTP pour Hypertext Transfer Protocol) qui contourne les mandataires HTTP. La surveillance des systèmes fait partie intégrante des programmes de surveillance continue et d'intervention en cas d'incident de l'organisation et les résultats d'une telle surveillance servent de fondement à ces programmes. Les exigences en matière de surveillance du système, dont la surveillance selon le type de système, peuvent se trouver dans d'autres contrôles (par exemple, les contrôles AC-02G, AC-02(07), AC-02(12)a, AC-17(01), AU-13, AU-13(01), AU-13(02), CM-03F, CM-06D, MA-03A, MA-04A, SC-05(03)b, SC-07A, SC-07(24)b, SC-18B et SC-43B). Les ajustements apportés aux niveaux de surveillance du système sont basés sur des renseignements relatifs au maintien de l'ordre, du renseignement brut ou d'autres sources d'information. La légalité des activités de surveillance du système repose sur les lois, les décrets, les directives, la réglementation, les politiques, les normes et les lignes directrices applicables.

SI-04(01) — Système de détection d’intrusion dans l’ensemble du système (---)

Énoncés :

Connecter et configurer les outils individuels de détection d’intrusion en un système de détection panorganisationnel.

Responsable : Aucun

Discussion :

Combiner les outils individuels de détection d’intrusion en un système panorganisationnel unique permet d’offrir une plus grande couverture et des capacités de détection efficaces additionnelles. L’information contenue dans un outil de détection d’intrusion peut être partagée dans l’ensemble de l’organisation, ce qui rend la capacité de détection panorganisationnelle plus robuste et puissante.

SI-04(02) — Outils et mécanismes automatisés aux fins d'analyse en temps réel (---)

Énoncés :

Utiliser des outils et mécanismes automatisés pour prendre en charge l'analyse des événements en temps quasi réel.

Responsable : Aucun

Discussion :

Les outils et mécanismes automatisés comprennent les outils et mécanismes de surveillance des événements basés sur l'hôte, le réseau, le transport ou le stockage, ou les technologies de GIES offrant des analyses en temps réel des alertes ou des notifications générées par les systèmes organisationnels. Des techniques de surveillance automatisées peuvent faire courir des risques d'atteinte à la vie privée inattendus, puisque les contrôles automatisés peuvent se connecter à des systèmes externes ou indépendants. La mise en correspondance des enregistrements entre ces systèmes peut établir des recoupements et entraîner des conséquences imprévues. Les organisations évaluent et documentent ces risques dans leur EFVP et prennent des décisions conformément à leur plan du programme de protection de la vie privée.

SI-04(03) — Intégration d’outils et de mécanismes automatisés (---)

Énoncés :

Employer des outils et des mécanismes automatisés afin d’intégrer des outils et mécanismes de détection d’intrusion dans les mécanismes de contrôle d’accès et de flux.

Responsable : Aucun

Discussion :

L’utilisation d’outils et de mécanismes automatisés pour intégrer les outils et mécanismes de détection d’intrusion aux mécanismes de contrôle d’accès et de flux facilite une intervention rapide lors d’attaques en permettant la reconfiguration de ces mécanismes en vue d’isoler et d’éliminer rapidement les attaques.

SI-04(04) — Trafic de communications entrant et sortant (---)

Énoncés :

a. Déterminer les critères à utiliser pour détecter les activités ou conditions inhabituelles ou non autorisées relatives au trafic de communications entrant et sortant
b. Surveiller le trafic de communications entrant et sortant [Affectation : fréquence définie par l'organisation] pour détecter toute [Affectation : activité ou condition inhabituelle ou non autorisée définie par l'organisation]

Responsable : Aucun

Discussion :

Les activités ou conditions inhabituelles ou non autorisées liées au trafic de communications entrant et sortant du système comprennent le trafic interne qui indique la présence de code malveillant ou l'utilisation non autorisée de code ou de justificatifs légitimes dans des systèmes organisationnels, ou la propagation sur des composants de système, le signalement de systèmes externes et l'exportation non autorisée de l'information. Les preuves du code malveillant ou de l'utilisation non autorisée de code ou de justificatifs légitimes permettent de détecter les systèmes ou les composants de systèmes potentiellement compromis.

SI-04(05) — Alertes générées par le système (---)

Énoncés :

Alerter [Affectation : personnel ou rôles définis par l'organisation] lorsque les indications de compromission réelle ou potentielle suivantes se présentent : [Affectation : indicateurs de compromission définis par l'organisation].

Responsable : Aucun

Discussion :

Les alertes peuvent provenir de sources diverses, comme des enregistrements de vérification ou des mécanismes de protection contre les programmes malveillants, des mécanismes de détection ou de prévention des intrusions, ou des dispositifs de protection des frontières, tels les pare-feu, les passerelles et les routeurs. Les alertes peuvent être envoyées automatiquement ou être transmises par téléphone, par courriel ou par message texte. Le personnel organisationnel sur la liste de notification des alertes peut comprendre les administratrices et administrateurs de système, les propriétaires responsables de la mission et des activités, les propriétaires de système, les propriétaires, gardiennes ou gardiens de l'information, les hauts fonctionnaires du ministère responsables de la gouvernance de la sécurité, les hauts fonctionnaires ou cadres supérieures ou supérieurs en matière de protection de la vie privée, ou les responsables de la protection de la vie privée. Contrairement aux alertes générées par le système, les alertes générées par les organisations dans le contrôle SI-04(12) mettent l'accent sur les sources d'information externes au système, comme les rapports des activités suspectes et les rapports sur les menaces internes potentielles.

SI-04(06) — Restriction des utilisatrices et utilisateurs non privilégiés (---)

Énoncés :

Annulé : Intégré au contrôle AC-06(10).

Responsable : Aucun

SI-04(07) — Réponse automatisée à des événements suspects (---)

Énoncés :

a. Informer [Affectation : personnel responsable de l'intervention en cas d'incident désigné par l'organisation (par nom ou rôle)] des événements suspects ayant été détectés
b. Prendre les mesures suivantes lors de la détection : [Affectation : mesures les moins perturbatrices définies par l'organisation visant à mettre fin aux événements suspects]

Responsable : Aucun

Discussion :

Les mesures les moins perturbatrices comprennent l'envoi de demandes d'intervention du personnel.

SI-04(08) — Protection de l’information de surveillance (---)

Énoncés :

Annulé : Intégré au contrôle SI-04.

Responsable : Aucun

SI-04(09) — Mise à l'essai des outils et des mécanismes de surveillance (---)

Énoncés :

Mettre à l'essai les outils et les mécanismes de surveillance des intrusions [Affectation : fréquence définie par l'organisation].

Responsable : Aucun

Discussion :

Il est nécessaire de tester les outils et les mécanismes de surveillance des intrusions pour s'assurer qu'ils fonctionnent correctement et qu'ils répondent toujours aux objectifs de l'organisation en matière de surveillance. La fréquence et la profondeur des tests dépendent du type d'outils et de mécanismes dont l'organisation se sert et des méthodes de déploiement des outils et des mécanismes.

SI-04(10) — Visibilité des communications chiffrées (---)

Énoncés :

Prendre les mesures nécessaires pour rendre [Affectation : trafic de communications chiffrées défini par l'organisation] visible aux [Affectation : mécanismes et outils de surveillance du système désignés par l'organisation].

Responsable : Aucun

Discussion :

Les organisations trouvent un équilibre entre le besoin de chiffrer le trafic de communications et de protéger la confidentialité des données, et celui d'avoir accès au trafic pour en effectuer la surveillance. L'organisation détermine si l'exigence en matière de visibilité s'applique au trafic chiffré interne, au trafic chiffré qui sera envoyé à l'externe ou à un sous-ensemble de types de trafic.

SI-04(11) — Analyse des anomalies du trafic de communications (---)

Énoncés :

Analyser le trafic de communications sortant des interfaces externes au système et [Affectation : points internes dans le système définis par l'organisation] afin de relever les anomalies.

Responsable : Aucun

Discussion :

Les points internes définis par l'organisation comprennent les sous-réseaux et les sous-systèmes. Les anomalies dans les systèmes organisationnels comprennent les transferts de fichiers volumineux, les connexions permanentes à long terme, les tentatives d'accès à l'information depuis des emplacements inattendus, l'utilisation de protocoles et de ports inhabituels, l'utilisation de protocoles réseau non surveillés (par exemple, l'utilisation du protocole IPv6 lors d'une transition au protocole IPv4) et les tentatives de communication avec des adresses externes présumées malveillantes.

SI-04(12) — Alertes automatisées générées par l'organisation (---)

Énoncés :

Alerter [Affectation : personnel ou rôles définis par l'organisation] au moyen de [Affectation : mécanismes automatisés définis par l'organisation] lors de répercussions potentielles des activités inhabituelles ou inappropriées suivantes sur la sécurité ou la protection de la vie privée : [Affectation : liste définie par l'organisation des activités inhabituelles ou inappropriées qui déclenchent des alertes].

Responsable : Aucun

Discussion :

Le personnel organisationnel sur la liste de notification des alertes comprend les administratrices et administrateurs de système, les propriétaires responsables de la mission ou des activités, les propriétaires de système, les hauts fonctionnaires du ministère responsables de la sécurité de l'information, les hauts fonctionnaires ou cadres supérieures ou supérieurs en matière de protection de la vie privée, les responsables de la sécurité des systèmes ou les responsables de la protection de la vie privée. Par alertes automatisées générées par l'organisation, on entend les alertes de sécurité générées par les organisations et celles diffusées par l'intermédiaire de moyens automatisés. Les sources des alertes générées par l'organisation mettent l'accent sur les autres entités, comme les rapports des activités suspectes et les rapports sur les menaces internes potentielles. Contrairement aux alertes générées par l'organisation, les alertes générées par le système dans le contrôle SI-04(05) mettent l'accent sur les sources d'information qui sont internes aux systèmes, comme les enregistrements de vérification.

SI-04(13) — Analyse des modèles de trafic et d'événements (---)

Énoncés :

a. Analyser les modèles de trafic et d'événements pour le système
b. Développer des profils représentant les modèles de trafic et d'événements communs
c. Utiliser les profils de trafic et d'événements pour calibrer les dispositifs de surveillance des systèmes

Responsable : Aucun

Discussion :

Relever et comprendre les modèles de trafic de communication et d'événements aide les organisations à fournir de l'information utile aux dispositifs de surveillance des systèmes afin de relever le trafic et les événements suspects ou anormaux lorsqu'ils surviennent. Une telle information peut aider à réduire le nombre de faux positifs et de faux négatifs durant la surveillance des systèmes.

SI-04(14) — Détection d’intrusion sans fil (---)

Énoncés :

Utiliser un système de détection d’intrusions sans fil (WIDS pour Wireless Intrusion Detection System) pour identifier les dispositifs sans fil indésirables et détecter les tentatives d’attaque et les compromissions ou infractions potentielles liées au système.

Responsable : Aucun

Discussion :

Les signaux sans fil peuvent se propager au-delà des frontières des installations de l’organisation. L’organisation doit rechercher proactivement les connexions sans fil non autorisées, et exécuter des analyses rigoureuses pour détecter les points d’accès sans fil non autorisés. Les analyses sans fil ne se limitent pas nécessairement aux installations qui hébergent les systèmes, mais peuvent être effectuées à l’extérieur pour vérifier que des points d’accès sans fil non autorisés ne sont pas connectés au système organisationnel.

SI-04(15) — Communications entre un réseau sans fil et un réseau filaire (---)

Énoncés :

Utiliser un système de détection d'intrusion pour surveiller le trafic de communications sans fil lorsqu'il passe d'un réseau sans fil à un réseau filaire.

Responsable : Aucun

Discussion :

Les réseaux sans fil sont fondamentalement moins sécurisés que les réseaux filaires. Par exemple, les réseaux sans fil sont plus susceptibles de faire l'objet d'une écoute clandestine ou d'une analyse du trafic que les réseaux filaires. Dans le cas de communications sans fil à filaires, le réseau sans fil devrait devenir un port d'entrée du réseau câblé. Étant donné qu'il est plus facile d'obtenir un accès non autorisé au réseau depuis des points d'accès sans fil que des points d'accès câblés, il pourrait être nécessaire de procéder à une surveillance accrue du trafic acheminé entre les réseaux sans fil et câblés pour détecter les activités malveillantes. Utiliser des systèmes de détection d'intrusion pour surveiller le trafic des communications sans fil aide à garantir que le trafic ne contienne aucun code malveillant avant de traverser le réseau filaire.

SI-04(16) — Corrélations entre les résultats des activités de surveillance (---)

Énoncés :

Établir des corrélations entre les outils et les mécanismes de surveillance employés dans l'ensemble du système.

Responsable : Aucun

Discussion :

Établir des corrélations entre les résultats des différents outils et mécanismes de surveillance des systèmes peut fournir une vue d'ensemble plus complète des activités se déroulant dans le système. Établir des corrélations entre les outils et les mécanismes de surveillance qui travaillent habituellement de manière isolée – notamment, les logiciels de protection contre les programmes malveillants, la surveillance des hôtes et la surveillance des réseaux – peut fournir une vue d'ensemble de l'organisation et révéler des modèles d'attaques qui seraient autrement restés inaperçus. Comprendre les capacités et les limites de différents outils et mécanismes de surveillance et savoir comment maximiser l'utilisation des renseignements générés par ces outils et mécanismes peut aider l'organisation à mettre sur pied, exploiter et maintenir des programmes de surveillance efficaces. La corrélation de l'information sur la surveillance est particulièrement importante lorsque les organisations passent des anciennes aux nouvelles technologies (par exemple, la transition des protocoles réseau IPv4 à IPv6).

SI-04(17) — Connaissance intégrée de la situation (---)

Énoncés :

Mettre en corrélation les résultats de la surveillance des activités physiques, des cyberactivités et des activités de la chaîne d'approvisionnement pour développer une connaissance intégrée de la situation à l'échelle organisationnelle.

Responsable : Aucun

Discussion :

Établir des corrélations entre l'information résultant d'activités de surveillance provenant de sources plus diverses permet d'obtenir une connaissance intégrée de la situation. Une connaissance intégrée de la situation basée sur des activités de surveillance physique, de cybersurveillance et de surveillance de la chaîne d'approvisionnement améliore la capacité de l'organisation de détecter plus rapidement les attaques sophistiquées et d'enquêter sur les méthodes et techniques utilisées par les attaquants. Contrairement au contrôle SI-04 (16) qui vise à établir des corrélations entre les différentes informations liées à la cybersurveillance, une connaissance intégrée de la situation met en corrélation des éléments qui n'appartiennent pas uniquement au cyberdomaine. La corrélation entre l'information sur la surveillance et les multiples activités permet de révéler les attaques contre les organisations menées par les auteurs de menace dont les activités s'étendent dans plusieurs vecteurs d'attaque.

SI-04(18) — Analyse du trafic et exfiltrations masquées (---)

Énoncés :

Analyser le trafic des communications sortant en destination des interfaces externes du système et des points intérieurs suivants pour y détecter des exfiltrations masquées d'information : [Affectation : points intérieurs dans le système définis par l'organisation].

Responsable : Aucun

Discussion :

Les points internes définis par l'organisation comprennent les sous-réseaux et les sous-systèmes. Par masqué, on entend un procédé qui peut être utilisé pour exfiltrer l'information, comme la stéganographie.

SI-04(19) — Risque envers les personnes (---)

Énoncés :

Mettre en œuvre [Affectation : surveillance supplémentaire définie par l'organisation] des personnes qui ont été identifiées par [Affectation : sources définies par l'organisation], car elles représentent un plus grand risque.

Responsable : Aucun

Discussion :

On peut se fier à diverses sources pour déterminer si une personne pose de plus grands risques qu'une autre, comme les dossiers du personnel, les organismes de renseignement, les organismes d'application de la loi et d'autres sources crédibles. La surveillance des personnes est coordonnée avec les cadres supérieures et supérieurs de la gestion, des services juridiques, de la sécurité, de la protection des renseignements personnels et des ressources humaines, qui procèdent à une telle surveillance. La surveillance est effectuée conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables.

SI-04(20) — Utilisatrice ou utilisateur privilégié (---)

Énoncés :

Mettre en oeuvre la surveillance supplémentaire suivante des utilisatrices et utilisateurs privilégiés : [Affectation : surveillance supplémentaire définie par l'organisation].

Responsable : Aucun

Discussion :

Les utilisatrices et utilisateurs privilégiés ont accès à de l'information plus sensible, comme l'information liée à la sécurité, que le reste des utilisatrices et utilisateurs généraux. L'accès à une telle information signifie que les utilisatrices et utilisateurs privilégiés peuvent potentiellement causer des dommages plus grands aux systèmes et aux organisations que les utilisatrices ou utilisateurs non privilégiés. Par conséquent, la mise en oeuvre d'une surveillance supplémentaire des utilisatrices et utilisateurs privilégiés permet de s'assurer que les organisations peuvent relever les activités malveillantes le plus rapidement possible et prendre les mesures appropriées.

SI-04(21) — Périodes d’essai (---)

Énoncés :

Mettre en œuvre la surveillance supplémentaire suivante des personnes pendant [Affectation : période probatoire définie par l’organisation] : [Affectation : surveillance supplémentaire définie par l’organisation].

Responsable : Aucun

Discussion :

Au cours des périodes probatoires, la situation d’emploi des employées et employés n’est pas permanente au sein des organisations. La surveillance accrue des personnes dont la situation d’emploi n’est pas permanente ou qui ne peuvent accéder à l’information qui réside sur le système peut aider à relever les activités potentiellement malveillantes ou les comportements inappropriés.

SI-04(22) — Services réseau non autorisés (---)

Énoncés :

a. Détecter les services réseau qui n'ont pas été autorisés ou approuvés par [Affectation : processus d'autorisation et d'approbation définis par l'organisation]
b. [Sélection (un choix ou plus) : Vérifier; Alerter {Affectation : personnel ou rôles définis par l'organisation}] lorsqu'une menace est détectée

Responsable : Aucun

Discussion :

Les services réseau non autorisés ou non approuvés comprennent, les services dans les architectures axées sur le service qui manquent de vérification ou de validation organisationnelle et qui pourraient donc être non fiables ou servir d'agent malveillant infiltré dans un service légitime.

SI-04(23) — Dispositifs au niveau de l'hôte (---)

Énoncés :

Mettre en œuvre les mécanismes de surveillance au niveau de l'hôte suivants sur [Affectation : composants de systèmes désignés par l'organisation] : [Affectation : mécanismes de surveillance au niveau de l'hôte désignés par l'organisation].

Responsable : Aucun

Discussion :

La surveillance au niveau de l'hôte collecte l'information concernant l'hôte (ou le système dans lequel il réside). Les composants de systèmes dans lesquels la surveillance au niveau de l'hôte peut être mise en œuvre comprennent les ordinateurs blocs-notes et les appareils mobiles. L'organisation pourrait envisager d'employer des mécanismes de surveillance au niveau de l'hôte provenant de plusieurs développeuses, développeurs ou fournisseurs de produits.

SI-04(24) — Indicateurs de compromission (---)

Énoncés :

Découvrir, collecter et distribuer à [Affectation : personnel ou rôles définis par l'organisation] les indicateurs de compromission fournis par [Affectation : sources définies par l'organisation].

Responsable : Aucun

Discussion :

Les indicateurs de compromissions sont des artéfacts judiciaires des intrusions qui ont été relevées dans le système de l'organisation au niveau de l'hôte ou du réseau. Ils fournissent de l'information précieuse sur les systèmes qui ont été compromis. Les indicateurs de compromission peuvent comprendre la création de valeurs de clés de Registre. Les indicateurs de compromission du trafic réseau comprennent des éléments du localisateur de ressources uniformes (URL pour Universal Resource Locator) ou du protocole qui indiquent que les serveurs ont reçu des instructions de commande et de contrôle (C2) d'un programme malveillant. L'adoption et la distribution rapides des indicateurs de compromission peuvent améliorer la sécurité de l'information en réduisant le laps de temps pendant lequel les systèmes et les organisations sont vulnérables aux mêmes exploits ou attaques. Les indicateurs de menace, les tactiques, les techniques, les procédures et les autres indicateurs de compromission peuvent être accessibles dans le cadre de coopérations gouvernementales et non gouvernementales, comme le Forum of Incident Response and Security Teams (FIRST), l'Échange canadien de menaces cybernétiques (ECMC) et le ministère de la Cybersécurité et du Numérique (MCN) en tant qu'équipe d'intervention en cas d'urgence informatique (CERT-QC).

SI-04(25) — Optimisation de l’analyse du trafic réseau (---)

Énoncés :

Fournir de la visibilité du trafic réseau aux interfaces des systèmes externes et internes clés afin d’optimiser l’efficacité des dispositifs de surveillance.

Responsable : Aucun

Discussion :

Le trafic chiffré, les architectures de routage asymétriques, les limites relatives aux capacités et à la latence, et la transition des anciennes aux nouvelles technologies (par exemple, la transition des protocoles réseau IPv4 à IPv6) peuvent donner lieu à des zones de vulnérabilité au moment d’analyser le trafic réseau. Limiter la collecte, le déchiffrement, le prétraitement et la distribution du trafic pertinent aux dispositifs de surveillance peut simplifier l’efficacité et l’utilisation des dispositifs et optimiser l’analyse du trafic.

SI-05 — Alertes, avis et directives de sécurité (---)

Énoncés :

a. Recevoir régulièrement de [Affectation : organisations externes désignées par l'organisation] des alertes, des avis et des directives de sécurité concernant les systèmes
b. Générer les alertes, les avis et les directives de sécurité internes, au besoin
c. Diffuser les alertes, les avis et les directives de sécurité à : [Sélection (un choix ou plus) : {Affectation : personnel ou rôles définis par l'organisation}; {Affectation : éléments au sein de l'organisation définis par l'organisation}; {Affectation : organisations externes désignées par l'organisation}]
d. Mettre en œuvre les directives de sécurité dans les délais prescrits ou informer l'organisation émettrice du degré de non-respect

Responsable : Aucun

Discussion :

Le CERT-QC produit les alertes et les avis de sécurité visant à assurer une connaissance de la situation dans l'ensemble du gouvernement. Les directives de sécurité sont émises par le ministère de la Cybersécurité et du Numérique (MCN) ou d'autres organisations désignées ayant la responsabilité et l'autorité d'émettre de telles directives. La conformité aux directives de sécurité est essentielle en raison de la nature critique d'un grand nombre de ces directives et des effets néfastes immédiats possibles sur les opérations et les biens organisationnels, sur les utilisatrices et utilisateurs, sur d'autres organisations et sur l'ensemble du pays dans l'éventualité où les directives ne sont pas mises en œuvre rapidement. Les organisations externes comprennent les partenaires de la chaîne d'approvisionnement, les partenaires externes de la mission ou des activités, les fournisseurs de services externes et les autres organisations homologues ou de soutien.

SI-05(01) — Alertes et avis automatisés (---)

Énoncés :

Utiliser [Affectation : mécanismes automatisés définis par l'organisation] pour diffuser l'information contenue dans les alertes et les avis de sécurité à l'ensemble de l'organisation.

Responsable : Aucun

Discussion :

Le nombre important de changements aux systèmes organisationnels et aux environnements opérationnels font en sorte qu'il est nécessaire de diffuser de l'information concernant la sécurité à une vaste gamme d'entités organisationnelles pour qui la réussite des fonctions liées à la mission et aux activités de l'organisation est de première importance. En fonction de l'information fournie par les alertes et les avis de sécurité, il peut s'avérer nécessaire d'effectuer des changements à chacun des trois niveaux hiérarchiques de la gestion des risques liés à la sécurité de l'information, comme le niveau de gouvernance, le niveau du processus lié à une mission à une activité, ou le niveau du système d'information.

SI-06 — Vérification des fonctions de sécurité et de protection de la vie privée (---)

Énoncés :

a. Vérifier l'exploitation correcte de [Affectation : fonctions de sécurité et de protection de la vie privée définies par l'organisation]
b. Procéder à la vérification des fonctions indiquées dans le contrôle SI-06A [Sélection (un choix ou plus) : {Affectation : états transitionnels du système définis par l'organisation}; à la demande d'une utilisatrice ou un utilisateur qui possède les privilèges appropriés; {Affectation : période définie par l'organisation}]
c. Alerter [Affectation : personnel ou rôles définis par l'organisation] advenant l'échec des tests de vérification de la sécurité et de la protection de la vie privée
d. [Sélection (un choix ou plus) : Arrêter le système; Redémarrer le système; {Affectation : autres mesures définies par l'organisation}] lorsque des anomalies sont relevées

Responsable : Aucun

Discussion :

Les états transitionnels des systèmes comprennent notamment le démarrage, le redémarrage, l'arrêt et l'interruption. Les notifications du système comprennent les voyants lumineux sur le matériel, les alertes électroniques à l'intention des administratrices et administrateurs de systèmes et les messages affichés sur les consoles locales. Contrairement à la vérification des fonctions de sécurité, la vérification des fonctions de protection de la vie privée veille à s'assurer que les fonctions de protection de la vie privée fonctionnent comme prévu et sont approuvées par la ou le haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée approprié, ou que les attributs de protection de la vie privée sont appliqués ou utilisés comme prévu.

SI-06(01) — Notification des tests de sécurité infructueux (---)

Énoncés :

Annulé : Intégré au contrôle SI-06.

Responsable : Aucun

SI-06(02) — Soutien automatisé pour les tests distribués (---)

Énoncés :

Mettre en œuvre des mécanismes automatisés pour soutenir la gestion des tests distribués des fonctions de sécurité et de protection de la vie privée.

Responsable : Aucun

Discussion :

L'utilisation des mécanismes automatisés pour soutenir la gestion des tests de fonctionnalité distribués permet d'assurer l'intégrité, l'opportunité, l'exhaustivité et l'efficacité de ces tests.

SI-06(03) — Rapports sur les résultats des vérifications (---)

Énoncés :

Faire rapport des résultats de la vérification des fonctions de sécurité et de protection de la vie privée à [Affectation : personnel ou rôles définis par l'organisation].

Responsable : Aucun

Discussion :

Parmi les membres du personnel de l'organisation pour qui les résultats de la vérification des fonctions de sécurité et de protection de la vie privée pourraient représenter une question d'intérêt, on compte les agentes et agents de sécurité des systèmes, les hauts fonctionnaires dans la gouvernance de la sécurité du ministère et les hauts fonctionnaires ou cadres supérieures et supérieurs en matière de protection de la vie privée.

SI-07 — Intégrité des logiciels, des micrologiciels et de l'information (---)

Énoncés :

a. Employer des outils de vérification pour détecter les changements non autorisés qui sont apportés aux logiciels, aux micrologiciels et à l'information suivants : [Affectation : logiciels, micrologiciels et information désignés par l'organisation]
b. Prendre les mesures suivantes lorsque des changements non autorisés sont détectés dans les logiciels, les micrologiciels et l'information : [Affectation : actions définies par l'organisation]

Responsable : Aucun

Discussion :

Les changements non autorisés apportés aux logiciels, aux micrologiciels et à l'information peuvent être dus à des erreurs ou à des activités malveillantes. Les logiciels comprennent les systèmes d'exploitation (y compris les composants internes comme les noyaux ou les pilotes), les intergiciels et les applications. Les interfaces de micrologiciel comprennent l'interface micrologicielle extensible unifiée (UEFI pour Unified Extensible Firmware Interface) et le système de base d'entrée/sortie (BIOS pour Basic Input/Output System). L'information comprend les renseignements personnels et les métadonnées qui contiennent les attributs de sécurité et de protection de la vie privée associés à l'information. Les mécanismes de vérification de l'intégrité – y compris les vérifications de la parité, les vérifications cycliques de la redondance, les hachages cryptographiques et les outils connexes – peuvent automatiquement surveiller l'intégrité des systèmes et des applications hébergées.

SI-07(01) — Contrôles d’intégrité (---)

Énoncés :

Effectuer un contrôle de l’intégrité de [Affectation : logiciels, micrologiciels et information définis par l’organisation] [Sélection (un choix ou plus) : au démarrage; à {Affectation : états transitionnels ou événements touchant la sécurité définis par l’organisation}; {Affectation : fréquence définie par l’organisation}].

Responsable : Aucun

Discussion :

Les événements touchant la sécurité comprennent, l’identification de nouvelles menaces envers lesquelles les systèmes sont vulnérables et l’installation de nouveaux logiciels, matériel ou micrologiciels. Les états transitionnels comprennent le démarrage, le redémarrage, l’arrêt et l’interruption.

SI-07(02) — Automatisation des avis d'atteinte à l'intégrité (---)

Énoncés :

Utiliser des outils automatisés qui notifient [Affectation : personnel ou rôles définis par l'organisation] lors de la découverte d'écarts durant la vérification de l'intégrité.

Responsable : Aucun

Discussion :

L'utilisation d'outils automatisés pour signaler les atteintes à l'intégrité des systèmes et de l'information et pour avertir le personnel de l'organisation en temps opportun est essentielle pour assurer une intervention efficace contre les risques. Parmi les membres du personnel pour qui les atteintes à l'intégrité de l'information et des systèmes représentent une question d'intérêt, on compte les propriétaires responsables de la mission et des activités, les propriétaires des systèmes, les hauts fonctionnaires dans la gouvernance de la sécurité du ministère, les hauts fonctionnaires ou cadres supérieures et supérieurs en matière de protection de la vie privée appropriés, les administratrices et administrateurs de système, les développeuses et développeurs de logiciels, les intégratrices et intégrateurs de systèmes, les responsables de la sécurité de l'information et les responsables de la protection de la vie privée.

SI-07(03) — Outils de vérification de l’intégrité gérés centralement (---)

Énoncés :

Utiliser des outils de vérification de l’intégrité gérés centralement.

Responsable : Aucun

Discussion :

Les outils de vérification de l’intégrité gérés centralement offrent une plus grande conformité dans l’application de tels outils et peuvent faciliter une couverture plus exhaustive des mesures liées à la vérification de l’intégrité.

SI-07(04) — Emballage avec sceau d’inviolabilité (---)

Énoncés :

Annulé : Intégré au contrôle SA-12.

Responsable : Aucun

SI-07(05) — Automatisation des interventions en cas d'atteinte à l'intégrité (---)

Énoncés :

[Sélection (un choix ou plus) : Arrêter le système; Redémarrer le système; Mettre en œuvre {Affectation : contrôles définis par l'organisation}] automatiquement lorsque des atteintes à l'intégrité sont relevées.

Responsable : Aucun

Discussion :

Les organisations peuvent définir les différentes réponses aux vérifications de l'intégrité selon le type d'information, des renseignements précis ou une combinaison des deux. Les types d'information comprennent les micrologiciels, les logiciels et les données d'utilisateur. Les renseignements précis comprennent les micrologiciels de démarrage pour certains types de machines. La mise en œuvre automatique des contrôles dans les systèmes organisationnels comprend l'annulation des changements apportés, l'arrêt du système ou le déclenchement d'une alerte de vérification dès qu'un changement non autorisé s'effectue dans un fichier de sécurité essentiel.

SI-07(06) — Protection cryptographique (---)

Énoncés :

Mettre en œuvre des mécanismes de chiffrement pour détecter les modifications non autorisées apportées aux logiciels, aux micrologiciels et à l'information.

Responsable : Aucun

Discussion :

Les mécanismes cryptographiques utilisés pour protéger l'intégrité comprennent les signatures numériques, le calcul et l'application d'un hachage signé faisant appel à la cryptographie asymétrique, la protection de la confidentialité de la clé utilisée pour produire le hachage, et l'utilisation de la clé publique pour vérifier l'information de hachage. Les organisations qui ont recours à des mécanismes de chiffrement devraient également considérer des solutions de gestion de clés cryptographiques.

SI-07(07) — Intégration de la détection et de l'intervention (---)

Énoncés :

Intégrer la détection des changements non autorisés apportés à la capacité d'intervention en cas d'incident de l'organisation : [Affectation : changements de sécurité apportés au système définis par l'organisation].

Responsable : Aucun

Discussion :

Intégrer la détection et l'intervention aide à s'assurer que les événements sont suivis, surveillés, corrigés et conservés à des fins historiques. Il est important de conserver des documents historiques pour être en mesure de reconnaître et de discerner les actions adverses pendant une longue période et pour de possibles actions en justice. Les changements qui influent sur la sécurité comprennent les changements non autorisés apportés aux paramètres de configuration ou l'élévation non autorisée des privilèges sur le système.

SI-07(08) — Vérification des capacités en cas d'événements importants (---)

Énoncés :

Après avoir détecté une possible atteinte à l'intégrité, fournir les capacités nécessaires pour vérifier l'événement et mettre en œuvre les mesures suivantes : [Sélection (un choix ou plus) : générer un enregistrement de vérification; alerter les utilisatrices et utilisateurs actuels; alerter {Affectation : personnel ou rôles définis par l'organisation}; {Affectation : autres mesures définies par l'organisation}].

Responsable : Aucun

Discussion :

L'organisation sélectionne des mesures d'intervention du type de logiciel, du logiciel en particulier ou de l'information qui sont possiblement touchés par une atteinte à l'intégrité.

SI-07(09) — Vérification du processus de démarrage (---)

Énoncés :

Vérifier l'intégrité du processus de démarrage des composants de systèmes suivants : [Affectation : composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Il est essentiel d'assurer l'intégrité des processus de démarrage pour veiller à ce que les composants de systèmes soient sécurisés dès leur mise en marche. Les mécanismes de vérification de l'intégrité offrent un niveau d'assurance que seul du code sûr est exécuté pendant les processus de démarrage.

SI-07(10) — Protection des micrologiciels de démarrage (---)

Énoncés :

Mettre en œuvre les mécanismes suivants pour protéger l'intégrité du micrologiciel de démarrage dans [Affectation : composants de systèmes désignés par l'organisation] : [Affectation : mécanismes définis par l'organisation].

Responsable : Aucun

Discussion :

Des modifications non autorisées apportées aux micrologiciels de démarrage peuvent être un signe précurseur d'une attaque ciblée sophistiquée. Ces types d'attaques ciblées peuvent donner lieu à un déni de service permanent ou à la présence persistante d'un programme malveillant. Ces situations peuvent survenir si le micrologiciel est corrompu ou si le programme malveillant est intégré dans le micrologiciel. Les composants de systèmes peuvent protéger l'intégrité des micrologiciels de démarrage dans les systèmes organisationnels en vérifiant l'intégrité de l'authenticité de toutes les mises à jour des micrologiciels de démarrage avant d'appliquer les changements au moment du démarrage des systèmes et en empêchant les processus non autorisés de modifier les micrologiciels de démarrage.

SI-07(11) — Environnements clos aux privilèges restreints (---)

Énoncés :

Annulé : Transféré sous le contrôle CM-07(06).

Responsable : Aucun

SI-07(12) — Vérification de l’intégrité (---)

Énoncés :

Exiger que l’intégrité des logiciels suivants soit vérifiée avant exécution : [Affectation : logiciels désignés par l’organisation].

Responsable : Aucun

Discussion :

L’organisation vérifie l’intégrité des logiciels avant leur exécution afin de réduire les risques d’exécuter du code ou des programmes malveillants qui contiennent des erreurs découlant de modifications non autorisées. Les organisations considèrent la source du logiciel pour s’assurer que ce dernier et ses mises à jour proviennent de sources et/ou de sites autorisés et pour confirmer le caractère pratique des approches adoptées en ce qui a trait à la vérification de l’intégrité des logiciels, notamment la disponibilité de sommes de contrôle fiables de la part des développeuses, des développeurs et des fournisseurs de logiciels.

SI-07(13) — Exécution de code dans des environnements protégés (---)

Énoncés :

Annulé : Transféré sous le contrôle CM-07(07).

Responsable : Aucun

SI-07(14) — Code binaire ou exécutable sur machine (---)

Énoncés :

Annulé : Transféré sous le contrôle CM-07(08).

Responsable : Aucun

SI-07(15) — Authentification du code (---)

Énoncés :

Mettre en œuvre des mécanismes cryptographiques pour authentifier les composants logiciels ou micrologiciels suivants avant leur installation : [Affectation : composants logiciels ou micrologiciels désignés par l'organisation].

Responsable : Aucun

Discussion :

Par authentification cryptographique on entend la vérification des composants de logiciels ou de micrologiciels signés numériquement avec des certificats reconnus et approuvés par l'organisation. La signature du code est une méthode efficace de protection contre le code malveillant. Les organisations qui ont recours à des mécanismes de chiffrement devraient également considérer des solutions de gestion de clés cryptographiques.

SI-07(16) — Limite temporelle sur l'exécution des processus sans supervision (---)

Énoncés :

Faire en sorte que les processus ne puissent pas s'exécuter sans supervision pour plus de [Affectation : période définie par l'organisation].

Responsable : Aucun

Discussion :

L'imposition d'une limite temporelle sur l'exécution des processus sans supervision devrait s'appliquer aux processus pour lesquels le délai normal d'exécution peut être déterminé et aux situations où ces délais d'exécution sont dépassés au sein de l'organisation. La supervision peut être effectuée à l'aide des horloges des systèmes d'exploitation, d'interventions automatisées ou dans le cadre de la surveillance et des interventions manuelles en cas d'anomalies du processus du système.

SI-07(17) — Autoprotection des applications d'exécution (---)

Énoncés :

Mettre en œuvre [Affectation : contrôles définis par l'organisation] pour assurer l'autoprotection des applications d'exécution.

Responsable : Aucun

Discussion :

L'autoprotection des applications d'exécution fait appel à l'instrumentation du moteur d'exécution pour détecter et bloquer l'exploitation des vulnérabilités logicielles en tirant avantage de l'information tirée du logiciel en cours d'exécution. La prévention de l'exploitation du moteur d'exécution diffère des mesures de protection traditionnelles basées sur le périmètre dans la mesure où les mécanismes de protection et les pare-feu ne peuvent détecter et bloquer les attaques qu'au moyen de l'information réseau, sans connaître le contexte. La technologie d'autoprotection des applications d'exécution peut faire en sorte que les logiciels soient moins susceptibles aux attaques en surveillant ses intrants et en bloquant ceux qui pourraient donner lieu à des attaques. Elle peut également aider à protéger l'environnement d'exécution contre les changements indésirables et le trafiquage. Lorsqu'une menace est détectée, la technologie d'autoprotection des applications d'exécution peut prévenir l'exploitation et prendre d'autres mesures (par exemple, envoyer un message d'avertissement à l'utilisatrice ou utilisateur, mettre fin à la session de l'utilisatrice ou utilisateur, arrêter l'application ou envoyer une alerte au personnel de l'organisation). Les technologies d'autoprotection des applications d'exécution peuvent être déployées en mode surveillance ou en mode protection.

SI-08 — Protection contre les pourriels (---)

Énoncés :

a. Utiliser des mécanismes de protection contre les pourriels aux points d'entrée et de sortie du système pour détecter les messages non sollicités et intervenir, le cas échéant
b. Mettre à jour les mécanismes de protection contre les pourriels dès la diffusion de nouvelles versions, conformément à la stratégie et aux procédures de gestion des configurations de l'organisation

Responsable : Aucun

Discussion :

Les points d'entrée et de sortie du système comprennent les pare-feu, les serveurs d'accès à distance, les serveurs de courrier électronique, les serveurs Web, les serveurs mandataires, les stations de travail, les ordinateurs blocs-notes et les appareils mobiles. Les pourriels peuvent être transmis par différents moyens, y compris dans des courriels, dans les pièces jointes de courriels et par l'intermédiaire des accès Web. Les mécanismes de protection contre les pourriels comprennent les définitions de signature.

SI-08(01) — Gestion centrale (---)

Énoncés :

Annulé : Intégré au contrôle PL-09.

Responsable : Aucun

SI-08(02) — Mises à jour automatiques (---)

Énoncés :

Mettre à jour automatiquement les mécanismes de protection contre les pourriels [Affectation : fréquence définie par l'organisation].

Responsable : Aucun

Discussion :

Utiliser des mécanismes automatisés pour mettre à jour les mécanismes de protection contre les pourriels permet de s'assurer que les mises à jour sont effectuées sur une base régulière et de fournir le plus récent contenu et les plus récentes capacités de protection.

SI-08(03) — Capacité de perfectionnement continu (---)

Énoncés :

Mettre en œuvre des mécanismes de protection contre les pourriels avec une capacité d'apprentissage pour reconnaître le trafic de communications légitime plus efficacement.

Responsable : Aucun

Discussion :

Les mécanismes d'apprentissage comprennent les filtres bayésiens qui mettent à jour les paramètres des algorithmes de manière à séparer plus efficacement le trafic légitime et les pourriels en se basant sur les données saisies par les utilisatrices et utilisateurs.

SI-09 — Restrictions relatives à la saisie d'information (---)

Énoncés :

Annulé : Intégré aux contrôles AC-02, AC-03, AC-05 et AC-06.

Responsable : Aucun

SI-10 — Validation de la saisie d'information (---)

Énoncés :

Vérifier la validité des saisies d'information suivantes : [Affectation : saisies d'information dans le système définies par l'organisation].

Responsable : Aucun

Discussion :

Des règles de vérification de la validité de la syntaxe et des valeurs sémantiques des saisies du système – jeu de caractères, longueur, plage numérique, valeurs acceptables – sont mises en place pour s'assurer qu'elles respectent les définitions précisées en matière de format et de contenu. Par exemple, si l'organisation indique que seules les valeurs numériques entre 1 et 100 sont acceptées dans le champ d'une application donnée, les valeurs « 387 », « abc » ou « %K% » seront des saisies non valides qui seront refusées par le système. Les entrées valides varieront probablement d'un champ à l'autre dans l'application logicielle. Les applications suivent habituellement des protocoles bien définis qui utilisent des messages structurés (c'est-à-dire des commandes ou des requêtes) pour établir des communications entre les modules logiciels ou les composants de système. Les messages structurés peuvent contenir des données brutes ou non structurées parsemées de métadonnées ou d'information de contrôle. Si des applications logicielles utilisent des données saisies par un attaquant pour construire des messages structurés sans encoder de tels messages de manière adéquate, l'attaquant peut alors insérer des commandes malveillantes ou des caractères spéciaux qui pourraient faire en sorte que les données soient interprétées comme de l'information de contrôle ou des métadonnées. Par conséquent, le module ou le composant qui reçoit les saisies corrompues effectuera des opérations erronées ou interprétera les données incorrectement. Les saisies transmises aux interpréteurs sont filtrées au préalable pour empêcher que leur contenu soit interprété accidentellement comme des commandes. La validation des saisies permet de s'assurer que les saisies sont exactes et correctes et de prévenir des attaques, comme les scripts intersites et toute une gamme d'attaques par injection.

SI-10(01) — Fonction de correction manuelle (---)

Énoncés :

a. Fournir une fonction de correction manuelle pour la validation de la saisie de l'information suivante : [Affectation : saisies définies par l'organisation dans le contrôle de base (SI-10)]
b. Restreindre l'utilisation de la fonction de correction manuelle à [Affectation : personnes autorisées désignées par l'organisation]
c. Vérifier l'utilisation de la fonction de correction manuelle

Responsable : Aucun

Discussion :

Dans certaines situations, comme lors d'événements relevant de plans d'urgence, une fonction de correction manuelle pourrait être nécessaire à la validation en entrée. Les fonctions de correction manuelle ne sont utilisées que dans des cas restreints et pour les types de saisies définis par l'organisation.

SI-10(02) — Examen et résolution des erreurs (---)

Énoncés :

Examiner et résoudre les erreurs de validation en entrée dans les [Affectation : délais définis par l'organisation].

Responsable : Aucun

Discussion :

La résolution des erreurs de validation de saisies comprend la correction des causes d'erreurs systémiques et la répétition des transactions une fois la saisie corrigée. Les erreurs de validation en entrée sont celles liées aux saisies d'information définies par l'organisation dans le contrôle de base (SI-10).

SI-10(03) — Comportements prévisibles (---)

Énoncés :

Vérifier que le système se comporte d'une manière prévisible et informée lorsque des saisies non valides sont reçues.

Responsable : Aucun

Discussion :

Une vulnérabilité que l'on retrouve souvent dans les systèmes des organisations est le comportement imprévisible des systèmes lorsque des saisies non valides sont reçues. S'assurer que la prévisibilité du système permet de garantir que le système se comporte comme prévu lorsque des saisies non valides sont reçues en précisant les interventions que le système doit mettre en œuvre, ce qui facilite la transition du système vers un état connu sans incidences négatives ou imprévues. Les saisies non valides sont celles liées aux saisies d'information définies par l'organisation dans le contrôle de base (SI-10).

SI-10(04) — Chronométrage des interactions (---)

Énoncés :

Tenir compte du chronométrage des interactions entre les composants de systèmes lorsque vient le temps de déterminer les interventions appropriées à mettre en œuvre advenant des saisies non valides.

Responsable : Aucun

Discussion :

Le chronométrage des interfaces prend toute son importance lors des interventions requises quand des saisies non valides sont reçues dans les interfaces de protocole et quand un protocole doit mesurer l'incidence de l'intervention sur les autres protocoles de la pile de protocoles. Par exemple, les protocoles réseau sans fil de la norme 802.11 n'interagissent pas très bien avec les protocoles de contrôle de transmission (TCP) lorsque des paquets sont supprimés (ce qui pourrait être causé par l'entrée d'un paquet non valide). Les protocoles TCP laissent présumer que les pertes de paquets sont dues à la congestion, tandis que les paquets perdus sur les liens 802.11 le sont habituellement en raison de collisions ou de bruit sur le lien. Si le protocole TCP intervient pour une congestion, il effectue précisément la mauvaise intervention pour régler un événement de collision. Les adversaires peuvent être en mesure d'utiliser des comportements de protocoles apparemment acceptables de concert pour obtenir des résultats négatifs grâce à la construction de saisies non valides. Les saisies non valides sont celles liées aux saisies d'information définies par l'organisation dans le contrôle de base (SI-10).

SI-10(05) — Restriction des saisies provenant de sources de confiance et de formats approuvés (---)

Énoncés :

Restreindre l'utilisation des saisies d'information à [Affectation : sources de confiance définies par l'organisation] et à [Affectation : formats définis par l'organisation].

Responsable : Aucun

Discussion :

Restreindre l'utilisation des saisies aux sources de confiance et aux formats approuvés permet d'appliquer le concept des logiciels autorisés aux saisies d'information. Préciser les sources de confiance pour la saisie d'information et les formats acceptables de ces saisies réduit les risques d'activités malveillantes. Les saisies d'information sont celles définies par l'organisation dans le contrôle de base (SI-10).

SI-10(06) — Prévention de l’injection (---)

Énoncés :

Prévenir les injections de données non fiables.

Responsable : Aucun

Discussion :

Il est possible de prévenir les injections de données non fiables en ayant recours à une interface paramétrable ou à l’échappement des données de sortie (codage de sortie). Les interfaces paramétrables séparent les données du code de manière à ce que les injections de données malveillantes ou inattendues ne puissent pas changer la sémantique des commandes envoyées. L’échappement des données de sortie utilise des caractères précis pour indiquer à l’analyseur de l’interpréteur si les données sont fiables ou non. La prévention des injections de données non fiables vise les saisies d’information définies par l’organisation dans le contrôle de base (SI-10).

SI-11 — Traitement des erreurs (---)

Énoncés :

a. Générer des messages d'erreur qui fournissent l'information nécessaire à l'application de mesures correctives sans toutefois révéler des données qui pourraient être exploitées
b. Révéler les messages d'erreur seulement à [Affectation : personnel ou rôles définis par l'organisation]

Responsable : Aucun

Discussion :

L'organisation élabore la structure et le contenu des messages d'erreur. La mesure dans laquelle les systèmes peuvent gérer les conditions d'erreur repose sur la stratégie et les exigences de l'organisation. L'information exploitable comprend les détails relatifs aux traces de pile et à la mise en œuvre, les tentatives infructueuses de connexion où le mot de passe est saisi dans le champ du nom d'utilisateur par erreur, les renseignements liés à la mission et aux activités que l'on peut déduire de l'information consignée (ou qui s'y trouvent explicitement), ainsi que les renseignements personnels comme les numéros de compte, les numéros d'assurance sociale ou les numéros de carte de crédit. Les messages d'erreur peuvent servir de voie clandestine pour la transmission d'informations.

SI-12 — Gestion et conservation de l'information (---)

Énoncés :

Gérer et conserver l'information au sein du système et les sorties d'information du système conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes, aux lignes directrices et aux exigences opérationnelles applicables.

Responsable : Aucun

Discussion :

Les exigences en matière de gestion et de conservation de l'information s'appliquent à l'ensemble du cycle de vie de l'information et, dans certains cas, vont au-delà du retrait de l'élimination du système. L'information à conserver peut également comprendre des stratégies, des procédures, des plans, des rapports, des sorties de données découlant de la mise en œuvre de contrôles et d'autres types d'information administrative. Si les organisations ont un bureau de gestion de la documentation, il convient d'inclure le personnel de la gestion de la documentation dans ce processus. Les enregistrements produits à partir des sorties des contrôles mis en œuvre susceptibles d'être sujets à la gestion et à la conservation comprennent, sans s'y limiter : tous les contrôles XX-01, AC-06(09), AT-04, AU-12, CA-02, CA-03, CA-05, CA-06, CA-07, CA-08, CA-09, CM-02, CM-03, CM-04, CM-06, CM-08, CM-09, CM-12, CM-13, CP-02, IR-06, IR-08, MA-02, MA-04, PE-02, PE-08, PE-16, PE-17, PL-02, PL-04, PL-07, PL-08, PM-05, PM-08, PM-09, PM-18, PM-21, PM-27, PM-28, PM-30, PM-31, PS-02, PS-06, PS-07, PT-02, PT-03, PT-07, RA-02, RA-03, RA-05, RA-08, SA-04, SA-05, SA-08, SA-10, SI-04, SR-02, SR-04 et SR-08.

SI-12(01) — Limitation des éléments liés aux renseignements personnels (---)

Énoncés :

Limiter le traitement des renseignements personnels dans le cycle de vie de l'information aux éléments de renseignements personnels suivants : [Affectation : éléments des renseignements personnels définis par l'organisation].

Responsable : Aucun

Discussion :

Limiter la conservation des renseignements personnels tout au long du cycle de vie de l'information lorsque cette information n'est pas nécessaire à des fins opérationnelles aide à réduire le niveau de risque d'atteinte à la vie privée engendré par un système. Le cycle de vie de l'information comprend la création, la collecte, l'utilisation, le traitement, le stockage, la tenue à jour, la diffusion, la divulgation et l'élimination de l'information. Les évaluations des risques, de même que les lois, la réglementation et les politiques applicables, peuvent fournir des données utiles pour déterminer les éléments des renseignements personnels susceptibles de poser un risque.

SI-12(02) — Réduction des renseignements personnels utilisés aux fins de tests, de formation et de recherche (---)

Énoncés :

Utiliser les techniques suivantes pour limiter l'utilisation de renseignements personnels aux fins de recherche, de test ou de formation : [Affectation : techniques définies par l'organisation].

Responsable : Aucun

Discussion :

Les organisations peuvent minimiser le risque qui pèse sur la vie privée des individus en faisant appel à des techniques comme la dépersonnalisation ou les données synthétiques. Limiter l'utilisation des renseignements personnels tout au long du cycle de vie de l'information lorsque cette information n'est pas nécessaire aux fins de recherche, de test ou de formation aide à réduire le niveau de risque d'atteinte à la vie privée engendré par un système. Les évaluations des risques, de même que les lois, la réglementation et les politiques applicables, peuvent fournir des données utiles pour déterminer les techniques à utiliser et quand les utiliser.

SI-12(03) — Élimination de l'information (---)

Énoncés :

Utiliser les techniques suivantes pour éliminer, détruire ou supprimer l'information à la fin de la période de conservation : [Affectation : techniques définies par l'organisation].

Responsable : Aucun

Discussion :

Les organisations peuvent minimiser les risques liés à la sécurité et à la protection de la vie privée en éliminant l'information qui n'est plus nécessaire. L'élimination ou la destruction de l'information s'applique aux enregistrements originaux, ainsi qu'aux copies et aux archives, y compris les journaux système, qui peuvent contenir des renseignements personnels.

SI-13 — Prévention des pannes prévisibles (---)

Énoncés :

a. Déterminer la durée moyenne de fonctionnement avant défaillance (MTTF pour Mean Time to Failure) des composants de systèmes suivants dans des environnements d'exploitation donnés : [Affectation : composants de systèmes désignés par l'organisation]
b. Fournir des composants de système de remplacement et un mécanisme d'échange des rôles actifs et passifs des composants conformément aux critères suivants : [Affectation : critères de remplacement de la MTTF définis par l'organisation]

Responsable : Aucun

Discussion :

Bien que la MTTF soit essentiellement un problème de fiabilité, la prévention des pannes prévisibles vise à atténuer les défaillances potentielles des composants de systèmes qui fournissent des capacités de sécurité. Les taux de défaillance sont propres aux installations et ne tiennent pas compte des moyennes définies par l'industrie. L'organisation définit les critères de substitution des composants de systèmes en se basant sur la MTTF et en considérant les dommages que causerait une éventuelle défaillance des composants. Le transfert des responsabilités entre les composants actifs et passifs ne compromet en rien la sûreté, l'état de préparation opérationnelle ou les capacités de sécurité. La préservation des variables d'état des systèmes est également essentielle pour assurer le bon déroulement du processus de transfert. Le composant passif est accessible en permanence, sauf pendant une procédure de reprise après défaillance ou pour des motifs de maintenance.

SI-13(01) — Transfert des responsabilités d'un composant (---)

Énoncés :

Mettre les composants de systèmes hors service en transférant ses responsabilités à un composant de remplacement à l'intérieur de [Affectation : fraction ou pourcentage définis par l'organisation] de la durée moyenne de fonctionnement avant défaillance.

Responsable : Aucun

Discussion :

Il est important de transférer les responsabilités d'un composant de système principal à un autre composant de remplacement avant la défaillance du composant principal pour réduire le risque de dégradation ou de détérioration des fonctions liées à la mission ou aux activités de l'organisation. Procéder à de tels transferts selon un pourcentage de la MTTF permet aux organisations de faire preuve de proactivité en fonction de leur tolérance au risque. Cela dit, le remplacement prématuré des composants de systèmes peut donner lieu à de plus grands coûts d'exploitation des systèmes.

SI-13(02) — Limite temporelle sur l'exécution des processus sans supervision (---)

Énoncés :

Annulé : Intégré au contrôle SI-07(16).

Responsable : Aucun

SI-13(03) — Transfert manuel entre les composants (---)

Énoncés :

Procéder manuellement aux transferts entre les composants de systèmes actifs et passifs lorsque l'utilisation d'un composant actif atteint [Affectation : pourcentage défini par l'organisation] de la MTTF.

Responsable : Aucun

Discussion :

Par exemple, si la MTTF d'un composant de système est de 100 jours et que le pourcentage de la MTTF qui a été défini par l'organisation est de 90 %, le transfert manuel se sera effectué après 90 jours.

SI-13(04) — Installation des composants passifs et notification (---)

Énoncés :

Lors de la détection d'une défaillance d'un composant de système :
a. s'assurer que les composants passifs sont bien installés de manière transparente dans les [Affectation : délais définis par l'organisation]
b. [Sélection (un choix ou plus) : activer {Affectation : alarme définie par l'organisation}; mettre automatiquement le système hors tension; {Affectation : action définie par l'organisation}]

Responsable : Aucun

Discussion :

Le transfert automatique ou manuel de composants du mode passif au mode actif peut survenir lorsque la défaillance d'un composant est détectée.

SI-13(05) — Capacité de basculement (---)

Énoncés :

Fournir [Affectation : capacité de basculement définie par l'organisation] en [Sélection (un choix) : temps réel; temps quasi réel].

Responsable : Aucun

Discussion :

Par basculement, on entend le passage automatique à un système de remplacement lors de la défaillance du système principal. La capacité de basculement comprend la mise en miroir des opérations du système dans un site de traitement auxiliaire ou la mise en miroir périodique des données à intervalles réguliers durant une période définie par la durée de reprise de l'organisation.

SI-14 — Non-persistance (---)

Énoncés :

Mettre en œuvre des [Affectation : composants du système et services désignés par l'organisation] non persistants initialisés dans un état connu et interrompus [Sélection (un choix ou plus) : à la fin de la période d'utilisation; périodiquement {Affectation : fréquence déterminée par l'organisation}].

Responsable : Aucun

Discussion :

La mise en œuvre de composants et de services non persistants atténue les risques liés aux menaces persistantes avancées (MPA) en réduisant considérablement la capacité de ciblage des adversaires (par exemple, les créneaux et la surface d'attaque) qui préparent et lancent des attaques. En appliquant le concept de non-persistance à des composants sélectionnés du système, l'organisation dispose de ressources informatiques fiables dont l'état est connu, et ce, pendant une période précise qui ne laisse pas le temps aux adversaires d'exploiter les vulnérabilités de ses systèmes ou de ses environnements d'exploitation. Puisque les MPA sont des menaces sophistiquées de pointe en ce qui a trait à leurs capacités, à leurs intentions et à l'établissement de cibles, les organisations présument qu'à long terme, certaines attaques seront fructueuses. Les composants et services non persistants du système sont activés au besoin à l'aide d'informations protégées et sont interrompus périodiquement ou à la fin de la session. La non-persistance accroît la somme de travail des adversaires qui tentent de compromettre ou de pénétrer les systèmes organisationnels. Des composants non persistants du système peuvent être mis en œuvre en restaurant des composants de systèmes, en effectuant un redéploiement périodique de l'image ou en utilisant différentes techniques courantes de virtualisation. Les services non persistants peuvent être mis en œuvre au moyen de techniques de virtualisation en tant que machines virtuelles ou comme nouvelles instances de processus dans des machines physiques (persistantes et non persistantes). L'avantage des restaurations périodiques des composantes de systèmes et des services est qu'elles n'exigent pas que les organisations déterminent d'abord si les composants ou les services ont été compromis (ce qui peut parfois être difficile à déterminer). Les composants et services sont changés à une fréquence suffisante pour prévenir le déploiement d'attaques tout en maintenant la stabilité du système. La restauration de composants et services essentiels peut être effectuée périodiquement afin d'empêcher les adversaires d'exploiter les vulnérabilités optimales du système.

SI-14(01) — Restauration à partir de sources de confiance (---)

Énoncés :

Obtenir les données et les logiciels utilisés au cours de la restauration des composants de systèmes et des services à partir des sources de confiance suivantes : [Affectation : sources de confiance définies par l'organisation].

Responsable : Aucun

Discussion :

Les sources de confiance comprennent les supports non réinscriptibles provenant d'installations sélectionnées de stockage hors ligne.

SI-14(02) — Information non persistante (---)

Énoncés :

a. [Sélection (un choix) : Restaurer {Affectation : information définie par l'organisation} {Affectation : fréquence définie par l'organisation}; Générer {Affectation : information définie par l'organisation} sur demande]
b. Supprimer l'information qui n'est plus nécessaire

Responsable : Aucun

Discussion :

Conserver l'information plus longtemps que nécessaire en fait une cible potentielle pour les adversaires dotés de moyens sophistiqués qui cherchent à cibler les biens de grande importance afin de compromettre les systèmes en exfiltrant l'information ou en procédant à des divulgations ou à des modifications non autorisées. Pour l'information relative au système, une conservation de documents inutile fournit aux adversaires dotés de moyens sophistiqués l'information dont ils ont besoin pour faciliter la reconnaissance et se déplacer latéralement dans le système.

SI-14(03) — Connectivité non persistante (---)

Énoncés :

Établir des connexions au système sur demande et mettre fin aux connexions [Sélection (un choix) : une fois la demande terminée; après une période de non-utilisation].

Responsable : Aucun

Discussion :

Les connexions persistantes aux systèmes peuvent fournir aux adversaires dotés de moyens sophistiqués les chemins d'accès qui leur permettront de se déplacer latéralement dans les systèmes et, possiblement, se rapprocher des biens de grande importance. Limiter l'accessibilité à de telles connexions freine la capacité des adversaires à se déplacer librement entre les systèmes de l'organisation.

SI-15 — Filtrage des sorties d'information (---)

Énoncés :

Valider les sorties d'information des applications et/ou des programmes informatiques suivants pour s'assurer que l'information est conforme au contenu auquel l'on s'attend : [Affectation : applications et/ou programmes informatiques désignés par l'organisation].

Responsable : Aucun

Discussion :

Certains types d'attaques, comme les injections SQL (Structured Query Language) produisent des sorties d'information inattendues ou en contradiction avec les résultats auxquels l'on s'attend en temps normal de la part des applications ou des programmes informatiques. Le filtrage des sorties d'information met l'accent sur la détection de contenu étranger ou superflu pour l'empêcher de s'afficher, puis alerte les outils de surveillance que des comportements anormaux ont été découverts.

SI-16 — Protection de la mémoire (---)

Énoncés :

Mettre en place les contrôles suivants pour protéger la mémoire du système contre l'exécution de code non autorisé : [Affectation : contrôles définis par l'organisation].

Responsable : Aucun

Discussion :

Certains adversaires lancent des attaques dans l'intention d'exécuter du code dans des régions de mémoire non exécutables ou dans des régions de mémoire interdites. Les contrôles employés pour protéger la mémoire comprennent la prévention de l'exécution de données et le mécanisme de distribution aléatoire de l'espace d'adressage (ASLR pour Address Space Layout Randomization). Les contrôles de sécurité contre l'exécution de données peuvent être renforcés par du matériel ou des logiciels auxquels sont ajoutés des éléments matériels qui renforcent le mécanisme.

SI-17 — Procédures de sécurité intégrée (---)

Énoncés :

Mettre en place les procédures de sécurité intégrée indiquées lorsque les défaillances suivantes se produisent : [Affectation : liste des conditions de défaillance et des procédures de sécurité intégrée connexes établie par l'organisation].

Responsable : Aucun

Discussion :

Les conditions de défaillance comprennent la perte de communication entre des composants essentiels de systèmes ou entre des composants de systèmes et les installations opérationnelles. Les procédures de sécurité intégrée comprennent les alertes à l'intention du personnel et la diffusion de consignes claires sur les prochaines étapes à suivre. Les prochaines étapes pourraient consister à ne rien faire, à rétablir les paramètres de système, à arrêter les processus, à redémarrer le système ou à communiquer avec le personnel désigné de l'organisation.

SI-18 — Opérations liées à la qualité des renseignements personnels (---)

Énoncés :

a. Assurer l'exactitude, la pertinence, la rapidité et l'exhaustivité des renseignements personnels utilisés à des fins administratives tout au long du cycle de vie de l'information [Affectation : fréquence définie par l'organisation]
b. Corriger ou supprimer les renseignements personnels inexacts ou obsolètes

Responsable : Aucun

Discussion :

Les opérations liées à la qualité des renseignements personnels comprennent les étapes prises par l'organisation pour confirmer l'exactitude et la pertinence des renseignements personnels tout au long du cycle de vie de l'information. Le cycle de vie de l'information comprend la création, la collecte, l'utilisation, le traitement, le stockage, la tenue à jour, la diffusion, la divulgation et l'élimination des renseignements personnels. Les opérations liées à la qualité des renseignements personnels comprennent la modification et la validation des adresses dans le cadre de leur collecte ou de leur saisie dans les systèmes au moyen d'API utilisées pour la vérification automatisée des adresses. Vérifier la qualité des renseignements personnels consiste à faire le suivi des mises à jour ou des changements apportés aux données au fil du temps dans le but de permettre à l'organisation de savoir quels renseignements personnels ont été modifiés et de quelle manière advenant le cas où des renseignements erronés seraient découverts. Les mesures prises pour protéger la qualité des renseignements personnels sont basées sur la nature et le contexte des renseignements personnels, la façon dont ils sont utilisés et obtenus, ainsi que le potentiel des méthodes de dépersonnalisation employées.

SI-18(01) — Soutien à l'automatisation (---)

Énoncés :

Corriger ou supprimer les renseignements personnels inexacts ou obsolètes, ceux dont l'incidence a été mal déterminée ou ceux qui ont été mal dépersonnalisés au moyen de [Affectation : mécanismes automatisés définis par l'organisation].

Responsable : Aucun

Discussion :

Le recours à des mécanismes automatisés pour améliorer la qualité des données peut créer des risques d'atteinte à la vie privée par inadvertance. Les outils automatisés peuvent se connecter à des systèmes externes ou indépendants et la mise en correspondance des enregistrements entre ces systèmes peut établir des recoupements et entraîner des conséquences imprévues. Les organisations évaluent et documentent ces risques dans leur EFVP et prennent des décisions conformément à leurs plans du programme de protection de la vie privée. Comme les données sont obtenues et utilisées tout au long du cycle de vie de l'information, il est important de confirmer l'exactitude et la pertinence des renseignements personnels. Les mécanismes automatisés peuvent renforcer les procédures et processus actuels en matière de qualité des données et permettre à une organisation de mieux relever et gérer les renseignements personnels dans des systèmes à grande échelle. Par exemple, des outils automatisés peuvent grandement faciliter les efforts déployés pour normaliser constamment les données ou relever les données malformées. Les outils automatisés peuvent également servir à améliorer la vérification des données et à détecter les erreurs susceptibles de modifier incorrectement les renseignements personnels ou d'associer par erreur ces renseignements personnels à la mauvaise personne. Les capacités automatisées renforcent les processus et les procédures à grande échelle et permettent d'assurer une détection ou une correction plus granulaires des erreurs liées à la qualité des données.

SI-18(02) — Étiquetage des données (---)

Énoncés :

Employer les étiquettes de données pour automatiser la correction ou la suppression des renseignements personnels tout au long du cycle de vie de l'information dans les systèmes organisationnels.

Responsable : Aucun

Discussion :

Les renseignements personnels faisant l'objet d'un étiquetage comprennent les étiquettes qui font mention des autorisations de traitement, l'autorité en matière de collecte, la dépersonnalisation, le niveau d'incidence, la phase du cycle de vie de l'information, ainsi que les dates de conservation ou de la dernière mise à jour. Employer des étiquettes de données pour les renseignements personnels peut soutenir l'utilisation des outils d'automatisation visant à corriger ou à supprimer les renseignements personnels.

SI-18(03) — Collecte (---)

Énoncés :

Collecter les renseignements personnels directement des individus, dans la mesure du possible.

Responsable : Aucun

Discussion :

Les individus ou leurs représentantes et représentants désignés peuvent être des sources de renseignements personnels erronés. Les organisations considèrent des facteurs contextuels qui peuvent faire en sorte que des individus fournissent des renseignements personnels erronés. Des étapes supplémentaires peuvent être nécessaires pour valider les renseignements personnels, selon la façon dont ils sont utilisés et comment ils ont été obtenus. Les mesures prises pour valider l'exactitude des renseignements utilisés pour prendre des décisions quant aux droits, aux avantages ou aux privilèges des personnes relevant de programmes fédéraux peuvent être plus exhaustives que celles employées pour valider les renseignements personnels utilisés à des fins moins sensibles.

SI-18(04) — Demandes individuelles (---)

Énoncés :

Corriger ou supprimer les renseignements personnels lorsque des individus ou leurs représentantes ou représentants en font la demande.

Responsable : Aucun

Discussion :

Les renseignements personnels exacts qui sont maintenus par les organisations peuvent causer des problèmes aux individus, particulièrement en ce qui a trait aux fonctions liées aux activités pour lesquelles des renseignements inexacts pourraient mener à la prise de décisions inappropriées ou à un refus d'avantages et de services pour les individus. Même si l'information est exacte, certaines circonstances peuvent faire en sorte que les renseignements erronés causent des problèmes pour les individus qui surpassent les avantages que l'organisation qui maintient l'information en question pourrait tirer. Les organisations exercent un pouvoir discrétionnaire au moment de déterminer s'il convient de corriger ou de supprimer l'information personnelle selon l'ampleur des demandes, les changements à apporter, l'incidence des changements, ainsi que les lois, la réglementation et les politiques. Le personnel de l'organisation consulte la ou le haut fonctionnaire ou cadre supérieur et la conseillère ou le conseiller juridique en matière de protection de la vie privée concernant les instances appropriées de correction ou de suppression.

SI-18(05) — Avis de correction ou de suppression (---)

Énoncés :

Notifier [Affectation : destinataires des renseignements personnels désignés par l'organisation] et les individus que les renseignements personnels ont été corrigés ou supprimés.

Responsable : Aucun

Discussion :

Une fois que les renseignements personnels sont corrigés ou supprimés, les organisations prennent les mesures nécessaires pour veiller à ce que les destinataires de ces renseignements, ainsi que les individus avec qui les renseignements sont associés ou leurs représentantes et représentants désignés, soient mis au courant de la correction ou de la suppression des renseignements.

SI-19 — Dépersonnalisation (---)

Énoncés :

a. Supprimer les éléments de renseignements personnels suivants des jeux de données : [Affectation : éléments de renseignements personnels définis par l'organisation]
b. Évaluer l'efficacité de la dépersonnalisation [Affectation : fréquence définie par l'organisation] a
a. Tenir compte des préjudices découlant de l'atteinte à la vie privée si les renseignements pouvant être accessibles au public permettent de réidentifier les individus

Responsable : Aucun

Discussion :

À l'occasion, des programmes peuvent utiliser des renseignements personnels, alors qu'ils sont en mesure d'atteindre leur objectif sans recourir aux identificateurs personnels. S'il est possible d'atteindre l'objectif sans identificateurs directs, l'information devrait être dépersonnalisée. Par dépersonnalisation, on entend le processus visant à supprimer l'association entre un jeu de données d'identification et le sujet des données. Ce processus a pour objectif d'éviter que les renseignements personnels d'un individu soient apparents lors d'une utilisation ou d'une divulgation. Plusieurs jeux de données contiennent des renseignements personnels qui peuvent être utilisés pour reconnaître ou trouver l'identité d'un individu, comme son nom, son numéro d'assurance sociale, sa date et son lieu de naissance, le nom de jeune fille de sa mère ou ses données biométriques. Les jeux de données peuvent également contenir de l'information qui est liée ou qui peut être liée à un individu, comme les renseignements médicaux ou financiers et l'information sur les études ou l'emploi. L'élimination (la suppression) des renseignements personnels est une méthode de dépersonnalisation qu'il convient d'envisager lorsqu'une telle information n'est pas (ou plus) nécessaire pour répondre aux exigences prévues pour les données ou devrait être supprimée des jeux de données par des personnes formées pour accomplir une telle tâche. Par exemple, si le jeu de données n'est utilisé que pour générer des statistiques agrégées, les identificateurs qui ne sont pas nécessaires à la production de ces statistiques sont supprimés. Supprimer les identificateurs renforce la protection de la vie privée, puisque l'information supprimée ne peut pas être divulguée par inadvertance ou utilisée de façon inappropriée. Il convient de considérer les possibles préjudices découlant de l'atteinte à la vie privée si certains renseignements peuvent permettre de réidentifier l'individu, même sans identificateurs directs. Les organisations peuvent être sujettes à des définitions ou à des méthodes de dépersonnalisation particulières en vertu des lois, de la réglementation ou des politiques applicables. La réidentification est un risque résiduel des données dépersonnalisées. Les attaques par réidentification peuvent varier et comprendre la combinaison de nouveaux jeux de données ou d'autres améliorations apportées à l'analyse de données. Demeurer au courant des attaques potentielles et évaluer l'efficacité de la dépersonnalisation au fil du temps permet de soutenir la gestion de ce risque résiduel. Il est recommandé de planifier des évaluations régulières, continues et périodiques du risque de réidentification en passant en revue les stratégies de diffusion et en modifiant les termes des accords d'échange de renseignements, le cas échéant, à mesure que les circonstances changent.

SI-19(01) — Collecte (---)

Énoncés :

Dépersonnaliser les jeux de données au moment de la collecte en ne collectant pas les renseignements personnels.

Responsable : Aucun

Discussion :

Si un jeu de données provient d'un autre programme ou d'une autre entité, il est nécessaire de limiter l'information recherchée aux renseignements personnels seulement. Par exemple, si une organisation n'a pas l'intention d'utiliser le numéro d'assurance sociale d'une candidate ou d'un candidat, elle ne devrait pas collecter cette information. Les organisations devraient documenter la collecte, l'utilisation ou la divulgation des jeux de données dans une entente ou un accord sur l'échange d'information.

SI-19(02) — Archivage (---)

Énoncés :

Interdire l'archivage des éléments de renseignements personnels si ces éléments dans le jeu de données ne sont pas nécessaires une fois le jeu de données archivé.

Responsable : Aucun

Discussion :

Les jeux de données peuvent être archivés pour plusieurs raisons. À moins qu'une exigence fasse en sorte qu'il soit nécessaire de conserver les renseignements personnels, les jeux de données devraient être dépersonnalisés avant leur archivage. Si la suppression des renseignements personnels est envisagée, il convient de mettre en place une norme de disposition des documents et de s'assurer que la suppression des renseignements personnels respecte les normes de conservation de documents de l'organisation.

SI-19(03) — Diffusion (---)

Énoncés :

Supprimer les éléments de renseignements personnels d'un jeu de données avant sa diffusion si ces éléments n'ont pas à faire partie de la diffusion des données.

Responsable : Aucun

Discussion :

Avant de diffuser un jeu de données, une ou un responsable des données considère les usages prévus du jeu de données et détermine s'il est nécessaire de diffuser les renseignements personnels. Si les renseignements personnels ne sont pas nécessaires, ils peuvent être supprimés au moyen de techniques de dépersonnalisation.

SI-19(04) — Suppression, masquage, chiffrement, hachage ou remplacement des identificateurs directs (---)

Énoncés :

Supprimer, masquer, chiffrer, hacher ou remplacer les identificateurs directs dans un jeu de données.

Responsable : Aucun

Discussion :

Plusieurs processus peuvent être utilisés pour supprimer les identificateurs directs dans un jeu de données. Les colonnes du jeu de données qui contiennent un identificateur direct peuvent être supprimées. Lors du masquage, l'identificateur direct est transformé en caractère répétitif, comme XXXXXX ou
999999. Les identificateurs peuvent être chiffrés ou hachés de manière à ce que les enregistrements liés demeurent liés. Dans le cas du chiffrement ou du hachage, on emploie des algorithmes qui exigent l'utilisation d'une clé, notamment la norme de chiffrement avancée (AES pour Advanced Encryption Standard) ou un code d'authentification de message haché. Les mises en œuvre peuvent utiliser la même clé pour tous les identificateurs ou une clé différente pour chaque identificateur. L'utilisation d'une clé différente pour chaque identificateur offre un niveau plus élevé de sécurité et de protection de la vie privée. Les identificateurs peuvent également être remplacés par un mot clé, comme transformer « Jean Untel » en « PATIENT » ou le remplacer par une valeur de remplacement comme « Laura Secord ».

SI-19(05) — Contrôle de la divulgation de statistiques (---)

Énoncés :

Manipuler les données numériques, les tableaux croisés et les résultats statistiques de manière à ce qu'on ne puisse pas identifier un individu ou une organisation dans les résultats de l'analyse.

Responsable : Aucun

Discussion :

Plusieurs types d'analyses statistiques peuvent donner lieu à la divulgation de renseignements concernant des individus, même si seul un résumé est fourni. Par exemple, si un établissement d'enseignement qui publie un tableau mensuel avec le nombre d'étudiantes et étudiants inscrits appartenant à une minorité indique qu'il y avait 10 de ces étudiants sur 19 en janvier, puis 20 de ces étudiants sur 29 en mars, on pourra en déduire que l'étudiante ou étudiant qui s'est inscrit en février était issu d'une minorité. Il faut veiller à passer en revue toutes les données statistiques divulguées pour assurer la protection des renseignements personnels des individus.

SI-19(06) — Confidentialité différentielle (---)

Énoncés :

Prévenir la divulgation de renseignements personnels en ajoutant du bruit non déterministe aux résultats des opérations mathématiques avant de faire rapport des résultats.

Responsable : Aucun

Discussion :

La définition mathématique de la confidentialité différentielle indique que le résultat de l'analyse du jeu de données devrait être approximativement le même avant et après l'ajout ou la suppression d'un seul enregistrement de données (que l'on présume être les données d'un seul individu). Dans sa forme la plus fondamentale, la confidentialité différentielle s'applique uniquement aux systèmes d'interrogation en ligne. Elle peut toutefois être utilisée pour produire des classificateurs statistiques d'apprentissage automatique et des données synthétiques. La confidentialité différentielle est assurée au détriment de l'exactitude des résultats, forçant les organisations à quantifier le compromis entre la confidentialité et l'exactitude, la pertinence et l'utilité globales des jeux de données dépersonnalisés. Le bruit non déterministe peut comprendre l'ajout de petites valeurs randomisées aux résultats des opérations mathématiques dans l'analyse des jeux de données.

SI-19(07) — Algorithmes et logiciels validés (---)

Énoncés :

Procéder à la dépersonnalisation au moyen d'algorithmes validés et de logiciels homologués pour assurer la mise en œuvre des algorithmes.

Responsable : Aucun

Discussion :

Les algorithmes qui semblent supprimer les renseignements personnels dans un jeu de données peuvent en fait laisser de l'information permettant d'identifier un individu ou des données réidentifiables. Les logiciels qui prétendent mettre en œuvre un algorithme validé peuvent contenir des bogues ou déployer un algorithme différent. Les logiciels peuvent dépersonnaliser un type de données, comme les nombres entiers, mais ne pas dépersonnaliser d'autres types, comme les nombres à virgule flottante. Pour ces raisons, la dépersonnalisation est effectuée au moyen d'algorithmes et de logiciels ayant été validés.

SI-19(08) — Intrus motivé (---)

Énoncés :

Effectuer un test d'intrus motivé dans le jeu de données dépersonnalisé pour déterminer si ce dernier contient toujours des données identifiables ou si les données dépersonnalisées peuvent être réidentifiées.

Responsable : Aucun

Discussion :

Par test d'intrus motivé, on entend un test dans le cadre duquel une personne ou un groupe analyse une communication de données et des ressources particulières et tente de réidentifier un ou plusieurs individus dans le jeu de données dépersonnalisé. Ces tests permettent de révéler l'ampleur des connaissances internes, des ressources de calcul, des ressources financières et des compétences que les intrus doivent posséder pour réaliser les tests. Un test d'intrus motivé peut déterminer si la dépersonnalisation est insuffisante. Il peut également être un outil de diagnostic utile pour estimer si la dépersonnalisation est susceptible d'être suffisante. Par contre, le test ne peut en lui-même prouver que la dépersonnalisation est suffisante.

SI-20 — Contamination (---)

Énoncés :

Intégrer les données ou les capacités dans les systèmes ou les composants de systèmes suivants pour déterminer si les données organisationnelles ont été exfiltrées ou ont été supprimées de façon inappropriée de : [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

Plusieurs cyberattaques ciblent l'information organisationnelle ou l'information que l'organisation conserve au nom d'autres entités (par exemple, les renseignements personnels), puis exfiltrent ces données. Par ailleurs, des attaques internes et des procédures effectuées par erreur par les utilisatrices ou utilisateurs peuvent supprimer l'information sur le système, ce qui va à l'encontre des stratégies organisationnelles. Les approches en matière de contamination peuvent être passives ou actives. Une approche passive à la contamination peut consister à ajouter de faux noms de courriel et de fausses adresses dans une base de données interne. Si l'organisation reçoit un courriel à l'une des fausses adresses, elle sait que la base de données a été compromise. De plus, comme l'organisation sait que le courriel a été envoyé par une entité non autorisée, elle sait que tous les paquets de données compris dans le courriel contiennent probablement du code malveillant et que l'entité non autorisée peut possiblement avoir obtenu une copie de la base de données. Une autre approche à la contamination peut comprendre l'intégration de fausses données ou de données stéganographiques dans les fichiers pour permettre aux données d'être repérées dans le cadre d'analyses de source ouverte. Pour finir, une approche active à la contamination peut comprendre l'intégration d'un logiciel dans les données, qui est capable d'envoyer des signaux « à la maison » pour alerter l'organisation de sa « capture » (et possiblement son emplacement), et de fournir le chemin par lequel il a été exfiltré ou supprimé.

SI-21 — Actualisation de l'information (---)

Énoncés :

Actualiser [Affectation : information définie par l'organisation] [Affectation : fréquences définies par l'organisation] ou générer l'information sur demande et la supprimer lorsqu'elle n'est plus nécessaire.

Responsable : Aucun

Discussion :

Conserver l'information plus longtemps que nécessaire accroît la valeur de cette dernière et en fait une cible de choix pour les adversaires. Conserver l'information pour le délai minimal nécessaire pour soutenir les fonctions liées à la mission ou aux activités de l'organisation réduit la possibilité que des adversaires arrivent à compromettre, à capturer et à exfiltrer l'information.

SI-22 — Diversité de l'information (---)

Énoncés :

a. Relever les autres sources d'information pour [Affectation : fonctions et services essentiels définis par l'organisation] : [Affectation : autres sources d'information définies par l'organisation]
b. Utiliser une autre source d'information pour l'exécution des fonctions et des services essentiels sur [Affectation : systèmes ou composants de systèmes désignés par l'organisation] lorsque la source principale d'information est corrompue ou non disponible

Responsable : Aucun

Discussion :

Les mesures prises par un service ou une fonction d'un système découlent souvent de l'information reçue. La corruption, la fabrication, la modification ou la suppression de cette information pourrait avoir une incidence sur la capacité de la fonction du service à exécuter adéquatement les actions prévues. Le fait d'avoir plusieurs sources d'intrants fait en sorte que le service ou la fonction peut continuer de s'exécuter advenant la corruption ou l'indisponibilité d'une source. Il est possible que les autres sources d'information puissent être moins précises ou exactes que la source principale. Avoir des sources d'information non optimales peut tout de même fournir un niveau de qualité suffisant pour permettre à la fonction ou au service essentiel d'être exécuté, même en cas de dégradation ou de détérioration.

SI-23 — Fragmentation de l’information (---)

Énoncés :

Selon [Affectation : circonstances définies par l’organisation] :
a. fragmenter l’information suivante : [Affectation : information définie par l’organisation]
b. distribuer l’information fragmentée dans l’ensemble des systèmes ou des composants de systèmes suivants : [Affectation : systèmes ou composants de systèmes désignés par l’organisation]

Responsable : Aucun

Discussion :

Un objectif de la menace persistante avancée est d’exfiltrer l’information précieuse. Une fois exfiltrée, cette information ne peut généralement pas être récupérée par l’organisation. Par conséquent, cette dernière peut envisager de diviser l’information en des éléments disparates et de les distribuer dans plusieurs systèmes ou composants de systèmes et dans de nombreux emplacements. De telles mesures augmenteront les efforts que les adversaires devront déployer pour capturer et exfiltrer l’information voulue et permettront, ce faisant, d’accroître la probabilité de la détection. La fragmentation de l’information a une incidence sur la capacité de l’organisation à accéder à l’information de manière opportune. L’ampleur de la fragmentation est dictée par l’incidence ou le niveau de classification (et la valeur) de l’information, par le renseignement reçu au sujet des menaces et par le recours à la contamination des données (c’est-à-dire si l’information dérivée de la contamination des données concernant l’exfiltration de certaines données pourrait donner lieu à la fragmentation de l’information restante).

SI-400 — Station de travail administrative dédiée (---)

Énoncés :

Exiger que les opérations administratives ou de superutilisatrices ou superutilisateurs soient réalisées à partir d'une station de travail physique dédiée à ces tâches précises et isolée des autres fonctions et réseaux. La station ne devrait pas, entre autres, avoir accès à Internet.

Responsable : Aucun

Discussion :

Une station de travail administrative dédiée (STAD) est typiquement constituée d'un terminal d'utilisateur et d'une très petite sélection de logiciels conçus pour interfacer avec le système cible. Aux fins du présent contrôle, une station de travail est un système à partir duquel les tâches d'administration sont réalisées, par opposition au système cible. La STAD doit être renforcée pour le rôle afin de réduire la probabilité qu'un point d'extrémité de superutilisateur ou d'administrateur soit compromis par un auteur de menace (ce qui entraînerait logiquement la compromission du système cible). Les outils bureautiques typiques ne sont pas nécessaires sur la STAD. Toutes les applications et tous les services non essentiels doivent être supprimés. Les STAD n'ont pas de jonction de domaine, ne peuvent pas télécharger de correctifs à partir d'Internet et ne peuvent pas mettre à jour la documentation dans les applications en réseau. Les serveurs bastion ne sont pas une substitution à l'exigence imposant le recours à des STAD. Les connexions par l'entremise d'un serveur bastion doivent être effectuées à partir d'une STAD. Les serveurs bastions permettent de centraliser la journalisation des activités administratives, de simplifier l'isolation réseau des serveurs critiques et de fournir un point de transfert commun pour les administratrices et administrateurs avec séparation des tâches (par exemple, où les correctifs d'un logiciel sont préparés par une administratrice ou un administrateur afin d'être installés par une ou un autre). Si un RPV est utilisé pour fournir la connectivité réseau, celui-ci doit automatiquement exclure tous les autres accès réseau à l'exception du RPV. La STAD doit être en mesure d'accéder à d'autres réseaux que celui-ci qu'elle administre. L'interface de gestion du système cible doit se limiter à la gestion du réseau et ne pas être accessible aux réseaux plus vastes, comme les réseaux locaux des stations de travail de l'organisation ou Internet. Si plusieurs réseaux cibles sont administrés par la même STAD logique, tous les réseaux doivent avoir le même profil de sécurité (par exemple, une seule STAD ne peut pas administrer un réseau SECRET et un réseau PROTÉGÉ B). Les logiciels de terminaux virtuels qui émulent un terminal simple devraient également résider sur une STAD.

SI-400(01) — Station de travail administrative dédiée avec client léger (---)

Énoncés :

Mettre en œuvre une STAD virtualisée à l'intérieur d'une STAD client léger physique isolée du réseau.

Responsable : Aucun

Discussion :

Les administratives et administrateurs qui doivent gérer de nombreuses infrastructures peuvent choisir d'utiliser une STAD client léger physique qui peut exécuter plusieurs STAD virtualisées pour les différents réseaux. Le client léger peut être employé dans une infrastructure de postes de travail virtuels (VDI pour Virtual Desktop Infrastructure), où la STAD physique est l'hôte de l'hyperviseur d'une STAD virtuelle, ou dans un client léger à démarrage réseau où le système d'exploitation du client léger est chargé depuis le réseau à administrer. Le client léger physique ne doit pas disposer d'un accès indépendant au réseau.

SI-400(02) — RPV sur réseau privé d'opérateur (---)

Énoncés :

Connecter une STAD à un réseau cible au moyen d'un réseau privé d'opérateur (par exemple, un service LAN privé virtuel [VPLS pour Virtual Private LAN] ou une commutation multiprotocole par étiquette [MPLS pour Multiprotocol Label Switching]) avec chiffrement de RPV.

Responsable : Aucun

Discussion :

Lorsqu'un réseau est administré à partir d'un lieu distant, les passerelles RPV reliées à Internet et les points d'extrémités du RPV sont vulnérables aux attaques menées par des auteurs de menace ayant recours à un réseau public. Passer à un réseau privé d'opérateur éliminera les vulnérabilités liées à l'Internet public et permettra de réduire le nombre d'auteurs de menace compétents. Cela dit, le réseau peut tout de même être vulnérable aux attaques visant la confidentialité ou l'intégrité qui sont menées depuis l'intérieur du réseau de l'opérateur. Par conséquent, un RPV est toujours requis dans le réseau de l'opérateur.

SI-400(03) — Réseau local (---)

Énoncés :

Connecter une STAD à un réseau cible au moyen d'un réseau local seulement.

Responsable : Aucun

Discussion :

Pour réduire davantage la probabilité d'une attaque sur le réseau, une STAD doit être connectée au système cible au moyen d'un réseau local seulement. Le système cible peut alors refuser l'accès administratif sauf pour le segment local.

SI-400(04) — Accès par console seulement (---)

Énoncés :

Connecter une STAD au système cible par l'intermédiaire des ports de la console seulement.

Responsable : Aucun

Discussion :

Pour éliminer la probabilité d'une attaque visant le réseau, une STAD doit être connectée au système cible directement par l'intermédiaire des ports série locaux. Le système peut alors refuser l'accès administratif à tous les réseaux.

SI-400(05) — Station de travail physique dédiée (---)

Énoncés :

Utiliser une station de travail physique unique comme STAD.

Responsable : Aucun

Discussion :

Pour réduire la possibilité d'attaque avec déplacement latéral entre les réseaux administrés, il convient d'utiliser une station de travail physique pour chaque réseau cible et d'éviter tout partage des ressources de la STAD.

SI-400(06) — Accès administratif hétérogène (---)

Énoncés :

Utiliser un système d'exploitation différent pour la STAD et le système cible.

Responsable : Aucun

Discussion :

La STAD et le système cible peuvent être touchés par la même vulnérabilité, offrant du même coup un moyen d'attaque unique pour les deux. Si la STAD et les systèmes cibles exécutent des systèmes d'exploitation différents, il faudra déployer des efforts plus grands pour les compromettre tous les deux.

SR

Gestion des risques liés à la chaîne d'approvisionnement

Supply Chain Risk Management

SR-01 — Politique et procédures de gestion des risques liés à la chaîne d'approvisionnement (---)

Énoncés :

a. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation] :

1. une politique de gestion des risques liés à la chaîne d'approvisionnement (GRCA) [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui : (a) définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité (b) est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables

2. des procédures pour faciliter la mise en oeuvre de la politique de GRCA et des contrôles connexes

b. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à la GRCA

c. Passer en revue et mettre à jour, par rapport à la GRCA :

1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]

Responsable : Aucun

Discussion :

La politique et les procédures de GRCA portent sur les contrôles appartenant à la famille SR, ainsi que sur les contrôles liés à la chaîne d'approvisionnement des autres familles mises en oeuvre dans les systèmes et au sein des organisations. La politique de gestion des risques est un facteur important dans l'établissement de telles politiques et procédures. Les politiques et les procédures contribuent à l'assurance de la sécurité et de la protection de la vie privée. Par conséquent, il est important que les programmes de sécurité et de protection de la vie privée collaborent à l'élaboration de la politique et des procédures de GRCA. En règle générale, les politiques et les procédures liées au programme de sécurité et de protection de la vie privée au niveau organisationnel sont préférables et peuvent éliminer le besoin pour des politiques et des procédures propres à la mission ou au système. La politique peut être intégrée à la politique générale de sécurité et de protection de la vie privée ou, inversement, elle peut être représentée par de multiples politiques tenant compte de la nature complexe de certaines organisations. Les procédures peuvent être établies pour les programmes de sécurité et de protection de la vie privée, pour les processus liés à la mission ou aux activités, et pour les systèmes, le cas échéant. Les procédures décrivent comment les politiques ou les contrôles sont mis en oeuvre et peuvent s'appliquer aux personnes ou aux rôles qui font l'objet de la procédure. Les procédures peuvent être documentées dans les plans de sécurité et de protection de la vie privée du système ou dans un ou plusieurs documents distincts. Les événements qui peuvent précipiter une mise à jour de la politique et des procédures de GRCA comprennent les conclusions d'une évaluation ou d'une vérification, des incidents ou violations de sécurité, et des changements apportés aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables. Répéter les contrôles ne constitue pas une politique ou une procédure organisationnelle.

SR-02 — Plan de gestion des risques liés à la chaîne d'approvisionnement (---)

Énoncés :

a. Élaborer un plan pour gérer les risques liés à la chaîne d'approvisionnement associés à la recherche, au développement, à la conception, à la fabrication, à l'acquisition, à la livraison, à l'intégration, à l'exploitation, à la maintenance et à l'élimination des systèmes, des composants de systèmes ou des services qui s'y rapportent [Affectation : systèmes, composants de systèmes ou services désignés par l'organisation]
b. Passer en revue et mettre à jour le plan de GRCA [Affectation : fréquence définie par l'organisation] ou au besoin pour tenir compte des changements organisationnels, environnementaux ou en matière de menaces
c. Protéger le plan de GRCA contre les divulgations ou les modifications non autorisées

Responsable : Aucun

Discussion :

La dépendance aux produits, aux systèmes et aux services de fournisseurs externes, ainsi que la nature des relations avec ces fournisseurs, présente un niveau accru de risque pour une organisation. Les menaces pouvant augmenter les risques liés à la sécurité et à la protection de la vie privée incluent la production non autorisée, la falsification, le trafiquage, le vol, l'insertion de logiciel ou de matériel malveillant et les mauvaises pratiques de fabrication et de développement dans la chaîne d'approvisionnement. Les risques liés à la chaîne d'approvisionnement peuvent être endémiques ou systémiques d'un élément ou d'un composant, d'un système, d'une organisation, d'un secteur ou du gouvernement. La gestion des risques liés à la chaîne d'approvisionnement est une tâche complexe à plusieurs facettes nécessitant des efforts coordonnés au sein d'une organisation afin d'établir des relations de confiance et de communiquer avec les parties prenantes internes et externes. Les activités de GRCA comprennent l'identification et l'évaluation des risques, la détermination des mesures appropriées de réponse aux risques, l'élaboration de plans de GRCA visant à documenter les mesures de réponse et la surveillance du rendement par rapport aux plans. Le plan de GRCA (au niveau du système) vise une mise en œuvre en particulier et fournit la mise en œuvre, les exigences, les contraintes et les implications de la stratégie à ce sujet. Ce plan peut être indépendant ou intégré aux plans de sécurité et de protection de la vie privée du système. Les plans de GRCA portent sur la gestion, la mise en œuvre et la surveillance des contrôles de GRCA ainsi que le développement ou le maintien des systèmes pendant le cycle de développement des systèmes (CDS) à l'appui des fonctions liées à la mission et aux activités de l'organisation. Puisque les chaînes d'approvisionnement peuvent varier considérablement au sein d'une même organisation et d'une organisation à l'autre, les plans de GRCA sont adaptés aux programmes individuels et aux contextes organisationnels et opérationnels. Les plans de GRCA personnalisés posent les bases nécessaires pour déterminer si une technologie, un service, un composant de système ou un système convient aux fins prévues et s'il faut également adapter les contrôles en conséquence. Les plans de GRCA sur mesure aident les organisations à concentrer leurs ressources sur les fonctions les plus critiques de la mission et des activités conformément aux exigences liées à la mission et aux activités, ainsi qu'à l'environnement de risque. Les plans de GRCA comprennent une expression de la tolérance de l'organisation aux risques liés à la chaîne d'approvisionnement, les stratégies ou les contrôles d'atténuation des risques acceptables liés à la chaîne d'approvisionnement, un processus visant à évaluer et à surveiller continuellement les risques liés à la chaîne d'approvisionnement, les approches à adopter pour la mise en œuvre et la communication du plan, une description et une justification des mesures d'atténuation prises relativement aux risques liés à la chaîne d'approvisionnement, et les rôles et responsabilités connexes. Pour finir, les plans de GRCA portent sur les exigences liées au développement de systèmes et de composants de système fiables, sécurisés, résilients et protégeant la protection de la vie privée, ce qui comprend l'application des principes du développement sécurisé mis en œuvre dans le cadre des processus d'ingénierie de la sécurité des systèmes basée sur le cycle de vie (voir le contrôle SA-08).

SR-02(01) — Établissement d'une équipe de GRCA (---)

Énoncés :

Mettre en place une équipe de GRCA composée de [Affectation : personnel, rôles et responsabilités définis par l'organisation] pour diriger et soutenir les activités de GRCA suivantes : [Affectation : activités de GRCA définies par l'organisation].

Responsable : Aucun

Discussion :

Pour mettre en œuvre les plans de GRCA, les organisations devraient adopter une approche coordonnée axée sur les équipes pour relever et évaluer les risques liés à la chaîne d'approvisionnement et gérer ces risques au moyen de techniques d'atténuation programmatiques et techniques. L'approche axée sur les équipes permet aux organisations de procéder à l'analyse de leur chaîne d'approvisionnement, de communiquer avec des partenaires ou parties prenantes internes et externes, et d'en venir à un consensus quant aux ressources qu'il convient d'utiliser pour la GRCA. L'équipe de GRCA se compose du personnel de l'organisation à qui on a attribué différents rôles et différentes responsabilités pour assurer la direction et le soutien des activités de GRCA, ce qui comprend, entre autres, les fonctions liées à la gestion des risques, aux TI, à la passation de marché, à la sécurité de l'information, au respect de la vie privée, à la mission ou aux activités, à la chaîne d'approvisionnement, à la logistique, à l'approvisionnement et à la continuité des activités, ainsi que d'autres fonctions de nature juridique. Les membres de l'équipe de GRCA prennent part à divers aspects du CDS et ont collectivement une connaissance des processus d'acquisition, des pratiques juridiques, des vulnérabilités, des menaces et des vecteurs d'attaque et une expertise dans ces domaines, en plus de comprendre les aspects techniques et les dépendances des systèmes. L'équipe de GRCA peut être un prolongement des processus de gestion des risques liés à la sécurité et à la protection de la vie privée ou prendre part à une équipe de gestion des risques de l'organisation.

SR-03 — Contrôles et processus de la chaîne d'approvisionnement (---)

Énoncés :

a. Mettre en place un ou plusieurs processus pour relever et corriger les faiblesses ou les lacunes dans les éléments et les processus de la chaîne d'approvisionnement de [Affectation : systèmes ou composants de systèmes désignés par l'organisation] en coordination avec [Affectation : personnel de la chaîne d'approvisionnement désigné par l'organisation]
b. Utiliser les contrôles suivants pour offrir une protection contre les risques liés à la chaîne d'approvisionnement pour les systèmes, les composants de systèmes ou les services qui s'y rapportent ainsi que pour limiter les conséquences ou les dommages potentiels associés aux événements de la chaîne d'approvisionnement : [Affectation : contrôles de la chaîne d'approvisionnement définis par l'organisation]
c. Documenter les processus et les contrôles liés à la chaîne d'approvisionnement qui ont été sélectionnés et mis en œuvre dans [Sélection (un choix) : plans de sécurité et de protection de la vie privée; plan de GRCA; {Affectation : document défini par l'organisation}]

Responsable : Aucun

Discussion :

Les éléments de la chaîne d'approvisionnement incluent les organisations, les entités ou les outils qui servent à la recherche, au développement, à la conception, à la fabrication, à l'acquisition, à la livraison, à l'intégration, à l'exploitation, à la maintenance et à l'élimination des systèmes et des composants de systèmes. Les processus de la chaîne d'approvisionnement incluent les processus de développement du matériel, des logiciels et des micrologiciels; les procédures d'expédition et de traitement; les programmes de sécurité du personnel et de sécurité physique; les outils, les techniques et les mesures de gestion des configurations pour le maintien de la provenance; ou les autres programmes, processus ou procédures associés au développement, à l'acquisition, à la maintenance et à l'élimination des systèmes et des composants de système. Les éléments et les processus de la chaîne d'approvisionnement peuvent être fournis par les organisations, les intégratrices et intégrateurs de systèmes ou les fournisseurs externes. Les faiblesses ou les lacunes des éléments ou des processus de la chaîne d'approvisionnement représentent des vulnérabilités potentielles qui peuvent être exploitées par des adversaires afin de nuire à l'organisation et à sa capacité de réaliser sa mission ou ses activités. Le personnel de la chaîne d'approvisionnement se compose de personnes à qui on a attribué des responsabilités ou des rôles au sein de la chaîne d'approvisionnement.

SR-03(01) — Base d’approvisionnement diversifiée (---)

Énoncés :

Employer un ensemble diversifié de sources pour les composants de systèmes et les services suivants : [Affectation : composants de systèmes et services désignés par l’organisation].

Responsable : Aucun

Discussion :

Diversifier l’approvisionnement en systèmes, en composants de systèmes et en services peut réduire la probabilité que les adversaires arrivent à identifier et à cibler la chaîne d’approvisionnement et puissent limiter les répercussions d’un événement lié à la chaîne d’approvisionnement ou d’une compromission. Trouver plusieurs fournisseurs pour des composants de remplacement peut réduire la probabilité qu’un composant de remplacement devienne non disponible. Avoir recours à un ensemble diversifié de développeuses et développeurs ou de fournisseurs de services logistiques peut limiter les répercussions d’une catastrophe naturelle ou d’un autre événement lié à la chaîne d’approvisionnement. Les organisations devraient envisager de concevoir le système de manière à inclure du matériel et des composants diversifiés.

SR-03(02) — Limitation des dommages (---)

Énoncés :

Employer les contrôles suivants pour limiter les dommages pouvant être causés par d'éventuels adversaires qui pourraient identifier et cibler la chaîne d'approvisionnement organisationnelle : [Affectation : contrôles définis par l'organisation].

Responsable : Aucun

Discussion :

Les contrôles que l'on peut mettre en place pour réduire la probabilité que des adversaires arrivent à identifier et à cibler la chaîne d'approvisionnement consistent, notamment, à éviter d'acheter des configurations personnalisées ou non standard, à employer une liste de fournisseurs autorisés qui jouissent d'une réputation durable dans l'industrie, à respecter les calendriers de maintenance prédéterminés et à appliquer les mises à jour et les correctifs aux mécanismes de prestation, à tenir à jour un plan d'urgence en cas d'événement lié à la chaîne d'approvisionnement, à recourir à des mesures exceptionnelles en matière d'approvisionnement qui offrent des exclusions par rapport aux engagements et aux obligations, à utiliser des parcours de distribution diversifiés et à réduire le temps s'écoulant entre la décision d'acheter et la date de livraison.

SR-03(03) — Transfert d’exigences à des sous-traitants (---)

Énoncés :

S’assurer que les contrôles compris dans les contrats conclus avec les entrepreneurs principaux sont également inclus dans les contrats des sous-traitants.

Responsable : Aucun

Discussion :

Pour gérer efficacement et globalement les risques liés à la chaîne d’approvisionnement, il est important que les organisations s’assurent que les contrôles de GRCA sont inclus à tous les niveaux de la chaîne d’approvisionnement. On doit notamment s’assurer que les principaux fournisseurs ont mis en place les processus nécessaires pour faciliter le transfert d’exigences des contrôles de GRCA aux sous-traitants. Les contrôles sujets à un transfert d’exigences sont abordés dans le contrôle SR-03B.

SR-04 — Provenance (---)

Énoncés :

Documenter, surveiller et maintenir une provenance valide des systèmes et des composants de systèmes suivants, ainsi que de leurs données connexes : [Affectation : systèmes et composants de systèmes désignés par l'organisation et données connexes].

Responsable : Aucun

Discussion :

Tous les systèmes et composants de systèmes ont un point d'origine et peuvent être modifiés au cours de leur existence. La provenance est la chronologie de l'origine, du développement, de la propriété, de l'emplacement et des changements apportés à un système ou à un composant de système, ainsi qu'aux données connexes. Elle peut également comprendre le personnel et les processus utilisés pour interagir avec les systèmes, les composants ou les données connexes, ou pour y apporter des modifications. Les organisations devraient envisager d'élaborer des procédures (voir le contrôle SR-01) pour affecter les responsabilités liées à la création, au maintien et à la surveillance de la provenance des systèmes et des composants de systèmes, pour transférer la documentation et la responsabilité de la provenance d'une organisation à l'autre et pour prévenir et surveiller les changements non autorisés qui sont apportés aux enregistrements de provenance. Les organisations devraient employer des méthodes pour documenter, surveiller et maintenir des bases de provenance valides pour les systèmes, les composants de systèmes et les données connexes. Ces mesures aident à suivre, à évaluer et à documenter les changements apportés à la provenance, notamment ceux apportés à la configuration ou aux éléments de la chaîne d'approvisionnement, et permettent de garantir la non-répudiation de l'information relative à la provenance et des enregistrements des changements apportés à la provenance. Les facteurs à considérer relativement à la provenance sont abordés tout au long du cycle de développement des systèmes et intégrés aux contrats et aux autres ententes, le cas échéant.

SR-04(01) — Identité (---)

Énoncés :

Établir et maintenir une identification unique des éléments de la chaîne d'approvisionnement, des processus et du personnel associé au système désigné et aux composants de systèmes essentiels : [Affectation : éléments de la chaîne d'approvisionnement, processus et personnel associé aux systèmes et aux composants de systèmes essentiels désignés par l'organisation].

Responsable : Aucun

Discussion :

Il est essentiel d'être au fait des éléments et des parties prenantes qui font partie de la chaîne d'approvisionnement d'une organisation pour avoir une vue d'ensemble des activités liées à la chaîne d'approvisionnement et de leur nature. Il est également important de maintenir une vue d'ensemble des activités liées à la chaîne d'approvisionnement pour surveiller et relever les événements et les activités comportant un niveau élevé de risque. Sans cette vue d'ensemble des éléments, des processus et des parties prenantes de la chaîne d'approvisionnement, il est difficile pour les organisations de comprendre et de gérer les risques et de les rendre moins susceptibles de faire face à des événements préjudiciables. Les éléments de la chaîne d'approvisionnement incluent les organisations, les entités ou les outils qui servent à la recherche, au développement, à la conception, à la fabrication, à l'acquisition, à la livraison, à l'intégration, à l'exploitation, à la maintenance et à l'élimination des systèmes et des composants de systèmes. Les processus liés à la chaîne d'approvisionnement comprennent le processus de développement du matériel, des logiciels et des micrologiciels, les procédures d'expédition et de manutention, les outils, les techniques et les mesures de gestion des configurations permettant d'assurer la provenance; les programmes de sécurité physique et du personnel ou d'autres programmes, procédures ou processus associés à la production et à la distribution d'éléments de la chaîne d'approvisionnement. Le personnel de la chaîne d'approvisionnement comprend des personnes dont les rôles et les responsabilités consistent à sécuriser la recherche et le développement, la conception, la fabrication, l'acquisition, la livraison, l'intégration, l'exploitation, la maintenance et l'élimination d'un système ou d'un composant de système. Les méthodes d'identification sont suffisantes pour soutenir une enquête advenant un changement dans la chaîne d'approvisionnement (par exemple, l'achat d'une entreprise d'approvisionnement), une compromission ou un événement.

SR-04(02) — Suivi et localisation (---)

Énoncés :

Établir et maintenir une identification unique des systèmes et des composants de systèmes essentiels suivants aux fins de suivi tout au long de la chaîne d'approvisionnement : [Affectation : systèmes et composants de systèmes essentiels désignés par l'organisation].

Responsable : Aucun

Discussion :

Procéder au suivi de l'identification unique des systèmes et des composants de systèmes au cours des activités de développement et de transport offre une structure d'identité fondamentale à l'établissement et au maintien de la provenance. Par exemple, les composants de systèmes peuvent être étiquetés au moyen de numéros de série ou d'un radio-identifiant. Les étiquettes et les indicateurs peuvent aider à accroître la visibilité de la provenance d'un système ou d'un composant de système. Un système ou un composant de système peut comporter qu'un seul identificateur unique. Les méthodes d'identification sont suffisantes pour soutenir une investigation informatique advenant une compromission ou un événement lié à la chaîne d'approvisionnement.

SR-04(03) — Attestation de l'authenticité et de la non-altérité (---)

Énoncés :

Employer les contrôles suivants pour attester que le système ou le composant de système qui a été livré n'a pas été altéré : [Affectation : contrôles définis par l'organisation].

Responsable : Aucun

Discussion :

Pour plusieurs systèmes ou composants de systèmes – en particulier le matériel –, des moyens techniques peuvent être employés pour déterminer si les éléments sont authentiques ou s'ils ont été altérés. Il pourrait notamment être possible d'avoir recours à des étiquettes optiques et nanotechnologiques, à des fonctions impossibles à cloner physiquement, à une analyse des canaux auxiliaires, à la vérification du hachage cryptographique, aux signatures numériques et à des étiquettes d'inviolabilité visibles. Les contrôles peuvent également comprendre la surveillance des performances hors normes qui peuvent être un signe de trafiquage ou de contrefaçon. Les organisations peuvent tirer avantage des processus des fournisseurs et des entrepreneurs pour attester qu'un système ou un composant est authentique et n'a pas été altéré et pour remplacer tout système ou composant suspect. Il pourrait être possible de relever et d'atténuer certains signes de trafiquage avant d'accepter la livraison, comme un emballage irrégulier, des sceaux brisés et des étiquettes erronées. Si on soupçonne qu'un système ou un composant de système a été altéré ou contrefait, le fournisseur, l'entrepreneur ou le fabricant d'équipement d'origine peut être en mesure de remplacer l'article ou de fournir un moyen criminalistique de déterminer l'origine de la contrefaçon ou de l'altération de l'article. Les organisations peuvent fournir de la formation au personnel sur la façon de reconnaître les livraisons de systèmes ou de composants suspectes.

SR-04(04) — Intégrité de la chaîne d'approvisionnement – Pedigree (---)

Énoncés :

Employer [Affectation : contrôles définis par l'organisation] et procéder à [Affectation : analyse définie par l'organisation] pour assurer l'intégrité du système ou des composants de systèmes en validant la composition interne et la provenance des technologies, des produits et des services critiques ou essentiels à la mission.

Responsable : Aucun

Discussion :

L'information faisant autorité en ce qui concerne la composition interne des composants de systèmes et la provenance de la technologie, des produits et des services constitue une base de confiance solide. La validation de la composition interne et de la provenance des technologies, des produits et des services est ce qu'on appelle le « pedigree ». En microélectronique, cela comprend la composition matérielle des composants. Pour les logiciels, cela comprend la composition du code de source ouverte et du code propriétaire, notamment la version du composant à un moment précis. Les pedigrees renforcent l'assurance que les revendications formulées par les fournisseurs concernant la composition interne et la provenance des produits, des services et des technologies sont bel et bien valides. La validation de la composition interne et de la provenance peut être réalisée au moyen des divers artéfacts ou dossiers de preuve que les fabricants et les fournisseurs produisent au cours de la recherche et du développement, de la conception, de la fabrication, de l'acquisition, de la livraison, de l'intégration, de l'exploitation, de la maintenance et de l'élimination de la technologie, des produits et des services. Les artéfacts de preuve comprennent, sans s'y limiter, les étiquettes d'identification des logiciels, les indicateurs, l'inventaire des composants logiciels, les déclarations des fabricants sur les attributs des plateformes (par exemple, les numéros de série, l'inventaire des composants matériels) et les mesures (par exemple, les codes de hachage des micrologiciels) qui sont étroitement liées au matériel à proprement dit.

SR-05 — Stratégies, outils et méthodes d'acquisition (---)

Énoncés :

Utiliser les stratégies d'acquisition, les méthodes d'approvisionnement et les outils de passation de marchés suivants afin de déterminer, de contrer et d'atténuer les risques associés à la chaîne d'approvisionnement : [Affectation : stratégies d'acquisition, outils de passation de marchés et méthodes d'approvisionnement définis par l'organisation].

Responsable : Aucun

Discussion :

Le recours au processus d'acquisition fournit un véhicule important pour la protection de la chaîne d'approvisionnement. Il existe de nombreux outils et de nombreuses techniques, notamment le masquage de l'utilisation finale d'un système ou d'un composant de système, les achats voilés ou filtrés, l'exigence d'un emballage avec sceau d'inviolabilité ou le recours à une distribution fiable ou contrôlée. Les résultats d'une évaluation des risques liés à la chaîne d'approvisionnement peuvent orienter et informer le choix des stratégies, des outils et des méthodes qui conviennent le mieux à la situation. Les outils et les techniques peuvent fournir une protection contre la production non autorisée, le vol, la modification, la contrefaçon, l'insertion de code malveillant ou de porte dérobée et les mauvaises pratiques de développement tout au long du cycle de développement des systèmes. Les organisations devraient également penser à offrir des mesures incitatives pour les fournisseurs afin de mettre en œuvre des contrôles et de favoriser la transparence des processus et des pratiques de sécurité et de protection de la vie privée. Elles peuvent également fournir un libellé de contrat qui traite de l'interdiction d'utiliser des composants contaminés ou contrefaits et restreindre les achats des fournisseurs qui ne sont pas dignes de confiance. Les organisations devraient considérer de fournir des programmes de formation et de sensibilisation pour le personnel concernant les risques liés à la chaîne d'approvisionnement, les stratégies d'atténuation disponibles et les circonstances appropriées pour utiliser les programmes. Les méthodes utilisées pour examiner et protéger les plans de développement, la documentation et les preuves doivent être appropriées selon les exigences de sécurité et de protection de la vie privée de l'organisation. Les contrats peuvent également préciser les exigences relatives à la protection des documents.

SR-05(01) — Approvisionnement adéquat (---)

Énoncés :

Employer les contrôles suivants pour assurer un approvisionnement adéquat de [Affectation : composants de systèmes essentiels désignés par l'organisation] : [Affectation : contrôles définis par l'organisation].

Responsable : Aucun

Discussion :

Des adversaires pourraient tenter de contrecarrer les opérations organisationnelles en entravant l'approvisionnement de composants essentiels des systèmes ou en interférant avec les activités des fournisseurs. Les organisations peuvent assurer le suivi de la durée moyenne de fonctionnement avant défaillance des systèmes et des composants pour atténuer la perte temporaire ou permanente de fonction du système. Les contrôles qui permettent d'assurer un approvisionnement adéquat des composants de systèmes essentiels comprennent l'utilisation de multiples fournisseurs tout au long de la chaîne d'approvisionnement pour les composants essentiels identifiés, l'emmagasinage de composants de rechange pour garantir le déroulement des activités dans des périodes essentielles à la mission et la détermination des composants identiques ou similaires sur le plan des fonctionnalités qui pourraient être utilisés, le cas échéant.

SR-05(02) — Évaluation préalable à la sélection, à l'acceptation, à la modification ou à la mise à jour (---)

Énoncés :

Procéder à l'évaluation d'un système, d'un composant du système ou d'un service qui s'y rapporte préalablement à la sélection, à l'acceptation, à la modification ou à la mise à jour.

Responsable : Aucun

Discussion :

Des membres du personnel de l'organisation ou des parties prenantes externes indépendantes devraient procéder à l'évaluation des systèmes, des composants, des outils et des services pour relever les signes de trafiquage, les vulnérabilités accidentelles et intentionnelles ou les preuves de non-conformité avec les contrôles de la chaîne d'approvisionnement. Cela comprend le code malveillant, les processus malveillants, les logiciels défectueux, les portes dérobées et la contrefaçon. Les évaluations peuvent comprendre les examens des propositions de conceptions, les inspections visuelles ou physiques et les analyses dynamiques, les inspections visuelles, par rayon X ou des particules magnétiques, les simulations, les tests de la boîte blanche, grise ou noire, les tests à données aléatoires, les essais marginaux et les tests d'intrusion (voir le contrôle SR-06(01)). Les preuves cumulées pendant les évaluations devraient être documentées de façon à ce que les organisations puissent procéder aux mesures consécutives. Les preuves générées au cours des évaluations organisationnelles et indépendantes des éléments de la chaîne d'approvisionnement peuvent être utilisées pour améliorer les processus de la chaîne d'approvisionnement et guider le processus de GRCA. Les preuves peuvent être obtenues lors d'évaluations de suivi. Les preuves et les autres documents peuvent être communiqués conformément aux ententes organisationnelles.

SR-06 — Évaluations et examens des fournisseurs (---)

Énoncés :

Évaluer et examiner les risques liés à la chaîne d'approvisionnement associés aux fournisseurs, aux entrepreneures ou aux entrepreneurs ainsi que le système, le composant de système ou le service fourni par ces derniers [Affectation : fréquence définie par l'organisation].

Responsable : Aucun

Discussion :

Une évaluation et un examen du risque associé aux fournisseurs incluent les processus de GRCA et des risques liés à la sécurité; la propriété, le contrôle et l'influence de l'étranger (PCIE) et la capacité des fournisseurs à évaluer efficacement les fournisseurs, les entrepreneuses et les entrepreneurs subalternes de deuxième ou troisième niveau. Les examens peuvent être effectués par l'organisation ou une tierce partie indépendante. Les examens devraient considérer les processus et les contrôles documentés, le renseignement provenant de toute source et l'information accessible au public concernant le fournisseur, l'entrepreneuse ou l'entrepreneur. Les organisations peuvent utiliser de l'information de source ouverte pour surveiller les signes d'information volée, d'un mauvais développement, de mauvaises pratiques de contrôle de la qualité, d'une fuite de renseignements ou d'une contrefaçon. Dans certains cas, il pourrait être approprié ou nécessaire de partager les résultats des évaluations et des examens avec d'autres organisations conformément aux règles et aux politiques applicables, ou aux accords et contrats interorganisationnels.

SR-06(01) — Tests et analyse (---)

Énoncés :

Employer [Sélection (un choix ou plus) : analyse organisationnelle; analyse d'une tierce partie indépendante; tests par l'organisation; tests par une tierce partie indépendante] des éléments de la chaîne d'approvisionnement, des parties prenantes et des processus suivants relativement au système, au composant de système ou au service qui s'y rapporte : [Affectation : éléments de la chaîne d'approvisionnement, processus, intervenantes et intervenants désignés par l'organisation].

Responsable : Aucun

Discussion :

Il convient de tenir compte de la relation entre les entités et les procédures dans la chaîne d'approvisionnement, comme le développement et la livraison. Les éléments de la chaîne d'approvisionnement incluent les organisations, les entités ou les outils qui servent à la recherche, au développement, à la conception, à la fabrication, à l'acquisition, à la livraison, à l'intégration, à l'exploitation, à la maintenance et à l'élimination des systèmes, des composants de systèmes ou des services qui s'y rapportent. Les processus liés à la chaîne d'approvisionnement comprennent les programmes de GRCA, les stratégies et les plans de mise en œuvre de la GRCA, les programmes de sécurité physique et du personnel, les processus de développement du matériel, des logiciels et des micrologiciels, les outils, les techniques et les mesures de gestion des configurations permettant d'assurer la provenance, les procédures d'expédition et de manutention, ainsi que les programmes, les procédures ou les processus associés à la production et à la distribution des éléments de la chaîne d'approvisionnement. Les intervenants de la chaîne d'approvisionnement sont des personnes auxquelles on a attribué des responsabilités ou des rôles particuliers au sein de la chaîne d'approvisionnement. Les preuves générées et collectées par les analyses et les tests menés sur les éléments, les processus et les parties prenantes de la chaîne d'approvisionnement sont documentées et utilisées de façon à éclairer les prises de décision et les activités relatives à la gestion organisationnelle des risques.

SR-07 — Sécurité opérationnelle de la chaîne d'approvisionnement (---)

Énoncés :

Employer les contrôles de sécurité opérationnelle (OPSEC pour Operational Security) pour protéger l'information relative à la chaîne d'approvisionnement pour le système, le composant de système ou le service qui s'y rapporte : [Affectation : contrôles d'OPSEC définis par l'organisation].

Responsable : Aucun

Discussion :

Le contrôle d'OPSEC de la chaîne d'approvisionnement étend la portée de l'OPSEC de manière à inclure les fournisseurs actuels et éventuels. L'OPSEC est un processus qui consiste à identifier l'information critique, à analyser des actions amies accompagnant les opérations et les autres activités visant à identifier les actions pouvant être observées par d'éventuels adversaires, à déterminer les indicateurs que les adversaires pourraient obtenir et mettre en perspective ou interpréter de façon à révéler des renseignements essentiels en assez de temps pour causer des dommages aux organisations, à mettre en œuvre les mesures de protection et les contremesures visant à éliminer les vulnérabilités exploitables ou à les réduire à un niveau acceptable et à imaginer comment les amalgames de renseignements pourraient compromettre la confidentialité des utilisatrices, des utilisatrices ou les utilisations de la chaîne d'approvisionnement. L'information de la chaîne d'approvisionnement comprend les identités des utilisatrices et utilisateurs, les utilisations des systèmes, des composants de systèmes et des services qui s'y rapportent, les identités des fournisseurs, les exigences de sécurité et de protection de la vie privée, les configurations des systèmes et des composants, les processus des fournisseurs, les spécifications de conception et les résultats des tests et des évaluations. L'OPSEC de la chaîne d'approvisionnement peut exiger que les organisations soustraient aux fournisseurs l'information relative à la mission et aux activités, et peut inciter ces organisations à avoir recours à des intermédiaires dans le but de taire l'identité des utilisatrices et des utilisateurs ou les utilisations des systèmes, des composants de systèmes ou des services qui s'y rapportent.

SR-08 — Ententes de notification (---)

Énoncés :

Mettre en place des ententes et des procédures avec les entités qui prennent part à la chaîne d'approvisionnement du système, du composant de système ou du service qui s'y rapporte pour [Sélection (un choix ou plus) : la notification des compromissions touchant la chaîne d'approvisionnement; les résultats des évaluations ou des vérifications; {Affectation : information définie par l'organisation}].

Responsable : Aucun

Discussion :

La mise en place d'ententes et de procédures facilite la communication entre les entités de la chaîne d'approvisionnement. Le signalement précoce des compromissions et des compromissions potentielles de la chaîne d'approvisionnement pouvant nuire ou ayant pu nuire aux systèmes ou aux composants des systèmes de l'organisation est essentiel aux organisations qui veulent réagir efficacement à de tels incidents. Les résultats des évaluations ou des vérifications comprennent l'information de source ouverte qui a contribué à la prise d'une décision ou à un résultat, et qui pourrait être utilisée pour aider l'entité de la chaîne d'approvisionnement à répondre à des préoccupations ou à améliorer ses processus.

SR-09 — Résistance au trafiquage et détection (---)

Énoncés :

Mettre en œuvre un programme de protection contre le trafiquage pour le système, le composant de système ou le service qui s'y rapporte.

Responsable : Aucun

Discussion :

Les technologies, les outils et les techniques de protection contre le trafiquage offrent un niveau de protection pour les systèmes, les composants de systèmes et les services contre plusieurs menaces, notamment la rétro-ingénierie, la modification et la substitution. Les modalités robustes d'identification combinées aux moyens permettant de contrer et de détecter le trafiquage sont essentielles, lorsqu'il s'agit d'assurer la protection des systèmes et des composants pendant la distribution et l'utilisation.

SR-09(01) — Phases multiples du cycle de développement de systèmes (---)

Énoncés :

Avoir recours à des technologies, des outils et des techniques de protection contre le trafiquage tout au long du cycle de développement de systèmes.

Responsable : Aucun

Discussion :

Le cycle de développement de systèmes comprend la recherche et le développement, la conception, la fabrication, l'acquisition, la livraison, l'intégration, l'exploitation, la maintenance et l'élimination. Les organisations devraient utiliser une combinaison de dispositifs matériels et logiciels pour contrer et détecter le trafiquage. Les organisations devraient avoir recours à l'obscurcissement et aux autovérifications pour rendre la rétro-ingénierie et les modifications difficiles, chronophages et onéreuses pour les adversaires. La personnalisation des systèmes et des composants de systèmes peut rendre les substitutions plus faciles à détecter, ce qui permet de limiter les dommages.

SR-10 — Inspection des systèmes ou des composants (---)

Énoncés :

Inspecter les systèmes ou les composants de systèmes suivants [Sélection (un choix ou plus) : de façon aléatoire; tous les {Affectation : fréquence définie par l'organisation}, lorsque {Affectation : indications concernant le besoin de mener une inspection définies par l'organisation}] pour détecter le trafiquage : [Affectation : systèmes ou composants de systèmes désignés par l'organisation].

Responsable : Aucun

Discussion :

L'inspection des systèmes ou des composants de systèmes aux fins de résistance au trafiquage et de détection porte sur le trafiquage physique et logique et s'applique aux systèmes et aux composants de systèmes à l'extérieur des zones contrôlées par l'organisation. Il convient de procéder à une inspection lorsqu'il y a des changements dans l'emballage, les spécifications, le site de fabrication ou l'entité de la pièce achetée et lorsque des personnes reviennent d'un voyage dans un lieu à risque élevé.

SR-11 — Authenticité des composants (---)

Énoncés :

a. Développer et mettre en œuvre une stratégie et des procédures qui visent à combattre la contrefaçon et qui prévoient la mise en place de mesures visant à détecter et à prévenir l'entrée de dispositifs contrefaits dans les systèmes
b. Signaler les composants de systèmes qui ont été contrefaits à [Sélection (un choix ou plus) : source de composant contrefait; {Affectation : organisations externes responsables du signalement désignées par l'organisation}; {Affectation : personnel ou rôles définis par l'organisation}]

Responsable : Aucun

Discussion :

Les sources de composants contrefaits pourraient comprendre les fabricants, les développeuses et développeurs, les fournisseurs et les entrepreneuses et entrepreneurs. Les stratégies et les procédures visant à combattre la contrefaçon renforcent la résistance au trafiquage et fournissent un niveau de protection contre l'introduction de code malveillant.

SR-11(01) — Formation anticontrefaçon (---)

Énoncés :

Former [Affectation : personnel ou rôles définis par l'organisation] dans le domaine de la détection des composants contrefaits de systèmes (y compris les composants matériels, logiciels et microgiciels).

Responsable : Aucun

SR-11(02) — Contrôle des configurations pour l'entretien et la réparation des composants (---)

Énoncés :

Maintenir le contrôle des configurations pour les composants de systèmes suivants appelés à subir un entretien ou une réparation, ainsi que des composants réparés ou entretenus qui sont appelés à retourner à leur lieu de service : [Affectation : composants de systèmes désignés par l'organisation].

Responsable : Aucun

SR-11(03) — Analyse anticontrefaçon (---)

Énoncés :

Analyser les composants de systèmes [Affectation : fréquence définie par l'organisation] pour détecter la contrefaçon.

Responsable : Aucun

Discussion :

Le type du composant détermine le type d'analyse à effectuer (par exemple, une analyse d'applications Web si le composant est une application Web).

SR-12 — Mise hors service des composants (---)

Énoncés :

Éliminer [Affectation : données, documents, outils ou composants de systèmes désignés par l'organisation] au moyen des techniques et des méthodes suivantes : [Affectation : techniques et méthodes définies par l'organisation].

Responsable : Aucun

Discussion :

Les données, les documents, les outils ou les composants de systèmes peuvent être mis hors service à tout moment durant le cycle de développement des systèmes (non seulement au cours de la phase d'élimination ou de retrait du cycle de vie). Par exemple, la mise hors service peut survenir au cours de la recherche, du développement, de la conception, du prototypage, de l'exploitation ou de la maintenance et comprendre des méthodes comme le nettoyage de disque, le retrait des clés cryptographiques ou la réutilisation partielle des composants. Les risques de compromission lors de la mise hors service touchent les données physiques et logiques, y compris les documents papier et les fichiers numériques, les documents portant sur l'expédition et la livraison, les clés USB contenant du code logiciel ou les routeurs et serveurs complets qui contiennent des supports permanents sur lesquels on retrouve de l'information sensible ou exclusive. De plus, une mise hors service adéquate des composants de systèmes aide à empêcher que les composants en question ne soient introduits dans le marché semi-clandestin (marché gris).