CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

PL-09

Gestion centrale

Juill. 2026

Votre gouvernement

Québec

PL

Planification de la cybersécurité

Planning

PL-09 — Gestion centrale (-F-) (Obligatoire)

Énoncés :

Centraliser la gestion des [Affectation : contrôles et processus connexes définis par l'organisation].

Paramètres :

- géré centralement par l'OP : mesures PM-05, CM-08, AT-02, AT-02(01), AC-19, AU-12 - géré centralement par le ministère de la Cybersécurité et du Numérique (MCN) : mesure RA-05
aaQC. en tout temps; OP, COCD et CGCD

Responsable : Partagée

Date limite de mise en oeuvre : 2024-12-14

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.