CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

CA-02

Évaluations de contrôle

Juill. 2026

Votre gouvernement

Québec

CA

Évaluation des systèmes et autorisation

Security Assessment and Authorization

CA-02 — Évaluations de contrôle (PaFF)

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.