CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

CA-06

Autorisation

Juill. 2026

Votre gouvernement

Québec

CA

Évaluation des systèmes et autorisation

Security Assessment and Authorization

CA-06 — Autorisation (PaFF)

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.