CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

SA-24

Conception aux fins de cyberrésilience

Juill. 2026

Votre gouvernement

Québec

SA

Acquisition sécurisée des systèmes/services

System and Services

SA-24 — Conception aux fins de cyberrésilience (PcEE)

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.