



CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

CA-07

Surveillance continue

Juill. 2026



Évaluation des systèmes et autorisation

Security Assessment and Authorization

CA-07 – Surveillance continue (PaFF)

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]

Paramètres :

- a. minimalement les mesures de sécurité mises en place conformément aux exigences gouvernementales
- b. à définir par l'organisme selon le contexte; minimalement 1 fois par année
- g. chef sécurité de la sécurité de l'information organisationnelle; mensuellement

Responsable : OP

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.