



CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

AU-06

Examen, analyse et production de rapports liés aux enregistrements de vérification

Juill. 2026



Journaux d'audit, traçabilité des actions

Audit and Accountability

AU-06 – Examen, analyse et production de rapports liés aux enregistrements de vérification (PaF-)

Énoncés :

- a. Examiner et analyser les enregistrements de vérification du système tous les [Affectation : fréquence définie par l'organisation] pour déceler toute indication de [Affectation : activités inappropriées ou inhabituelles définies par l'organisation] et les répercussions potentielles d'activités inappropriées ou inhabituelles
- b. Faire rapport des résultats à [Affectation : personnel ou rôles définis par l'organisation]
- c. Ajuster le niveau d'examen, d'analyse et de rapports d'enregistrements de vérification dans le système lorsqu'un changement fondé sur des renseignements relatifs au maintien de l'ordre, du renseignement brut ou d'autres sources crédibles d'information est apporté au risque

Paramètres :

- a. minimalement 1 fois par semaine; à définir par l'organisme
- b. à définir par l'organisme (ex.: détenteur, responsable de cybersécurité, etc.)

Responsable : OP

Discussion :

L'examen, l'analyse et les rapports des dossiers vérification portent sur la journalisation en matière de sécurité et de protection de la vie privée de l'information qu'effectuent les organisations, ce qui comprend la journalisation qui découle de la surveillance de l'utilisation d'un compte, de l'accès à distance, de la connectivité sans fil, de la connexion d'appareils mobiles, de paramètres de configuration, de l'inventaire des composants de système, de l'utilisation d'outils de maintenance et de télémaintenance, de l'accès physique, de la température et de l'humidité, de la livraison et du retrait d'équipement, de communications aux frontières du système et de l'utilisation de code mobile et de voix sur protocole Internet (VoIP pour Voice over Internet Protocol). Les résultats peuvent être communiqués aux entités organisationnelles, comme l'équipe d'intervention en cas d'incident, le service de dépannage et le bureau de la sécurité ou de la protection de la vie privée. Dans la mesure du possible, les renseignements personnels devraient être supprimés des journaux de vérification s'ils ne sont pas nécessaires aux processus de production de rapports. Si les organisations ne sont pas autorisées à examiner et à analyser les enregistrements de vérification ou si elles sont incapables de mener de telles activités, les activités d'examen et d'analyse peuvent être menées par les organisations disposant d'une telle autorité. Il est possible d'ajuster la fréquence, la portée ou la profondeur de l'examen, de l'analyse ou des rapports de vérification des dossiers pour répondre aux besoins organisationnels lorsqu'une nouvelle information est reçue.