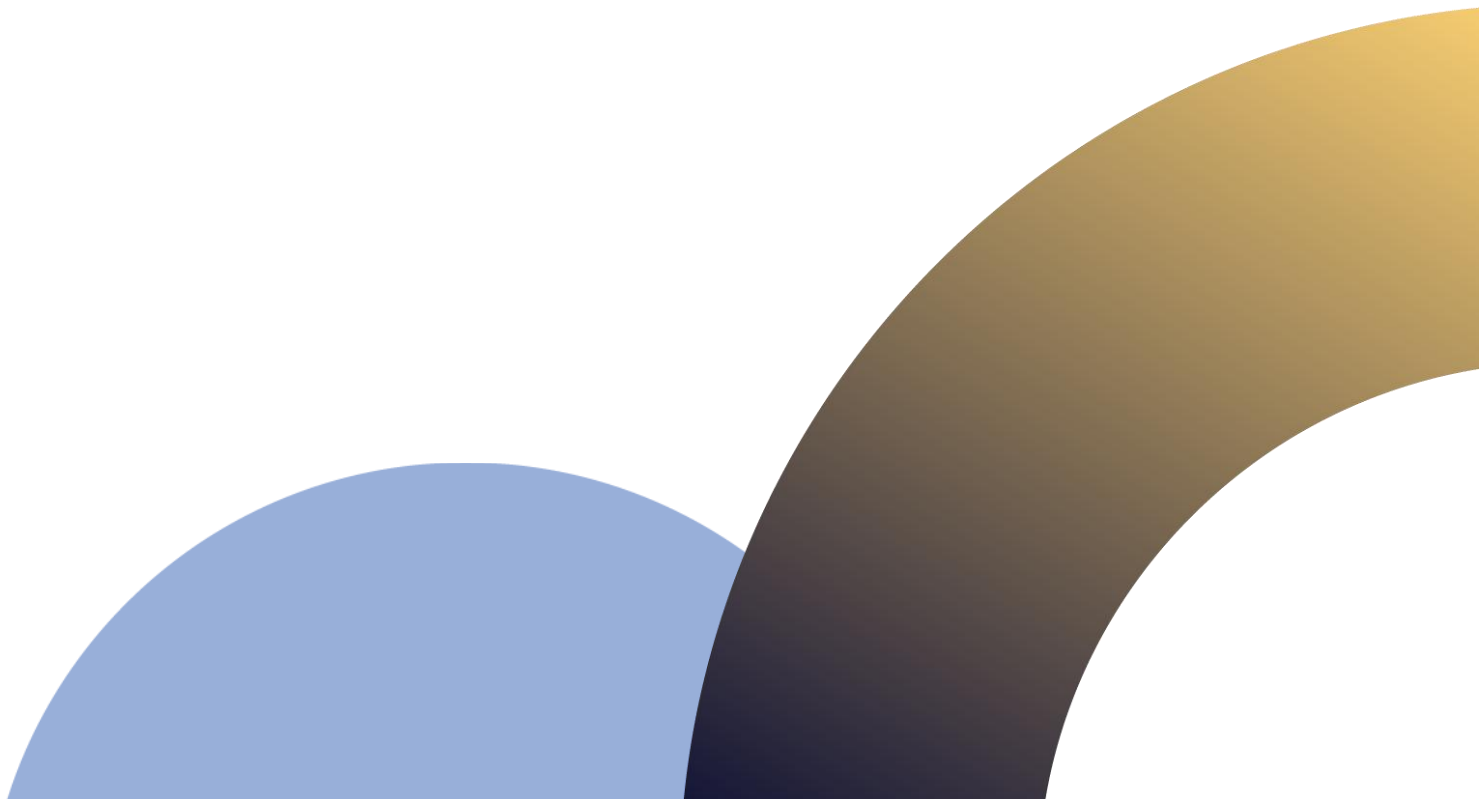
Non protégé

Audit de la cybersécurité (Avis de mise en œuvre de la politique sur la sécurité)

Rapport sommaire (pour publication en ligne)

Direction générale de la
vérification et de l'évaluation
Juillet 2025



Vous pouvez lire cette publication en ligne à l'adresse https://ised-isde.canada.ca/site/verification-evaluation/fr/verification-interne/rapports-verification-interne-annee-fiscale/audit-cybersecurite-avis-mise-oeuvre-politique-securite-rapport-sommaire

Pour obtenir un exemplaire de cette publication ou un format substitut (braille, gros caractères, etc.), veuillez remplir le formulaire de demande de publication à l'adresse https://www.ic.gc.ca/eic/site/iccat.nsf/frm-fra/EABV-9E9HE7 ou écrire à l'adresse suivante :

Centre de services aux citoyens d'ISDE
Innovation, Sciences et Développement économique Canada
édifice C.D. Howe
235, rue Queen
Ottawa, ON K1A 0H5
Canada

Téléphone (sans frais au Canada) : 1-800-328-6189
Téléphone (international) : 613-954-5031
ATS (pour les malentendants) : 1-866-694-8389
Heures de bureau : de 8 h 30 à 17 h (heure de l'Est)
Courriel : ISED@Canada.ca

Autorisation de reproduction

No de cat. Iu4-447/2026F-PDF

ISBN 978-0-660-79608-6

Also available in English under the title *Audit of Cyber Security (Security Policy Implementation Notice).*

Iu4-447/2026F-PDF
ISBN 978-0-660-79608-6

Contexte

La cybersécurité au gouvernement du Canada (GC)

En août 2024, le Secrétariat du Conseil du Trésor (SCT) a publié l'*Avis de mise en œuvre de la Politique sur la sécurité (AMOPS) : Renforcement de la cybersécurité* afin de renforcer les exigences énoncées dans la *Politique sur la sécurité du gouvernement* et la *Politique sur les services et le numérique*. L'AMOPS vise à :

- réduire la surface d'attaque globale et à minimiser le risque d'accès non autorisé aux systèmes d'information du GC dès que possible;
- remédier diligemment aux vulnérabilités exploitées connues afin de protéger les systèmes d'information du GC et de réduire les cyberincidents;
- réaliser des progrès mesurables permettant une meilleure connaissance des actifs des ministères et organismes et des vulnérabilités qui y sont associées.

Pour atteindre ces objectifs, l'AMOPS prévoyait que tous les ministères mettent en place des mesures appropriées pour protéger les actifs de Technologie de l'information (TI). Ces mesures incluent le déploiement de capteurs au niveau de l'hôte, l'élaboration d'un plan visant à identifier, à évaluer et à corriger les vulnérabilités énoncées dans la liste des 25 principales vulnérabilités établie par le SCT, et la mise en œuvre de solutions d'authentification multifacteur et de mesures de sécurité conçues pour résister à l'hameçonnage. Le SCT avait établi un échéancier variant de trois à neuf mois, selon l'initiative. Innovation, Sciences et Développement Économique (ISDE) devait satisfaire à toutes les exigences de cybersécurité de l'AMOPS en mai 2025.

Mise en œuvre de l'AMOPS à ISDE

À ISDE, le Secteur du service de transformation numérique (SSTN) et le dirigeant principal de l'information (DPI) sont responsables de l'élaboration, de la mise en œuvre, du renforcement et du suivi des exigences, des pratiques et des contrôles ministériels en matière de sécurité des TI. La responsabilité de veiller au respect des exigences de l'AMOPS est déléguée au directeur de la sécurité, qui agit également à titre de responsable ministériel de la cybersécurité. Le directeur doit rendre compte des progrès réalisés au DPI et au Comité de gestion du dirigeant principal de l'information.

Missions antérieures

De 2020 à 2025, la Direction générale de la vérification et de l'évaluation (DGVE) a mené cinq missions portant sur divers aspects et contrôles de l'environnement de cybersécurité d'ISDE, notamment sur les points de terminaison et le nuage. De nombreux éléments demandés par le SCT dans l'AMOPS, tels que l'authentification multifacteur, la gestion des vulnérabilités et la gestion des rustines, ont été vérifiés dans le cadre de ces missions. Cependant, les exigences de l'AMOPS sont différentes, ce qui nécessite un regard neuf sur ces éléments.

Objectif et portée de l'audit

Cette mission avait pour objectif d'évaluer la conformité d'ISDE à l'AMOPS.

La mission portait sur l'évaluation de la conformité à toutes les exigences de l'AMOPS applicables à ISDE, notamment :

- l'examen des dossiers ministériels sur les systèmes d'information qui soutiennent les services et les activités critiques dans l'outil de gestion du portefeuille des applications du Bureau du dirigeant principal de l'information du SCT ou dans un outil comparable;
- le déploiement de capteurs du Centre canadien pour la cybersécurité (CCC) sur tous les points de terminaison des clients, conformément aux Mesures de protection du nuage du gouvernement du Canada;
- l'élaboration d'un plan suivant une approche fondée sur les risques afin d'identifier, d'évaluer et de corriger les vulnérabilités énoncées dans la liste des 25 principales vulnérabilités établie par le SCT et la mise en œuvre de mesures d'atténuation;
- l'élaboration d'un plan de gestion des rustines qui définit clairement les rôles et les responsabilités;
- l'intégration de systèmes accessibles au public dans le Système national de notification de cybermenace du CCC;
- la mise en œuvre de configurations d'accès à distance sécurisées qui imposent une authentification multifacteur conçue pour résister à l'hameçonnage et qui fournissent une connexion sécurisée et encryptée au réseau intégré du gouvernement du Canada.

Cet audit portait sur tous les points de terminaison et tous les systèmes internes et publics gérés par ISDE. Il couvrait la période d'août 2024 à mai 2025. Les actifs de technologie de l'information gérés par Services Partagés Canada (SPC) n'étaient pas inclus dans la portée de la mission.

Démarche

La méthodologie utilisée comprenait diverses procédures visant à atteindre l'objectif de la mission, telles que :

- l'examen de documents;
- des entrevues;
- des présentations détaillées des systèmes et des processus;
- l'échantillonnage et le test des points de terminaison et des configurations d'accès à distance sécurisées.

Critères

En fonction de l'évaluation des risques de l'entité, des critères et des sous-critères d'examen liés à l'objectif général ont été élaborés pour cette mission (voir l'annexe A). Ils suivent généralement la structure des exigences de l'AMOPS.

Conformité

Cette mission a été menée conformément aux normes de l'Institut des auditeur internes et à la *Politique sur l'audit interne* du Conseil du Trésor, comme le confirment les résultats du programme d'assurance et d'amélioration de la qualité de la Direction générale de la vérification et de l'évaluation.

Constatations et conclusions

Les constatations et les conclusions de cet audit ont été communiquées à l'interne au SSTN, au DPI, au sous-ministre et au Comité ministériel d'audit. Pour des raisons de sécurité, la Direction générale de la vérification et de l'évaluation ne publie pas les constatations d'audit liées aux analyses de cybersécurité.

Annexe A : Critères d'examen

Critères d'examen	Sous-critères
Critère thématique - Identifier les actifs	
Critère 1 : Une visibilité complète et continue des actifs est assurée, ainsi que leur surveillance, afin de gérer efficacement les risques liés à la cybersécurité du réseau intégré d'ISDE.	Les renseignements saisis dans le système de gestion du portefeuille des applications (GPA) pour les applications critiques à la mission sont exacts et complets.
	Les capteurs du CCC ont été déployés sur les points de terminaison.
	Les capteurs infonuagiques du CCC ont été entièrement déployés, conformément aux Mesures de protection du nuage du gouvernement du Canada.
Critère thématique – Comprendre l'exposition	
Critère 2 : Il existe une compréhension des risques liés à la sécurité des actifs afin de permettre une approche fondée sur les risques pour hiérarchiser les mesures d'atténuation.	Le plan visant à recenser, évaluer et corriger les vulnérabilités figurant dans la liste des 25 principales vulnérabilités est complet et fondé sur les risques.
	Le plan de gestion des rustines, qui vise à faciliter l'application des rustines pour corriger les vulnérabilités critiques, est complet et conforme aux directives du GC et de SPC.
	Les systèmes accessibles au public ont été intégrés au Système national de notification des cybermenaces du CCC. Ainsi, les ministères sont informés des services mal configurés, des vulnérabilités et des infrastructures compromises sur leur fourchette d'adresses IP.
Critère thématique – Réduire l'exposition	
Critère 3 : La surface d'attaque globale d'ISDE a été réduite et des mesures de protection ont été mises en place afin de minimiser le risque d'accès non autorisé aux systèmes d'information du ministère.	Des stratégies d'atténuation ont été mises en œuvre pour corriger les vulnérabilités figurant dans la liste des 25 principales vulnérabilités. Elles ont été choisies selon les plans d'action élaborés (en réponse au critère 6.2.2 de l'AMOPS), en accordant la priorité aux systèmes d'information accessibles au public.
	L'authentification multifacteur est appliquée avec des mesures de sécurité visant à garantir la résistance à l'hameçonnage de l'ensemble du processus d'authentification, par exemple en s'assurant que l'utilisateur s'authentifie à partir d'un appareil géré par le GC, en vérifiant que l'appareil est configuré correctement et en détectant toute géolocalisation anormale.
	Une connexion sécurisée et encryptée au réseau intégré du GC (section 3.1 des Exigences de configuration de l'accès à distance) utilisant des voies approuvées par le GC pour accéder à Internet plutôt qu'une connexion directe à Internet, afin de tirer parti du service de cyberdéfense du CCC.