Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat
Canada

Audit de la sécurité des TI – Phase I

Publié : le 2025-09-22

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

No de catalogue BT66-101/1-2025F-PDF
ISBN: 978-0-660-79019-0

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Audit of IT Security – Phase I

Audit de la sécurité des TI – Phase I

Sur cette page

Survol des résultats

▶ Dans cette section

Importance

Le Secrétariat du Conseil du Trésor du Canada (SCT) appuie un comité du Cabinet et son rôle d’organisme central. Par conséquent, il est essentiel de mettre en œuvre de bonnes pratiques en matière de sécurité des technologies de l’information (TI) pour assurer la protection des fonds de renseignements personnels et sensibles.

Objectif

Évaluer l’efficacité, la pertinence et la conformité des activités liées à la sécurité des TI du SCT afin de cerner, de gérer et d’atténuer les vulnérabilités et les menaces.

Portée

Examen des activités liées à la sécurité des TI du SCT pertinentes menées entre août 2022 et novembre 2024.

Observations

Dans l’ensemble, aucune constatation ne pose de risques importants ou graves pour les activités et les fonds de renseignements du SCT. Cependant, la direction pourrait se concentrer sur quelques domaines pour améliorer l’efficacité ou l’harmonisation avec les politiques pangouvernementales.

Recommandation

- On recommande à la secrétaire adjointe, Secteur des services ministériels, et dirigeante principale des finances d’examiner et de mettre à jour, au besoin, certains documents de politique et de procédure pour veiller à ce qu’ils soient complets et qu’ils cadrent avec les instruments de politique pangouvernementaux ou le cycle de vie de développement des systèmes du Ministère.

En l’absence de documents de politique et de procédure à jour, la capacité du Bureau de la vérification interne et de l’évaluation (BVIE) à évaluer la conformité et l’efficacité opérationnelle de certains contrôles liés à la sécurité des TI sera limitée dans les missions prévues au cours des prochaines années.

Considérations

Outre ce qui figure à la recommandation, les deux domaines qui peuvent doivent être examinés par la direction afin d’améliorer l’efficacité.

- Désigner un comité ministériel à titre de tribune pour présenter plus régulièrement de l'information à la haute direction ou solliciter ses commentaires sur les questions touchant à la sécurité des TI.
- Procéder à un examen de la façon dont les renseignements sont organisés dans le répertoire d'applications du Ministère.

Contexte

Il est clairement mentionné dans la Stratégie intégrée de cybersécurité du gouvernement du Canada que « le caractère de plus en plus numérique du gouvernement du Canada (GC) et sa dépendance à l'égard de la technologie de l'information font du GC une cible attrayante en raison des informations personnelles, des données de recherche précieuses et d'autres informations sensibles qu'il détient ». Il y est également mentionné que « le fait de garantir la confidentialité, l'intégrité et l'accessibilité des informations et des réseaux du GC est essentiel pour la prestation de services numériques sûrs et fiables [1] ».

Étant donné que le SCT appuie un comité du Cabinet et son rôle d'organisme central, de bonnes pratiques de sécurité des TI [2] sont essentielles pour protéger ses fonds de renseignements personnels et sensibles.

Au cours des cinq dernières années, les pratiques de sécurité des TI du SCT ont connu une évolution et des changements en raison du passage à des services plus infonuagiques, comme Microsoft 365 (M365), et des modèles de travail à distance et hybrides offerts aux employés.

À la lumière de cette transition vers les services infonuagiques, il s'agit du premier audit de la sécurité des TI mené par le BVIE. Étant donné que la sécurité des TI touche à un vaste éventail d'activités, le BVIE prévoit mener d'autres missions liées à la sécurité des TI au cours des prochaines années.

Aperçu de la mission

L'audit portait sur les activités menées entre août 2022 et novembre 2024 et touchant aux domaines d'intérêt suivants :

- la gouvernance de la sécurité des TI (rôles et responsabilités);
- le cadre de politique en matière de sécurité des TI;
- la planification et la mesure du rendement de la sécurité des TI;
- la gestion des risques liés à la sécurité des TI;
- les activités de sensibilisation et de formation des utilisateurs sur la sécurité des TI;
- l'acquisition et le développement de systèmes sécurisés (processus d'évaluation et d'autorisation de sécurité).

Pour en savoir plus sur la portée et la méthode de la mission, consultez l'annexe A.

Résultats

Dans l'ensemble, aucune constatation ne pose de risques importants ou graves pour les activités et les fonds de renseignements du SCT. Cependant, la direction pourrait se concentrer sur quelques domaines.

Domaine d’intérêt	Observations	Incidence	Recommandation
Rôles et responsabilités et cadre de politique	Bien que le Ministère dispose des documents sur le cadre de politique requis, certains documents étaient désuets et ne tenaient pas correctement compte de tous les rôles des personnes clés, comme le représentant désigné pour la cybersécurité. Malgré les documents ministériels désuets, les personnes clés comprenaient leurs rôles et responsabilités en ce qui concerne les instruments de politique pangouvernementaux.	Il existe un risque : • que les responsabilités présentent des lacunes et que les personnes clés soient incapables de remplir adéquatement leur mandat, ou qu’elles n’assument pas leurs rôles et responsabilités de manière uniforme; • que les employés ne connaissent pas et ne comprennent pas leurs rôles et responsabilités.	On recommande à la secrétaire adjointe, Secteur des services ministériels, et dirigeante principale des finances d’examiner et de mettre à jour, au besoin : • les documents ministériels sur le cadre de politique en matière de sécurité des TI; • les documents relatifs au processus d’évaluation et d’autorisation de sécurité. Cette mesure vise à garantir que les documents sont complets et cadrent avec les instruments de politique pangouvernementaux ou le cycle de vie de développement des systèmes du Ministère.

Domaine d’intérêt	Observations	Incidence	Recommandation
Processus d’évaluation et d’autorisation de sécurité *	Bien que le Ministère ait consigné le processus, il n’a pas expliqué clairement comment ce processus cadre avec le cycle de vie du développement des systèmes du Ministère. De plus, certains documents étaient désuets et ne tenaient pas compte de tous les rôles des personnes clés dans ce processus.	Il existe un risque : • que les responsabilités présentent des lacunes et que les personnes clés soient incapables de remplir adéquatement leur mandat, ou qu’elles n’assument pas leurs rôles et responsabilités de manière uniforme; • que les employés ne connaissent pas et ne comprennent pas leurs rôles et responsabilités.	On recommande à la secrétaire adjointe, Secteur des services ministériels, et dirigeante principale des finances d’examiner et de mettre à jour, au besoin : • les documents ministériels sur le cadre de politique en matière de sécurité des TI; • les documents relatifs au processus d’évaluation et d’autorisation de sécurité. Cette mesure vise à garantir que les documents sont complets et cadrent avec les instruments de politique pangouvernementaux ou le cycle de vie de développement des systèmes du Ministère.

Domaine d’intérêt	Observations	Incidence	Recommandation
*	Évaluation et autorisation de sécurité : processus d’évaluation et d’autorisation de sécurité des TI. Processus visant à établir et à maintenir la confiance envers la sécurité des systèmes d’information que le ministère utilise ou gère, tout en tenant compte des exigences des intervenants en matière de sécurité. Annexe B : Procédures obligatoires relatives aux mesures de sécurité de la technologie de l’information (Directive sur la gestion de la sécurité) (B.2.6).		

De plus, la direction pourrait se concentrer sur certains domaines pour gagner en efficacité.

Domaine d’intérêt	Observations	Incidence	Considération
Gouvernance	Bien qu’il n’y ait pas d’exigence de politiques, il est recommandé d’avoir des discussions régulières sur la sécurité des TI avec la haute direction. Il n’y a pas de comité de gestion ministériel désigné pour discuter périodiquement des questions liées à la sécurité des TI (comme les risques, les enjeux, les priorités). Il a été souligné que les questions liées à la sécurité des TI sont présentées et discutées de façon ponctuelle lors des réunions du comité de la haute direction.	En l’absence de discussions régulières avec la haute direction concernant la sécurité des TI, il est possible que l’ordre de priorité des activités ne soit pas correctement établi, que les ministères ne connaissent pas suffisamment les risques et les mesures d’atténuation devant être mises en œuvre, et qu’il n’y ait pas assez de renseignements pour la prise de décisions.	La direction pourrait envisager de nommer un comité ministériel à titre de tribune où les personnes clés, comme le dirigeant principal de l’information ou le représentant désigné pour la cybersécurité, pourraient : • fournir régulièrement de l’information à la haute direction sur les questions liées à la sécurité des TI; • au besoin, solliciter des commentaires qui les aideront à s’acquitter de leurs responsabilités, soit assurer le leadership stratégique, la coordination et la surveillance en matière de sécurité des TI à l’échelle du Ministère.

Domaine d’intérêt	Observations	Incidence	Considération
Processus d’évaluation et d’autorisation de sécurité	Bien que le Ministère ait un répertoire d’applications qu’il tient à jour, la façon dont les renseignements sont saisis et organisés n’est pas propice à la surveillance des résultats du processus d’évaluation et d’autorisation de sécurité ni au suivi des mesures correctives prises en raison des vulnérabilités persistantes.	Il existe un risque que les principales vulnérabilités ne soient pas corrigées en temps opportun. De plus, la direction pourrait miner sa capacité à planifier efficacement les activités futures, à surveiller les tendances ou à cerner les vulnérabilités potentielles à l’échelle du Ministère.	La direction pourrait envisager d’examiner la façon dont les renseignements sont organisés dans le répertoire d’applications pour veiller à ce que les renseignements clés nécessaires à la surveillance et à la prise de décisions puissent être facilement récupérés.

Pour les résultats des autres domaines évalués durant l’audit, consultez l’annexe B.

Pour le plan d’action et la réponse de la direction, consultez l’annexe C.

Annexe A – À propos de la mission

▶ Dans cette section

Pouvoir

La mission d’audit a été définie dans le plan intégré d’audit et d’évaluation 2021-2022 du SCT approuvé.

Énoncé de conformité

Cette mission d'audit a été menée conformément aux Normes internationales pour la pratique professionnelle de l'audit interne [3].

Objectif et portée

L'objectif de l'audit était d'évaluer l'efficacité, la pertinence et la conformité des activités liées à la sécurité des TI du SCT afin de cerner, de gérer et d'atténuer les vulnérabilités et les menaces.

La phase 1 se concentrait sur l'évaluation de l'efficacité du SCT :

- gouvernance de la sécurité des TI (rôles et responsabilités);
- cadre de politique en matière de sécurité des TI;
- planification et mesure du rendement de la sécurité des TI;
- gestion des risques liés à la sécurité des TI;
- activités de sensibilisation et de formation des utilisateurs sur la sécurité des TI;
- acquisition et développement de systèmes sécurisés (processus d'évaluation et d'autorisation de sécurité).

La portée ci-dessus de l'audit était fondée sur les résultats d'une évaluation des risques [4] et tenait compte de travaux effectués par d'autres fournisseurs de services consultatifs et de services d'assurance afin d'éviter les recoupements.

L'audit portait sur les activités liées à la sécurité des TI du SCT pertinentes menées entre août 2022 et novembre 2024.

La portée de l'audit ne comprenait pas :

- un examen des systèmes de planification des ressources organisationnelles du SCT [5];
- les contrôles qui se trouvent en dehors du domaine de responsabilité du SCT, y compris les contrôles exécutés par Services partagés Canada.

Méthode

L’approche et la méthode de l’audit étaient fondées sur les risques et étaient conformes aux Normes internationales pour la pratique professionnelle de l’audit interne. Les méthodes employées dans le cadre de la mission comprenaient :

- l’examen des instruments de politique et des procédures applicables du Conseil du Trésor et du Ministère relativement à la gestion et à l’administration de la fonction de sécurité des TI;
- l’examen des documents clés (par exemple, documents de gouvernance, cadre de politique en matière de sécurité des TI, stratégie de sécurité des TI, procédures opérationnelles normalisées, formation, campagnes de sensibilisation);
- des entrevues avec des partenaires clés du personnel de la Direction de la gestion de l’information et de la technologie;
- le passage en revue des processus (par exemple, structure de gouvernance, cadre de politique, processus d’évaluation et d’autorisation de sécurité);
- la mise à l’essai des contrôles (par exemple, processus d’évaluation et d’autorisation de sécurité).

Annexe B – Secteurs d’intérêt, critères d’audit connexes et résultats globaux

Secteur d’intérêt 1 – Un cadre détaillant adéquatement les exigences requises relativement aux responsabilités, aux politiques, à la planification et à la reddition de compte est en place pour garantir l’atténuation des risques liés à la sécurité des TI.

Critère	Résultats	Recommandation/considération
1.1 Gouvernance, rôles et responsabilités. Un cadre de gouvernance pour la sécurité des TI a été mis en place. Il comprend la définition des rôles et des responsabilités, la planification et la surveillance des investissements et la gestion des relations avec les tiers afin d'assurer la détermination et l'atténuation des risques liés à la sécurité des TI.	• Problème mineur dans le domaine cerné – documents de politique désuets • Possibilité d'assurer une surveillance supplémentaire selon les bonnes pratiques	• Recommandation 1 • Considération 1
1.2 Cadre de politique. Le cadre de politique en matière de sécurité des TI garantit que les contrôles de sécurité des TI requis sont mis en œuvre de manière uniforme et dûment communiqués.	• Problème mineur dans le domaine cerné – documents de politique désuets	• Recommandation 1

Critère	Résultats	Recommandation/considération
1.3 Planification et mesure du rendement. Il existe un plan de sécurité des TI complet et axé sur les risques qui comprend la surveillance du rendement et la gestion des vulnérabilités.	• Aucun problème constaté	• Aucune
1.4 Gestion des risques. Il existe un processus permettant de cerner, d'évaluer et d'atténuer de manière proactive les risques liés à la sécurité des TI.	• Aucun problème constaté	• Aucune
1.5 Sensibilisation et formation. Des activités de formation et de sensibilisation à la sécurité des TI cadrant avec la politique et adaptées à différents utilisateurs sont offertes.	• Aucun problème constaté	• Aucune

Secteur d'intérêt 2 – Le SCT a mis en œuvre des processus et des contrôles pour atténuer les risques en matière de sécurité des TI liés à l'acquisition et au développement de systèmes.

Critère	Résultats	Recommandation/considération
2.1 Processus d'évaluation et d'autorisation de sécurité. Il existe un processus pour cerner et atténuer en temps opportun les risques et les vulnérabilités en matière de sécurité des TI, le cas échéant.	• Problème mineur relevé dans le domaine – documents de procédure désuets • Possibilité d'améliorer la consignation des renseignements dans le cadre du répertoire	• Recommandation 1 • Considération 2

Annexe C – Plan d'action de la direction

▶ Dans cette section

À l'appui de l'examen et de la mise à jour des principaux documents liés à la sécurité des TI, la direction devait préparer une réponse et un plan d'action pour donner suite à la recommandation formulée.

Les éléments sur lesquels la direction peut se concentrer sont des points à prendre en compte dans la prise de décisions. Ils ne seront pas inclus dans le processus de suivi du BVIE. Par conséquent, aucune réponse de la direction ni aucun plan d'action n'ont été demandés.

Recommandation

On recommande à la secrétaire adjointe, Secteur des services ministériels, et dirigeante principale des finances d'examiner et de mettre à jour, au besoin :

- les documents ministériels sur le cadre de politique en matière de sécurité des TI;
- les documents relatifs au processus d'évaluation et d'autorisation de sécurité.

Cette mesure vise à garantir que les documents sont complets et cadrent avec les instruments de politique pangouvernementaux ou le cycle de vie de développement des systèmes du Ministère.

Réponse de la direction

Nous sommes d'accord avec la recommandation.

Mesures proposées pour la recommandation	Date de début	Date d'achèvement cible	Entité responsable
1. Mettre à jour les documents sur le cadre de politique en matière de sécurité des TI	Juin 2025	Septembre 2025	Gestionnaire de la Sécurité des TI
2. Mettre à jour les documents relatifs au processus d'évaluation et d'autorisation de sécurité	Juin 2025	Septembre 2025	Conseiller technique en évaluation et autorisation de sécurité

Considération à l'intention de la direction

Nous reconnaissons les avantages à nommer un comité de gouvernance à titre de tribune pour discuter des questions relatives à la sécurité des TI. Bien qu'il ne s'agisse pas d'une exigence, nous avons créé un plan d'action afin que la direction se penche sur le point suivant.

La direction pourrait envisager de nommer un comité ministériel à titre de tribune où les personnes clés, comme le dirigeant principal de l'information ou le représentant désigné pour la cybersécurité, pourraient :

- fournir régulièrement de l'information à la haute direction sur les questions liées à la sécurité des TI;
- au besoin, solliciter des commentaires qui les aideront à s'acquitter de leurs responsabilités, soit assurer le leadership stratégique, la coordination et la surveillance en matière de sécurité des TI à l'échelle du Ministère.

Réponse de la direction

Nous sommes d’accord avec la considération.

Mesures proposées pour la considération	Date de début	Date d’achèvement cible	Entité responsable
1. Créer un comité de TI au sein du SCT. a. L’un des mandats de ce comité sera de superviser la reddition de compte relativement à la sécurité des TI. b. Ce comité relèvera du Comité d’investissement et de ressources humaines au sein de la structure de gouvernance des comités du SCT et présentera des mises à jour au moins tous les trimestres.	Juillet 2025	Septembre 2025	Dirigeant principal de l’information

---

1 Stratégie intégrée de cybersécurité du GC

2 Bien que la cybersécurité soit considérée comme un sous-ensemble de la sécurité des TI, aux fins du présent rapport, la sécurité des TI et la cybersécurité sont utilisées de manière interchangeable.

3 La mission a été lancée et menée conformément à l’ancien Cadre international des pratiques professionnelles (normes en vigueur avant janvier 2025). Le présent rapport a donc été rédigé en suivant ces normes.

4 Une évaluation exhaustive des risques a été menée dans tous les domaines relatifs à la sécurité des TI conformément au cadre de cybersécurité du National Institute of Standards and Technology (NIST).

5 Les contrôles de TI des systèmes de planification des ressources organisationnelles font l’objet d’un audit chaque année et sont examinés de manière périodique dans le contexte du Cadre du contrôle interne de la gestion financière.

ISBN : 978-0-660-79019-0

Date de modification : 2025-10-03

xx
yy