AUDIT DE LA CYBERSÉCURITÉ

Division de l’audit interne et de l’évaluation

Décembre 2025

Public Prosecution Service of Canada
Service des poursuites pénales du Canada

Canada

Sur la recommandation du Comité ministériel d'audit, soumis à l'approbation du directeur des poursuites pénales le 11 décembre 2025.
Approuvé par le directeur des poursuites pénales le 22 décembre 2025.

This publication is also available in English.

Cette publication est disponible en format HTML sur le site Web http://www.ppsc-sppc.gc.ca/fra/

No de catalogue: J79-39/2026F-PDF

ISBN: 978-0-660-97849-9

TABLE DES MATIÈRES

SOMMAIRE

Contexte

Pour les ministères du gouvernement du Canada (GC), la cybersécurité est une responsabilité partagée entre Services partagés Canada (SPC), le Centre de la sécurité des télécommunications Canada (CST) et le Conseil du Trésor (CT) du Canada. Le Service des poursuites pénales du Canada (SPPC) compte également sur le ministère de la Justice du Canada (Justice Canada) pour gérer, dans le cadre d'un protocole d'entente, plusieurs de ses services de sécurité de la technologie de l'information, ses applications, ses services de développement de bases de données et ses services d'accès à distance.

Le Plan de sécurité stratégique 2021-2024 du SPPC visait, en partie, à demander aux Opérations de la TI et aux Services de sécurité de renforcer leurs capacités en matière de sécurité de la TI face à l'augmentation des cybermenaces, notamment en rapatriant les Services de sécurité de la TI de Justice Canada et en créant un service de sécurité de la TI qui satisfait aux exigences applicables.

Objectifs

Les objectifs de l'audit étaient les suivants :

a. veiller à ce que des processus de gouvernance et de gestion des risques en matière de sécurité de la TI soient en place et répondent aux exigences du cadre stratégique du GC;

b. veiller à ce que les employés du SPPC soient formés et connaissent les mesures de cybersécurité.

Conclusion de l'audit

En général, les politiques, procédures et processus du SPPC guident la gestion des activités de cybersécurité au sein de l'organisme, y compris les rôles et responsabilités qui sont définis et alignés avec les rôles du personnel interne et des partenaires externes. Il conviendrait d'apporter des améliorations afin de garantir que les inventaires de systèmes et de dispositifs soient exhaustifs et contiennent de l'information pouvant avoir une incidence sur les objectifs opérationnels.

[CAVIARDÉ].

Bien que l'organisme dispose d'éléments de sensibilisation et de formation en matière de sécurité, des lacunes subsistent qui peuvent nuire au développement de la culture de sensibilisation à la sécurité du SPPC. Parmi celles-ci, on compte, les faibles taux d'achèvement de la formation obligatoire à l'échelle de l'organisme et de la formation adaptée aux rôles et aux responsabilités du personnel responsable de la sécurité et des opérations de la TI. Il pourrait être avantageux d'offrir de la formation adaptée afin d'assurer la mobilisation, le maintien en poste et le perfectionnement des compétences, en particulier étant donné que le personnel de la TI en est encore à perfectionner ses capacités.

Sommaire des recommandations

1. Le directeur général principal, Services ministériels, doit s'assurer que le plan de sécurité organisationnel 2025-2028 soit rapidement mis au point, approuvé, puis rendu accessible aux employés du SPPC. Il conviendra d'évaluer régulièrement les progrès réalisés par rapport au Plan.
2. Le directeur général principal, Services ministériels, doit s'assurer que les inventaires de systèmes et de dispositifs soient exhaustifs et régulièrement tenus à jour. Il faudra envisager de garantir que les inventaires contiennent les informations pouvant avoir une incidence sur les objectifs opérationnels, comme la gestion du cycle de vie des dispositifs.
3. Le directeur général principal, Services ministériels, doit élaborer, consigner et mettre en œuvre une approche et un plan détaillés en matière de gestion des risques liés à la sécurité de la TI, conforme à la ligne directrice du Centre canadien pour la cybersécurité (CCC) La gestion des risques liés à la sécurité des TI: Une méthode axé sur le cycle de vie (ITSG-33) et qui rend compte :
    - des processus visant à recenser et à consigner les risques de cybersécurité à l'échelle de l'organisme;
    - de la tolérance aux risques, des responsables des risque et des structures de pouvoirs en matière de gestion de ces risques;
    - de la méthodologie pour l' ~~d~~'évaluation des risques (p. ex., probabilité, gravité et impact).
4. Le directeur général principal, Services ministériels, en collaboration avec les Ressources humaines, doit mettre en place et maintenir un mécanisme exhaustif afin de surveiller efficacement les exigences en matière de formation obligatoire sur la cybersécurité et d'en garantir la réalisation en temps opportun.

CONSTATATIONS ET RECOMMANDATIONS

Gouvernance

Politiques, procédures et processus pour la gestion de la cybersécurité au SPPC

Nos attentes

Nous nous attendions à ce que des structures et processus soient en place pour éclairer, orienter et surveiller les activités du SPPC, qui guident la gestion des risques de cybersécurité.

En général, les politiques, procédures et processus du SPPC orientent la gestion des activités de cybersécurité au sein de l'organisme, y compris les rôles et responsabilités qui sont définis et alignés avec les rôles du personnel interne et des partenaires externes. L'équipe responsable de la sécurité de la TI au SPPC se sert généralement de la ligne directrice ITSG-33 du CCC comme guide, qui décrit les principales activités de gestion des risques liés à la sécurité des TI devant être exercées au niveau organisationnel et au niveau des systèmes d'information au sein des organisations du GC.

Il existe un processus établi de gestion de l'identification et de l'authentification qui permet d'identifier et d'authentifier d'une manière particulière les utilisateurs, y compris plusieurs procédures de surveillance des comptes appliquées par le personnel de la sécurité de la TI. Des processus sont en place afin de garantir que les utilisateurs ayant des droits d'accès sont informés, autorisés et soumis à une vérification de sécurité et qu'ils bénéficient d'une séparation adéquate des tâches.

Les rôles et responsabilités, y compris ceux du dirigeant principal de l'information (DPI), du dirigeant principal de la sécurité (DPS) et de l'agent désigné pour la cybersécurité, sont consignés dans les descriptions de poste et les documents internes, notamment le guide opérationnel de la cybersécurité du SPPC, la directive du SPPC sur la gestion des privilèges d'administrateur et le plan de gestion des événements de cybersécurité (PGEC). Un examen des utilisateurs et des groupes affectés aux rôles d'administrateurs a généralement montré une séparation adéquate des tâches. La direction a été informée des lacunes repérées.

Au moment de l'audit, le plan de sécurité organisationnel (PSO) 2025-2028 était encore à l'état d'ébauche, faisant l'objet d'un examen approfondi, et n'avait pas été approuvé par le directeur général (DG) des Services de l'administration et DPI ni par l'administrateur général. Le PSO précédent est venu à échéance. La version provisoire du plan est conforme aux exigences de la Politique sur la sécurité du gouvernement du CT. Or, faute d'un PSO approuvé, l'organisme pourrait ne pas être en mesure de finaliser et de mettre en œuvre son plan stratégique, ce qui pourrait entraîner des perturbations et/ou des inefficacités opérationnelles.

Recommandation

1. Le directeur général principal, Services ministériels, doit s'assurer que le plan de sécurité organisationnel 2025-2028 soit rapidement mis au point, approuvé, puis rendu accessible aux employés du SPPC. Il conviendra d'évaluer régulièrement les progrès réalisés par rapport au plan.

CONSTATATIONS ET RECOMMANDATIONS

Pourquoi c'est important

En général, les politiques, procédures et processus du SPPC orientent la gestion des activités de cybersécurité au sein de l'organisme, y compris les rôles et responsabilités qui sont définis et consignés.

Des améliorations peuvent être apportées afin de garantir l'exhaustivité de l'information relative aux dispositifs physiques et aux systèmes d'information. [CAVIARDÉ].

Enfin, des améliorations peuvent être apportées pour veiller à ce que les utilisateurs qui occupent des rôles assortis de droits d'accès soient visés par une séparation adéquate des tâches, notamment en veillant à ce qu'un employé ne puisse pas à la fois modifier et évaluer les fonctions de sécurité de Microsoft 365.

Plans d'intervention et de rétablissement

Des contrôles de sécurité, comme la gestion de l'identification et de l'authentification, sont définis, consignés et mis en œuvre pour satisfaire aux exigences organisationnelles en matière de sécurité de la TI et en conformité avec les exigences du CT. Cependant, le Plan de continuité des activités (PCA) n'est pas actualisé, étant donné qu'il a été mis à jour pour la dernière fois en mai 2019, soit avant l'apport de changements importants liés au télétravail en raison de la pandémie de Covid-19 et de la mise en œuvre du modèle de travail hybride du gouvernement du Canada. Par ailleurs, bien que la version préliminaire du PSO 2025-2028 prévoit la réalisation d'une évaluation des répercussions sur les activités et d'une révision des plans de continuité des activités de l'organisme, le travail n'a pas été complété.

Le PGEC a été approuvé en juillet 2024 et décrit les activités d'intervention en cas d'incidents du SPPC et fournit des directives aux équipes du SPPC responsables de la cybersécurité et de la TI en cas de cyberincident. Néanmoins, ni le PGEC ni le PCA ne prévoient un processus de mise à l'essai et de mise à jour. Le PCA n'a pas été mis à l'essai depuis 2018. [CAVIARDÉ].

Inventaires des systèmes d'information et des dispositifs

Les dispositifs physiques et les systèmes d'information qui permettent au SPPC d'atteindre ses objectifs opérationnels sont généralement répertoriés et gérés. Bien que la ligne directrice ITSG-33 accorde une certaine souplesse aux ministères pour qu'ils déterminent la portée des documents relatifs aux inventaires des systèmes d'information et des dispositifs, il conviendra d'apporter des améliorations de sorte à garantir l'efficacité des inventaires, en réalisant des examens réguliers et en garantissant l'exhaustivité des renseignements recueillis.

Le SPPC a dressé un inventaire des systèmes d'information. On y recense plus de 70 systèmes, exploités par Justice Canada, SPC ou le SPPC, dont 20 systèmes qui sont la propriété technique du SPPC. Cependant, l'inventaire ne contient pas d'information relative à la propriété technique, ce qui peut entraîner un manque de visibilité entravant la prise de décision, compte tenu, notamment, de la complexité des responsabilités liées à la cybersécurité et à la TI au SPPC et chez ses partenaires (p. ex., SPC, Justice Canada). Les lacunes à cet égard ont été corrigées à la suite d'une demande présentée par l'équipe de l'audit interne, qui a donné lieu à la mise à jour de l'inventaire, qui contient maintenant de l'information précise quant à la propriété technique des 70 systèmes. L'examen et la mise à jour réguliers de l'inventaire des systèmes, y compris les renseignements sur la propriété technique, peuvent contribuer à assurer une meilleure visibilité en ce qui concerne la propriété technique, à l'interne et au sein des organismes qui fournissent des services de TI au SPPC (p. ex., SPC, Justice Canada).

Si les dispositifs physiques sont répertoriés, le SPPC peut apporter des améliorations à ses inventaires en veillant à ce que l'information soit exhaustive et en envisageant d'y inclure des renseignements, comme les numéros de série des ordinateurs et l'état du cycle de vie des dispositifs et systèmes. Le manque d'information sur les dispositifs peut avoir une incidence sur la rapidité et l'exactitude de la prise de décisions et entraîner un risque accru d'incidence opérationnelle sur le SPPC.

Recommandation

2. Le directeur général principal, Services ministériels, doit s'assurer que les inventaires de systèmes et de dispositifs soient exhaustifs et régulièrement tenus à jour. Il faut envisager de garantir que les inventaires contiennent les informations pouvant avoir une incidence sur les objectifs opérationnels, comme la gestion du cycle de vie des dispositifs.

CONSTATATIONS ET RECOMMANDATIONS

Gestion et évaluation du risque

Nos attentes

Nous nous attendions à ce que le SPPC comprenne les risques en matière de cybersécurité liés aux activités, aux biens et aux personnes. En outre, nous avions prévu que le SPPC ait établi ses priorités, contraintes, tolérances au risque et hypothèses et qu'il s'en serve pour étayer ses décisions en matière de risque opérationnel.

En général, la gestion des risques de cybersécurité au SPPC en est encore à un stade immature. Même si les responsables de la sécurité de la TI s'efforcent d'élaborer un cadre de gouvernance et de gestion du risque, aucun calendrier n'a encore été établi relativement à la mise en œuvre.

La Politique sur la sécurité du gouvernement exige la mise en place d'une gouvernance des risques liés à la sécurité, y compris les responsabilités en matière de contrôles de sécurité et les pouvoirs décisionnels relatifs à la gestion des risques liés à la sécurité. [CAVIARDÉ]. [CAVIARDÉ]. La détermination et la consignation des rôles et responsabilités en matière de gestion des risques, y compris la détermination de la tolérance aux risques, peuvent contribuer à préciser les responsabilités dans la fourniture de ces directives.

[CAVIARDÉ]. La ligne directrice ITSG-33 est utilisée à des fins de référence, mais certains éléments clés, comme l'élaboration et la mise en œuvre de contrôles de sécurité, la consignation d'un registre de risques globaux et la schématisation des processus conformément à la ligne directrice, en sont encore à leurs débuts. Ces activités sont considérées comme étant des initiatives à long terme, visées par des échéanciers de plus d'un an, principalement en raison des contraintes en matière de ressources (1,5 employé affecté à la tâche) et des priorités changeantes.

CONCLUSIONS ET RECOMMANDATIONS

Gestion et évaluation des risques

Pourquoi c'est important

[CAVIARDÉ].

[CAVIARDÉ]. Cela pourrait donner lieu à la révision de l'autorisation d'exploitation valide du système.

Même si elles sont souvent désignées à un niveau élevé, les menaces, les vulnérabilités, les répercussions et la suffisance des contrôles sont prises en considération et consignées afin de déterminer le niveau de risque dans le cadre du processus d'évaluation et autorisation de la sécurité (EAS). Des améliorations peuvent être apportées afin de mieux consigner les éléments des évaluations de risque (p. ex., énoncé des répercussions, caractère suffisant des contrôles, probabilités, méthodologie de classification des risques).

Les recommandations, interventions et mesures d'atténuation relatives aux risques résiduels recensés dans le cadre du processus d'EAS sont consignées dans un plan d'action et jalons pour obtenir l'autorisation d'exploitation du système. Cette dernière est accordée dans l'espoir que les risques résiduels seront atténués de façon adéquate. Certains éléments ont été mis en place, mais d'importantes contraintes en matière de ressources, ainsi que les priorités changeantes, ont empêché la mise en œuvre de plusieurs recommandations et mesures d'atténuation dans les délais prévus.

[CAVIARDÉ].

Recommandation

3. Le directeur général principal, Services ministériels, doit élaborer, consigner et mettre en œuvre une approche et un plan détaillés en matière de gestion des risques liés à la sécurité de la TI, conforme à la ligne directrice ITSG-33 du CCC, et qui rend compte :

- des processus visant à recenser et à consigner les risques de cybersécurité à l'échelle de l'organisme;
- de la tolérance aux risques, des responsables des risque et des structures de pouvoirs en matière de gestion de ces risques;
- de la méthodologie pour l'évaluation des risques (p. ex., probabilité, gravité et impact).

Formation et sensibilisation

Nos attentes

Nous nous attendions à ce que le SPPC possède une culture de sensibilisation à la sécurité reposant sur des éléments de sensibilisation et de formation adaptés, régulièrement examinés, actualisés et mis à la disposition de tous les utilisateurs ayant accès aux systèmes ministériels.

Pourquoi c'est important

Bien que l'organisme dispose d'éléments de sensibilisation et de formation en matière de sécurité, des lacunes subsistent qui peuvent nuire au développement de la culture de sensibilisation à la sécurité du SPPC. Parmi celles-ci, on compte, notamment, les faibles taux d'achèvement de la formation obligatoire à l'échelle de l'organisme et de la formation adaptée aux rôles et aux responsabilités du personnel responsable de la sécurité et des opérations de la TI. Il pourrait être avantageux d'offrir de la formation adaptée afin d'assurer la mobilisation, le maintien en poste et le perfectionnement des compétences, en particulier étant donné que le personnel de la TI en est encore à perfectionner ses capacités.

Le SPPC ne dispose ni d'une politique de sensibilisation et de formation en matière de sécurité ni d'un plan de sensibilisation et de formation en matière de sécurité de la TI. En l'absence d'un programme de sensibilisation et de formation en matière de sécurité de la TI, une formation axée sur les vulnérabilités actuelles liées aux utilisateurs et aux comportements acceptables des utilisateurs est offerte de façon ad-hoc, ainsi que deux cours obligatoires à l'intention de tous les employés.

Les deux cours obligatoires, offerts gratuitement par l'École de la fonction publique du Canada, sont les suivants : « Découvrez la cybersécurité (DDN235) » et « Sensibilisation à la sécurité (COR310). Une analyse des données a permis de constater que les taux d'achèvement enregistrés pour les deux cours sont faibles, soit 52 % et 65 % respectivement.

Le SPPC fournit généralement aux employés de l'information sur la sensibilisation à la sécurité, notamment des conseils sur le moment et la façon de signaler les incidents relatifs à la sécurité. L'information est principalement diffusée au moyen du site Intranet et d'un bulletin interne.

Une campagne contre l'hameçonnage a été menée par l'équipe de la TI du SPPC en mai 2025. Or, les priorités changeantes ont entraîné des retards dans l'analyse des données.

Enfin, nous avons constaté que le processus d'EAS réalisé pour Microsoft 365 a désignée l'absence d'un programme de formation en matière de sensibilisation à la sécurité comme un domaine à risque. En outre, des lacunes en matière de formation ont été cernées pour le personnel chargé de la sécurité et des opérations de la TI à la suite de la prise en charge de nouvelles responsabilités de TI par le SPPC et de l'expérience limitée dans certains domaines. En conséquence, de la formation obligatoire a été mise en place afin de remédier à ces lacunes. Après l'examen des certificats de réussite, nous avons constaté que sur les quatre employés travaillant dans le domaine de la cybersécurité, [CAVIARDÉ].

Recommandation

4. Le directeur général principal, Services ministériels, en collaboration avec les Ressources humaines, doit mettre en place et maintenir un mécanisme exhaustif afin de surveiller efficacement les exigences en matière de formation obligatoire sur la cybersécurité et d'en garantir la satisfaction en temps opportun.

PLANS D'ACTION DE LA DIRECTION

No	Recommandation	Risque	Plan d'action de la direction	Bureau de première responsabilité	Date cible
1	Le directeur général principal, Services ministériels, doit s'assurer que le plan de sécurité organisationnel 2025-2028 soit rapidement mis au point, approuvé, puis rendu accessible aux employés du SPPC. Il conviendra d'évaluer régulièrement les progrès réalisés par rapport au plan.	Modéré	La direction est d'accord avec la recommandation. Le DGP déterminera la méthode d'approbation du plan de sécurité organisationnel, qui sera ensuite présenté aux fins d'approbation. Le plan sera publié sur iNet. Un calendrier sera établi afin de rendre compte des progrès réalisés auprès de l'Équipe de gestion supérieure.	DG, DSA	31 janvier 2026
2	Le directeur général principal, Services ministériels, doit s'assurer que les inventaires de systèmes et de dispositifs soient exhaustifs et régulièrement tenus à jour. Il faudra envisager de garantir que les inventaires contiennent les informations pouvant avoir une incidence sur les objectifs opérationnels, comme la gestion du cycle de vie des dispositifs.	Modéré	La direction est d'accord avec la recommandation. Nous disposons actuellement d'un inventaire pour recenser les ordinateurs portables et les téléphones cellulaires gérés par l'organisme. Nous envisagerons d'ajouter des renseignements supplémentaires au sujet des nouveaux dispositifs. L'ajout de renseignements relatifs aux dispositifs actuels représenterait une charge de travail trop grande pour les ressources dont nous disposons actuellement.	Directeur, TI	31 mars 2026
3	Le directeur général principal, Services ministériels, doit élaborer, consigner et mettre en œuvre une approche et un plan détaillés en matière de gestion des risques liés à la sécurité de la TI, conforme à la ligne directrice ITSG-33 du CCC, et qui rend compte : • des processus visant à recenser et à consigner les risques de cybersécurité à l'échelle de l'organisme; • de la tolérance aux risques, des responsables de risque et des structures de pouvoirs en matière de gestion de ces risques; • de la méthodologie pour l'évaluation des risques (p. ex., probabilité, gravité et impact).	Modéré	La direction est d'accord avec la recommandation. Nous élaborerons une approche et un plan détaillés sur la gestion des risques liés à la sécurité de la TI. Il faudra du temps pour réaliser des progrès à cet égard en raison du manque de ressources.	Directeur, TI	31 mars 2027
4	Le directeur général principal, Services ministériels, en collaboration avec les Ressources humaines, doit mettre en place et maintenir un mécanisme exhaustif afin de surveiller efficacement les exigences en matière de formation obligatoire sur la cybersécurité et d'en garantir la satisfaction en temps opportun.	Modéré	La direction est d'accord avec la recommandation. Les RH collaboreront avec la haute direction dans le but d'ajouter un indicateur dans les ententes de rendement des cadres sur la réussite de leurs employés à la formation obligatoire. En outre, une fois par année, les RH achemineront aux responsables une liste des formations obligatoires que doivent suivre leurs employés.	Directeur, RH	31 juillet 2026

ANNEXE A – RENSEIGNEMENTS SUR L'AUDIT

Énoncée d'assurance

L'Audit a été effectué conformément aux Normes internationales pour la pratique professionnelle de l'audit interne de l'Institut des auditeurs internes, à la politique et à la directive du Conseil du Trésor sur l'audit interne, comme en témoignent les résultats de l'évaluation externe de l'assurance de la qualité.

Portée

L'audit a porté sur les contrôles et processus du SPPC et a exclu les domaines pour lesquels notre fournisseur de services, Justice Canada, est le responsable opérationnel désigné, conformément au protocole d'entente.

Méthodologie

Les activités suivantes s'inscrivent dans le cadre de la méthodologie appliquée :

- entretiens menés auprès de divers intervenants;
- examen et analyse des politiques, pratiques, procédures et directives consignées liées à la cybersécurité.

Domaines d'intérêt

1	Gouvernance
2	Gestion du risque
3	Sensibilisation et formation

ANNEXE B – LISTE DES ACRONYMES/ABRÉVIATIONS

CCC	Centre canadien pour la cybersécurité
CT	Conseil du Trésor du Canada
DPI	Dirigeant principal de l’information
EAS	Évaluation et autorisation de la sécurité
GC	Gouvernement du Canada
ITSG-33	La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie
Justice Canada	Ministère de la Justice du Canada
PCA	Plan de continuité des activités
PGEC	Plan de gestion des événements de cybersécurité
PSO	Plan de sécurité organisationnel
SPPC	Service des poursuites pénales du Canada
SPC	Services partagés Canada
TI	Technologie de l’information