Sécurité publique Canada | Public Safety Canada

Sécurité publique Canada

Audit interne de la sécurité des technologies de l'information

Le 30 avril 2020

Canada

No de Cat: PS4-263/2020F-PDF
ISBN: 978-0-660-35035-6

Table des matières

Sommaire

L'objectif de cet audit était d'évaluer le caractère adéquat et l'efficacité du cadre de contrôle de gestion pour la sécurité des TI[1] à Sécurité publique Canada (SP) ainsi que sa disposition à se conformer à la nouvelle *Politique sur la sécurité du gouvernement* du Conseil du Trésor (CT) et aux autres politiques, directives et normes pertinentes.

Pourquoi est-ce important?

Les ministères du gouvernement du Canada dépendent fortement de différents systèmes et processus informatiques pour remplir leur mandat. Il est donc essentiel de protéger ces systèmes informatiques contre les cybermenaces et les autres menaces afin d'assurer la confidentialité, l'intégrité et la disponibilité des informations qui y sont enregistrées.

Afin d'orienter la gestion des mesures de sécurité gouvernementales pour assurer la prestation fiable des programmes et des services du gouvernement du Canada, une mise à jour complète de l'ensemble des politiques du CT sur la sécurité a été approuvée au printemps 2019. Elle visait à s'assurer que la politique reflète adéquatement l'évolution du contexte opérationnel dynamique et la nécessité d'assurer un leadership stratégique pour la sécurité du gouvernement dans un contexte d'informatique d'entreprise et de prestation de services. Dans l'ensemble, ces mises à jour ont été effectuées afin de renforcer les pratiques de gestion de la sécurité au sein des ministères, avec les partenaires et partout au gouvernement, ainsi que pour assurer un degré de préparation approprié dans un environnement de risque dynamique.

Principales constatations

L'audit a permis de constater les points suivants :

- Sécurité publique Canada a mis en place un cadre de gouvernance à l'appui de la gestion des activités de sécurité informatique. Ce cadre pourrait cependant être amélioré afin de s'assurer que de bonnes pratiques de gestion des risques et une approche plus intégrée de gestion de la sécurité sont utilisées.
- Le Ministère a mis en place des mesures de contrôle afin de gérer les principales activités de sécurité informatique. Ces processus ne sont toutefois pas systématiquement suivis ni contrôlés de manière adéquate, pour assurer une conformité continue et une atténuation proactive des risques.
- Le Ministère a également défini les éléments d'un programme de formation et de sensibilisation à la sécurité informatique. Des améliorations sont cependant

[1] Cadre de contrôle de la sécurité des technologies de l'information : toutes les ressources d'une organisation, y compris les politiques, le personnel, les processus, les pratiques, les contrôles et les technologies, doivent être utilisées afin d'évaluer et d'atténuer les risques et les attaques en matière de sécurité informatique.

nécessaires afin de s'assurer que les employés comprennent mieux leurs responsabilités en matière de protection de la confidentialité, de la disponibilité et de l'intégrité des informations.

Recommandations

Recommandation 1

Le sous-ministre adjoint (SMA), Secteur de la gestion ministérielle (SGM) devrait examiner le cadre de gouvernance actuel afin de s'assurer qu'il soit harmonisé avec les exigences de la nouvelle *Politique sur la sécurité du gouvernement* du Conseil du Trésor et d'améliorer la prise de décisions stratégiques en matière de sécurité des technologies de l'information, en particulier :

- veiller à l'intégration systématique de la sécurité des TI au processus ministériel de gestion des risques liés à la sécurité;
- clarifier les rôles et les responsabilités des personnes et des organes de gouvernance en ce qui concerne la gestion des activités de sécurité des TI;
- veiller à ce que les instruments de politique internes, y compris les politiques, procédures et lignes directrices, soient mis à jour, approuvés, communiqués et révisés régulièrement afin d'en assurer la pertinence continue.

Recommandation 2

Le SMA du SGM devrait, en adoptant une approche fondée sur les risques, effectuer des examens et une surveillance continue des activités clés suivantes en matière de sécurité des TI, afin de s'assurer qu'elles respectent les processus établis pour la protection des informations ministérielles de nature délicate :

- gestion de l'accès aux systèmes informatiques;
- processus permettant de déterminer, d'évaluer et de signaler les incidents de sécurité informatique;
- prévention et gestion de toute perte de données, de tout dommage aux données ou de toute compromission des données de l'organisation;
- considérations liées à la sécurité dans le cycle de vie de l'élaboration des systèmes.

Recommandation 3

Le SMA du SGM devrait veiller à ce qu'un programme de sensibilisation et de formation soit élaboré pour la sécurité informatique et à ce qu'il soit mis en œuvre pour couvrir de manière exhaustive les risques liés à la sécurité informatique et faire en sorte que les

employés conservent les connaissances requises pour pouvoir s’acquitter de leurs responsabilités.

Conclusion

Des améliorations sont nécessaires pour que Sécurité publique Canada puisse établir un cadre de contrôle des activités de sécurité informatique qui soit bien défini et pleinement efficace, en plus d’être conforme à la *Politique sur la sécurité du gouvernement* révisée du Conseil du Trésor, ainsi qu’aux autres politiques, directives et normes pertinentes. Plus précisément, Sécurité publique Canada devra faire des efforts importants pour documenter, communiquer et assurer la conformité avec les pratiques de contrôle de la sécurité informatique exigées par le Conseil du Trésor et assurer leur application.

1 Introduction

1.1 Contexte

Les ministères du gouvernement du Canada dépendent fortement de différents systèmes et processus de technologie de l'information (TI) pour remplir leur mandat. Il est donc essentiel de protéger ces systèmes informatiques contre les cybermenaces et les autres menaces afin d'assurer la confidentialité, l'intégrité et la disponibilité des informations qui y sont enregistrées.

Services partagés Canada (SPC) est responsable de sécuriser l'infrastructure informatique sous-jacente sur laquelle s'appuient les systèmes informatiques de plus de 40 organisations gouvernementales. Les ministères, y compris Sécurité publique Canada (SP), sont responsables de la mise en œuvre de mesures de contrôle de sécurité afin de répondre aux exigences ministérielles en matière de sécurité informatique, conformément aux pratiques ministérielles. Bien que SPC doit gérer et sécuriser l'infrastructure de SP, SP doit gérer et sécuriser ses propres applications, données et dispositifs de bureau utilisés afin de maintenir l'intégrité des informations au sein de ses systèmes informatiques.

Afin d'orienter la gestion des mesures de sécurité gouvernementale pour assurer la prestation fiable de programmes et de services, une mise à jour complète de l'ensemble des politiques du Conseil du Trésor (CT) sur la sécurité a été approuvée au printemps 2019. La *Politique sur la sécurité du gouvernement* du CT, ainsi que les directives et normes connexes sont entrées en vigueur en juillet 2019, alors que la *Politique sur les services et le numérique* entrera en vigueur en avril 2020. Ces politiques remplaceront la précédente *Politique sur la sécurité du gouvernement* de 2009, la *Directive sur la gestion de la sécurité ministérielle* de 2009, ainsi que de nombreuses normes opérationnelles du CT sur la sécurité, comme la Gestion de la sécurité des technologies de l'information (GSTI).

La politique a été mise à jour pour refléter adéquatement l'évolution du contexte opérationnel dynamique et la nécessité d'assurer un leadership stratégique pour la sécurité du gouvernement dans un contexte d'informatique d'entreprise et de prestation de services. Dans l'ensemble, ces mises à jour ont été effectuées afin de renforcer globalement les pratiques de gestion de la sécurité au sein des ministères, avec les partenaires et partout au gouvernement, ainsi que pour assurer un degré de préparation approprié dans un environnement de risque dynamique.

Les politiques et les directives connexes ont également été mises à jour aux fins suivantes :

- rationaliser les instruments et les règles;

- renforcer la gouvernance par la nomination obligatoire d'un chef de la sécurité (CS);
- préciser les rôles et les responsabilités des principaux organismes chargés de la sécurité (dont Sécurité publique Canada) et des organisations de services internes intégrés[2] (par exemple, Services partagés Canada);
- renforcer le milieu et la culture par la création de nouvelles formations, ainsi que de nouvelles orientations et de nouveaux outils sur la sécurité afin de normaliser et de moderniser les pratiques organisationnelles.

La nomination d'un CS remplace l'exigence relative à la désignation d'un agent de sécurité du Ministère (ASM) présente dans la politique antérieure, et vise à donner un rôle plus stratégique à cette fonction. Le rôle du CS consiste donc à assurer le leadership, la coordination et la surveillance des activités de gestion de la sécurité ministérielle et se veut un complément à l'expertise et au leadership opérationnels au sein du Ministère. On s'attend à ce que les CS travaillent avec leurs partenaires pour assurer une gestion efficace de la sécurité. Le sous-ministre de SP a nommé le sous-ministre adjoint du Secteur de la gestion ministérielle et dirigeant principal des finances comme nouveau CS le 17 octobre 2019.

En vertu de la politique révisée, les administrateurs généraux sont également chargés de désigner les « hauts fonctionnaires » qui auront la responsabilité globale pour les aspects de sécurité d'un programme, d'un service ou d'un secteur d'activités ou pour une fonction de sécurité. Les hauts fonctionnaires peuvent inclure les responsables de programmes, le dirigeant principal des finances, le dirigeant principal de l'audit, le dirigeant principal de l'information, le chef de la protection des renseignements personnels et les divers fonctionnaires désignés en vertu d'une obligation légale. SP revoit actuellement sa structure de gouvernance pour y inclure la nouvelle fonction de CS et respecter les exigences de la politique du CT, ce qui inclut la désignation des hauts fonctionnaires, ainsi que leurs rôles et responsabilités correspondants.

1.2 Objectif et portée de l'audit

L'objectif de cet audit était d'évaluer le caractère adéquat et l'efficacité du cadre de contrôle de gestion pour la sécurité des TI[3] à SP ainsi que sa disposition à se

[2] Conformément à la *Politique sur la sécurité du gouvernement* de 2019, une organisation de services internes intégrés se définit comme tout « ministère ou organisme qui fournit des services internes intégrés à d'autres ministères du gouvernement du Canada. Ceci comprend les principaux organismes chargés de la sécurité qui fournissent des services de sécurité à l'échelle du gouvernement. »

[3] Cadre de contrôle de la sécurité des technologies de l'information : toutes les ressources d'une organisation, y compris les politiques, le personnel, les processus, les pratiques, les contrôles et les technologies, doivent être utilisées afin d'évaluer et d'atténuer les risques et les attaques en matière de sécurité informatique.

conformer à la nouvelle Politique sur la sécurité du gouvernement du CT et aux autres politiques, directives et normes pertinentes.

Cet audit portait sur les activités des TI au Ministère pendant la période allant du 1er avril 2018 au 30 septembre 2019, mais comprenait également un examen de documents pertinents produits avant cette période. L'audit concernait seulement les activités relatives à la sécurité des TI qui incombent à SP et qui sont reliées au réseau ministériel.

Elle excluait cependant les éléments suivants :

- l'équipement de sécurité des télécommunications (pièces d'équipement de cryptographie), l'infrastructure secrète du gouvernement du Canada (ISGC) et le réseau canadien Très secret puisqu'ils sont soumis à une vérification ou à un examen externe périodique;
- l'infrastructure et les services informatiques fournis par SPC ou d'autres prestataires de services tiers; certaines communications entre SP et d'autres ministères ont également été examinées, mais aucun examen direct n'a été effectué.

1.3 Méthodologie et approche de l'audit

Pour chaque critère établi, une méthode d'audit a été élaborée afin d'examiner adéquatement le secteur en fonction de l'objectif. Les termes « méthodologie » et « approche » font référence au travail servant à recueillir et à analyser des renseignements dans le but d'atteindre les objectifs de l'audit. Ce travail a permis de rassembler les éléments de preuve appropriés et en quantité suffisante pour que l'équipe d'audit puisse tirer des conclusions pour chaque objectif de l'audit.

Pour effectuer cet audit, les méthodologies suivantes ont été utilisées :

- entrevues sur la gestion de la sécurité des TI et les activités connexes auprès des employés;
- examen des instruments de politiques et des procédures applicables du Conseil du Trésor et du Ministère à l'égard de la gestion et de l'administration de la sécurité des TI;
- examen des documents connexes, y compris les comptes rendus de décisions des réunions des comités; et,
- revue de processus, tests et examen analytique.

1.4 Conformité aux normes professionnelles

Cet audit est conforme aux Normes internationales pour la pratique professionnelle de l'audit interne de l'Institut des auditeurs internes et à la Politique sur l'audit interne du

Gouvernement du Canada, comme soutenu par les résultats du programme d'assurance et d'amélioration de la qualité.

2 Constatations et recommandations

2.1 Constatation 1 : Sécurité publique Canada a mis en place un cadre de gouvernance à l'appui de la gestion des activités de sécurité informatique. Ce cadre pourrait cependant être amélioré afin de s'assurer que de bonnes pratiques de gestion des risques et une approche plus intégrée de gestion de la sécurité sont utilisées.

Au sein d'un ministère, différents processus et structures adéquats doivent être mis en place pour s'assurer que la haute direction possède suffisamment d'informations fiables pour orienter, diriger, gérer et contrôler les activités en matière de sécurité des TI de l'organisation. Les mécanismes de gouvernance et de surveillance devraient favoriser une prise de décisions fondées sur les risques qui tient également compte de toutes les mesures de contrôle de sécurité prévues dans une approche de gestion intégrée.

Processus de gouvernance et de gestion des risques

Pendant l'audit, l'ASM, le dirigeant principal de l'information (DPI), le directeur, sécurité de la GI/TI / agent de la sécurité de l'information, et le coordonnateur de la sécurité de la technologie de l'information (CSTI) ont travaillé en collaboration pour s'assurer que des mesures de sécurité appropriées étaient appliquées à tous les biens, activités et processus du Ministère.

Le programme de sécurité ministérielle de SP était dirigé par l'ASM, un cadre de la Direction générale des services ministériels. Il devait assurer la coordination de l'ensemble des fonctions sur la sécurité et la mise en œuvre des exigences prévues dans la politique sur la sécurité.

La gestion des ressources informatiques et d'information du Ministère, y compris la responsabilité opérationnelle de la sécurité des TI, était sous la responsabilité de la Direction générale du DPI.

La Direction générale comprend trois divisions :

- Services à la clientèle et applications;
- Gestion de l'information (GI);
- Sécurité de la GI/TI, interopérabilité et gestion du portefeuille.

Quant au CSTI (au sein de la division de la GI/TI et gestion du portefeuille), il était responsable de la gestion et de la coordination globales du programme ministériel de sécurité informatique, de la Directive en matière de sécurité des TI et des questions connexes.

Bien que SP n'avait pas d'organe de gouvernance pour s'occuper uniquement des questions de GI/TI, le Comité gestion ministériel (CGM) et le Comité de gestion des ressources (CGR) étaient les deux principaux organes de gouvernance de haut niveau responsables de soutenir les activités ministérielles de GI/TI, y compris les questions liées à la sécurité. Pendant l'audit, les discussions sur la sécurité de la GI/TI qui ont eu lieu pendant les réunions du CGM et du CGR ont notamment porté sur un aperçu du plan annuel de TI pour 2019-2020 et incluaient la présentation du tableau de bord trimestriel pour la GI/TI dans lequel figuraient des données générales sur les questions de GI/TI. Le DPI a également avisé l'équipe d'audit qu'il rencontrait périodiquement les cadres des différentes sections pour discuter de la GI et d'autres questions portant sur les TI si nécessaire (par exemple, la récente migration vers le système d'exploitation Windows 10).

En raison de l'importance accrue accordée à ce sujet, les personnes interrogées ont indiqué que le temps alloué pendant les réunions du CGM et du CGR est insuffisant pour discuter des questions de sécurité informatique, telles que les incidents de sécurité informatique, l'architecture informatique et les politiques et directives en matière de TI, et établir une orientation stratégique.

Conformément à la *Politique sur la sécurité du gouvernement* de 2019 du CT, l'administrateur général est responsable d'approuver un plan de sécurité ministériel triennal, qui est revu chaque année. Ce plan est un outil essentiel à la disposition des administrateurs généraux pour définir des orientations et des priorités en matière de gestion de la sécurité. Il devrait notamment permettre d'avoir une vue d'ensemble de tous les éléments des contrôles de sécurité et des risques associés afin de définir les stratégies, les buts, les objectifs, les priorités et les échéanciers en vue de l'amélioration de la sécurité au Ministère. Pendant l'audit, l'ASM a dirigé l'élaboration du plan de sécurité.

Le plan de sécurité de SP pour 2017-2020 n'incluait cependant pas les questions de sécurité de la GI/TI. Il était prévu de les inclure dans le plan ministériel de GI/TI pour 2019-2022, élaboré par le DPI.

Même si la Direction générale du DPI est consciente des risques pour la sécurité informatique au Ministère, SP n'utilise actuellement aucun mécanisme officiel pour identifier, analyser et évaluer systématiquement ces risques (en utilisant, par exemple, un registre des risques ou un autre outil similaire). Bien que les activités de sécurité informatique, telles que les interventions lors d'incidents de sécurité informatique, sont effectuées quotidiennement afin de soutenir le mandat de SP, elles sont menées au mieux des possibilités en fonction de la disponibilité des ressources et ne sont pas officiellement documentées, plutôt que d'être planifiées à la suite des résultats d'un processus global de gestion des risques.

Les risques en matière de sécurité des TI sont connus du Ministère, malgré l'absence de mécanisme formel. Il est cependant possible d'améliorer les processus de gestion de ces risques afin de s'assurer que tous les risques importants sont identifiés, enregistrés, étudiés, résolus et signalés en temps utile pour permettre une surveillance et une prise de décisions appropriées. Une incapacité à identifier et gérer efficacement et formellement les risques en matière de sécurité des TI pourrait entrainer une attribution des ressources non conforme aux priorités de gestion et aux principes de tolérance au risque.

Des améliorations aux pratiques ministérielles de gestion des risques en matière de sécurité des TI et de mécanismes de surveillance ont été apportées pendant l'audit. SP a déployé des efforts pour créer un registre des risques de sécurité. La Direction générale du DPI a, quant à elle, effectué une évaluation des mesures de contrôle de sécurité afin de dresser un inventaire des mesures de contrôle de sécurité des TI, de déterminer les lacunes en matière de mesures de contrôle et de rédiger des recommandations afin de combler ces lacunes. Ces efforts visent à éclairer la rédaction de la première année de la version 2020-2023 du plan de sécurité et à assurer une approche plus intégrée en ce qui concerne la gestion de la sécurité. La structure de gouvernance faisait également l'objet de révisions afin soutenir les responsabilités du CS nouvellement nommé.

Conformément aux nouvelles exigences en matière de gouvernance dans l'ensemble de politiques du CT, il faudrait examiner et préciser davantage les rôles, les responsabilités et les obligations de rendre compte des hauts fonctionnaires, tant dans les documents d'orientation internes que dans les descriptions de poste.

Politiques, procédures et lignes directrices

Il existe actuellement trois politiques, une directive, environ 30 normes et un guide relatifs à la sécurité à SP et la majorité d'entre eux n'a pas été mis à jour depuis 2011. Bon nombre de ces instruments de politique de SP font référence à des organes de gouvernance, à des postes ou à une terminologie obsolètes. Par exemple, la *Directive en matière de sécurité des technologies de l'information* de SP fait référence au Comité de la sécurité du Ministère, un comité qui n'existe plus, et au processus de certification et d'accréditation qui a été remplacé par le processus d'évaluation de sécurité et d'autorisation. Ces instruments ne font pas non plus référence à la délimitation des rôles entre SP et SPC en ce qui concerne la sécurisation de l'infrastructure informatique puisque cette dernière a été mise en place après la mise à jour de bon nombre des instruments en vigueur.

Bien que la direction soit consciente que les instruments de politique sur la sécurité du Ministère doivent être mis à jour pour s'harmoniser avec le nouvel ensemble de politiques du CT, les travaux de mise à jour n'avaient pas encore été entrepris au

moment de l’audit. De plus, le processus d’approbation des instruments de politique n’est pas bien défini au sein de SP. La majorité des instruments de politique ont été approuvés par le DPI, certains l’ont cependant été par le CGM et il a été impossible de trouver confirmation de l’approbation pour d’autres.

Afin d’assurer le respect des politiques et des normes de sécurité organisationnelles, les instruments de politique doivent être communiqués à tous les employés. L ‘audit a permis de constater que les employés n’ont pas facilement accès aux instruments de politique existants. Bien que certains instruments ministériels soient disponibles dans le système de gestion de l’information de SP ou sur l’intranet du ministère, l’équipe d’audit n’a pas pu s’assurer, dans certains cas, que les orientations et instruments de politique consultés étaient les dernières versions approuvées. L'audit n’a pas permis de constater qu’une stratégie de communication solide était en place pour informer les parties prenantes des instruments de politique disponibles et de leurs responsabilités en matière de sécurité des TI. Une communication claire et officielle en ce qui concerne les rôles et responsabilités contribue à une culture de la responsabilité, en plus d’aider à assurer la conformité.

Recommandation 1

Le sous-ministre adjoint (SMA), Secteur de la gestion ministérielle (SGM) devrait examiner le cadre de gouvernance actuel afin de s’assurer qu’il soit harmonisé avec les exigences de la nouvelle *Politique sur la sécurité du gouvernement* du Conseil du Trésor et d’améliorer la prise de décisions stratégiques matière de sécurité des technologies de l’information, en particulier :

- veiller à l’intégration systématique de la sécurité des TI au processus ministériel de gestion des risques liés à la sécurité;
- clarifier les rôles et les responsabilités des personnes et des organes de gouvernance en ce qui concerne la gestion des activités de sécurité des TI;
- veiller à ce que les instruments de politique internes, y compris les politiques, procédures et lignes directrices, soient mis à jour, approuvés, communiqués et révisés régulièrement afin d’en assurer la pertinence continue.

2.2 Constatation 2 : Sécurité publique Canada a mis en place des mesures de contrôle afin de gérer les principales activités de sécurité informatique. Ces processus ne sont toutefois pas systématiquement suivis ni contrôlés de manière adéquate pour assurer une conformité continue et une atténuation proactive des risques.

Des mesures de contrôle ministérielles suffisantes et adéquates devraient être mises en place pour atténuer les principaux risques en matière de sécurité informatique, et elles devraient être exécutées de la façon prévue. Plus particulièrement, l'audit a examiné les éléments suivants :

- si les contrôles d'accès aux systèmes informatiques sont mis en œuvre et examinés de façon périodique pour protéger les systèmes informatiques et empêcher tout accès non autorisé aux informations;
- si un processus efficace est en place pour détecter les incidents, en faire le suivi, les analyser, les évaluer et les signaler le plus rapidement possible;
- si des contrôles adéquats sont en place pour prévenir la perte des informations électroniques appartenant à l'organisation, les dommages qu'elles peuvent subir ou le vol de ces informations;
- si des contrôles de sécurité adéquats sont en place dans le processus d'élaboration des systèmes de TI afin d'éviter que les systèmes soient mis en œuvre sans être protégés par les mécanismes de sécurité adéquats.

Contrôles d'accès aux systèmes informatiques

Les responsables de l'audit se sont concentrés sur la gestion des contrôles d'accès relatifs aux privilèges administratifs, puisqu'il s'agit de l'une des dix principales mesures de sécurité informatique visant à protéger les réseaux connectés à Internet mentionnés par le Centre de la sécurité des télécommunications du Canada (CSTC). La *Directive sur la gestion de la sécurité* 2019 du SCT exige que les ministères définissent les privilèges d'accès en fonction des exigences de sécurité ministérielles, de la séparation des tâches, et de l'utilisation acceptable des systèmes d'information du gouvernement pour établir des mesures afin de contrôler l'utilisation des comptes ayant des privilèges administratifs. Cela comprend de limiter le nombre d'utilisateurs qui ont des privilèges administratifs. En principe, on devrait accorder le moins d'accès privilégiés possible et les accorder seulement lorsque cela est nécessaire. La *Directive* exige également que les ministères examinent les privilèges d'accès de façon périodique, et suppriment l'accès lorsqu'il n'est plus nécessaire (p. ex., lorsqu'un employé quitte le Ministère ou change de responsabilités).

Il revient à SPC de gérer les contrôles d'accès, y compris les accès privilégiés pour tous les comptes d'infrastructure, dont l'accès au réseau et au courrier électronique. Pour sa

part, SP doit indiquer à SPC quels comptes sont valides. Conformément à la Norme relative à l'accès aux systèmes de technologie de l'information adoptée en 2011 par SP, le CSTI est chargé de surveiller la conformité à la norme sur l'accès au système. Toutefois, la gestion des comptes repose principalement sur la Division du service à la clientèle et des applications et, dans certaines circonstances, les responsables fonctionnels (c'est-à-dire les utilisateurs finaux) du système peuvent conserver certaines responsabilités en ce qui concerne la gestion des comptes (par exemple, le SGDDI et SAP).

L'audit a permis de constater qu'il n'existe aucun processus documenté pour la surveillance régulière de la gestion des accès. L'examen du contrôle d'accès est effectué sur une base ad hoc par la Division du service à la clientèle et des applications selon la disponibilité des ressources. Le CSTI n'effectue ni examen périodique ni contrôle permanent en ce qui concerne les privilèges d'accès.

En outre, des employés qui ne travaillaient plus pour le Ministère avaient encore un accès privilégié au réseau alors que certains employés actuels avaient un accès administratif à des applications essentielles dont ils n'avaient pas besoin. La suppression des privilèges d'accès pour les employés nommés pour une durée indéterminée a lieu une fois le formulaire de départ soumis par l'employé visé. Les responsables de l'audit ont cependant été avisés que les formulaires de départ sont parfois omis lorsqu'un employé quitte le Ministère ou accepte de nouvelles responsabilités au sein de l'organisation.

Au cours de l'audit, SP a mis en place un nouvel outil logiciel de surveillance pour aider à gérer l'accès aux comptes avec privilèges. L'outil de surveillance d'accès aux comptes avec privilèges permet à l'équipe de Sécurité de la GI/TI de surveiller l'utilisation d'accès privilégié et les privilèges administratifs sur tous les systèmes de SP ainsi que de fournir un moyen de remplacer le besoin d'avoir ces accès privilégiés localement en employant l'outil de performer certaines taches au nom de l'utilisateur. Les éléments de preuve étaient cependant insuffisants pour présumer qu'un examen périodique des utilisateurs disposant de privilèges administratifs était effectué en complément de cet outil et pour vérifier si les comptes étaient vraiment gérés de façon efficace.

Gestion des incidents liés à la sécurité de la TI

La *Politique du gouvernement sur la sécurité* définit un événement lié à la sécurité comme tout événement, acte, omission ou situation qui pourrait porter atteinte à la sécurité du gouvernement, y compris les menaces, les vulnérabilités et les incidents de sécurité. D'autre part, elle définit un incident de sécurité comme un événement (ou un ensemble d'événements), un acte, une omission ou une situation qui a entraîné une compromission. Ces incidents peuvent être délibérés ou accidentels.

Des pratiques en matière de gestion des événements de sécurité doivent être définies, documentées, mises en œuvre, surveillées et maintenues pour assurer la surveillance, l'intervention et l'établissement de rapports en ce qui concerne les menaces, les vulnérabilités, les incidents de sécurité et les autres événements de sécurité. Elles permettent également de s'assurer que ces activités sont efficacement coordonnées au sein du Ministère, avec les partenaires et à l'échelle du gouvernement, pour gérer les répercussions éventuelles, appuyer la prise de décisions et permettre l'application de mesures correctives. Les événements et incidents de sécurité informatique peuvent être déterminés à l'aide de différentes sources comme les outils d'antivirus/anti-maliciel, les rapports hebdomadaires du Centre canadien pour la cybersécurité, les ratissages de sécurité, les courriels envoyés par le « National Institute of Standards and Technology », les notifications envoyées par l'entremise de la boîte aux lettres de sécurité de SP ou du service d'assistance ou ils peuvent être signalés directement à l'ASM ou au DPI.

Il n'y a cependant aucun suivi officiel des incidents de sécurité informatique à SP. Conformément à la Norme relative à la gestion des incidents de sécurité visant la technologie de l'information (TI) de SP, l'équipe des TIs doit assurer qu'il y a des mécanismes en place pour tenir compte du type, du volume et des coûts des incidents de sécurité des TI afin de les qualifier et de les surveiller et il incombe au CSTI de superviser les activités de gestion des incidents de sécurité des TI. Le personnel responsable de la sécurité des TI a indiqué que les incidents de sécurité informatique sont traités au fur et à mesure qu'ils sont reçus ou détectés. L'équipe d'audit a été informée que seuls quatre ou cinq incidents de sécurité informatique avaient été signalés ou avaient fait l'objet d'une enquête au cours des deux dernières années. Nous n'avons toutefois pas pu le confirmer, car il n'existe ni dossier ni rapport documenté à cet égard.

Des améliorations importantes en ce qui concerne le processus de gestion des incidents de sécurité informatique au sein de SP sont nécessaires. L'audit n'a pas permis de confirmer que tous les incidents de sécurité des TI avaient été consignés et traités de façon appropriée ni de garantir que des mesures correctives aient été mises en œuvre en temps utile. Un tel processus permettrait à SP d'avoir une idée plus précise du nombre et des types d'incidents de sécurité des TI et ainsi d'établir le niveau de menace global pour le Ministère et réagir en conséquence.

Sécurité des ressources de gestion de l'information

La *Politique du gouvernement sur la sécurité* du CT précise que « Les exigences, les pratiques et les mesures de sécurité de la gestion des renseignements sont définis, documentés, élaborés, évalués, surveillés et entretenus à chaque étape du cycle de vie de l'information afin de fournir une assurance raisonnable que l'information est

adéquatement protégée d'une manière qui respecte les obligations juridiques et autres et pèse le risque de préjudice et de menaces avec le coût d'appliquer des mesures de sauvegarde. »

SP crée, stocke et transmet des informations sur trois réseaux gouvernementaux :

- le réseau ministériel de SP (SGDDI) encadré par SPC, pour l'information protégée jusqu'au niveau de sécurité Protégé B;
- l'infrastructure secrète du GC (ISGC) encadré par SPC, pour l'information classifiée jusqu'au niveau de sécurité Secret;
- le réseau canadien Très secret encadré par le CSTC, pour l' information classifiée jusqu'au niveau de sécurité Très secrète.

Les dossiers électroniques générés par SP sont en grande partie stockés dans le SGDDI. Bien que la portée de l'audit n'ait pas inclus l'examen des informations stockées dans l'infrastructure secrète du GC et le réseau canadien Très secret, les responsables de l'audit ont tout de même examiné les mesures de contrôle en place qui empêchent des informations secrètes et très secrètes d'être stockées sur le réseau ministériel (SGDDI).

Le CGM reçoit des tableaux de bord trimestriels sur les mises à jour informatiques et de sécurité qu'il utilise à des fins de surveillance. Le tableau de bord pour le premier trimestre de 2019-2020 préparé par la Direction générale du DPI et présenté au CMR indiquait qu'environ [Caviardé] au-dessus du niveau Protégé B étaient stockés dans le SGDDI. Il se peut que ce problème soit lié à un certain nombre de facteurs, notamment la surclassification des documents par les employés de SP, le manque d'application de la réglementation, la connaissance limitée des normes de traitement des documents électroniques ou la difficulté d'utiliser l'infrastructure secrète du GC et d'y accéder. L'équipe d'audit n'a pas tenté de déterminer si un niveau de sécurité trop élevé avait été attribué aux documents. Pendant l'audit, ce nombre a été réduit à [Caviardé], et la possibilité pour les utilisateurs de sélectionner un niveau de classification au-dessus de Protégé B au moment de la sauvegarde d'un document dans le SGDDI a été supprimée. En outre, le personnel de la Direction générale du DPI travaillait avec les différents secteurs pour les conseiller sur l'examen et l'utilisation des niveaux de classification des documents et, si nécessaire, pour migrer les documents du réseau ministériel vers le réseau approprié.

À SP, les activités de surveillance visant à assurer le respect des exigences en matière de sécurité de l'information sont très limitées. Par exemple, environ [Caviardé] protégés ou classifiés étaient accessibles à tous les utilisateurs du SGDDI pendant l'audit. Les utilisateurs ne possédaient cependant pas nécessairement tous l'autorisation de

sécurité requise pour y accéder. Les documents stockés dans le SGDDI ne font l'objet d'aucun examen ou test périodique pour déterminer s'ils ont été correctement classés.

Les employés de SP ont une connaissance limitée des exigences en matière de traitement des documents électroniques et d'utilisation d'outils de transmission électronique sécurisés (par exemple Entrust). La transmission d'informations ou de documents sensibles de SP à des adresses électroniques personnelles sans protection supplémentaire comme le chiffrement ne fait pas non plus l'objet d'une surveillance. Sans pratiques ni mesures de contrôle adéquates pour s'assurer que les informations de SP sont protégées de façon appropriée, il est possible que des informations ne soient pas classifiées de manière appropriée ou traitées selon leur sensibilité et leur importance pour l'organisation.

L'avis de mise en œuvre de la *Politique sur la technologie de l'information* du SCT pour l'*Utilisation sécurisée des supports de stockage de données portatifs au gouvernement du Canada* exige que tous les ministères tiennent des registres des supports de stockage de données portatifs fournis au sein de leur organisation. Tous les supports de stockage de données portatifs doivent être contrôlés au moyen d'un mot de passe ou d'un identificateur biométrique, et l'information qui y est sauvegardée doit être chiffrée. Cette directive s'ajoute aux procédures de sécurité physique, mais ne les remplace pas. L'audit a permis de constater que SP ne tient pas de registre des clés USB fournies par le Ministère et que les mesures de contrôle mises en place pour vérifier si les personnes enregistrent des informations sensibles sur une clé USB sont limitées. En outre, SP n'examine pas le contenu des clés USB lorsque le Ministère effectue des ratissages de sécurité. Il y a donc un risque que les clés USB contiennent des informations sensibles non chiffrées, ce qui pourrait constituer un incident de sécurité.

Les données de tous les ordinateurs portables de SP doivent être chiffrées à l'aide d'un module de chiffrement approuvé par le CSTC. L'équipe d'audit a examiné l'image standard utilisée pour les ordinateurs portables et les tablettes ayant été migrés vers le système d'exploitation Windows 10 et a constaté que ces appareils sont chiffrés avec [Caviardé], un module de chiffrement approuvé par le CSTC. À l'avenir, le ministère a l'intention de chiffrer toutes les données stockées sur les ordinateurs de bureau et les ordinateurs portables et de désactiver tous les ports USB par défaut lorsque la mise à niveau vers Windows 10 aura été pleinement mise en œuvre dans l'ensemble du Ministère.

En l'absence d'un processus adéquat permettant de contrôler les supports de stockage de données portatifs, il y a un risque que les informations sensibles ne soient pas suffisamment protégées contre l'accès et la divulgation non autorisés.

Mesures de contrôle de sécurité pour les systèmes et applications informatiques

La *Directive sur la gestion de la sécurité* du SCT exige que tous les systèmes informatiques soient évalués et autorisés avant d'être mis en service en utilisant pour ce faire un processus d'évaluation et d'autorisation de sécurité (EAS) de la TI. Tout comme l'ancien processus de certification et d'accréditation, le processus d'évaluation de sécurité et d'autorisation de la TI est utilisé pour évaluer si les exigences applicables en matière de sécurité sont respectées pour un système ou un service particulier et si les contrôles et les mesures de protection fonctionnent de la façon prévue avant qu'un système soit mis en production.

SP a élaboré un Guide d'évaluation et d'autorisation de sécurité en 2016 pour le processus d'EAS de la TI, une Norme relative à la gestion des changements, des configurations et des versions, une Norme relative à la sécurité de la technologie de l'information (TI) dans le cycle chronologique de l'élaboration des systèmes (CCES), en plus d'avoir mis sur pied un conseil de contrôle des changements. La division de la Sécurité GI/TI est responsable de la gestion du processus d'évaluation de sécurité et d'autorisation de la TI, selon lequel un certain nombre d'exigences de sécurité informatique doivent être remplies avant qu'un système ne soit autorisé à être mis en production :

- description du profil du système;
- énoncé de sensibilité (ES);
- concept des opérations;
- matrice de traçabilité des exigences relatives à la sécurité (MTES);
- évaluation des facteurs relatifs à la vie privée (si le système contient des informations permettant d'identifier une personne);
- évaluation des vulnérabilités.

Une fois le processus d'évaluation et d'autorisation de sécurité de la TI effectué, la division de la Sécurité GI/TI prépare le rapport sur ce processus afin de recommander l'approbation. Un système informatique peut recevoir une autorisation d'exploitation complète, une autorisation d'exploitation provisoire ou aucune autorisation d'exploitation.

Bien qu'il y ait environ 50 systèmes et applications informatiques au sein de SP, les responsables de l'audit se sont concentrés sur les six applications indiquées par le Ministère comme étant essentielles à la mission. Cela a permis de constater que le rapport sur le processus d'évaluation de sécurité et d'autorisation de la TI n'a pas été rédigé pour les six applications essentielles, ce qui signifie que ces applications sont en production sans autorisation d'exploitation valide et qu'elles risquent donc de contenir des vulnérabilités relatives à la sécurité. SP a reconnu ce problème et l'a inclus dans son ébauche de registre des risques de sécurité.

SP a également mis en place un conseil de gestion des changements responsable de toutes les propositions en ce qui concerne les modifications à la gestion de la configuration ou au système. Avant la mise en œuvre de toute modification dans le système, le rapport sur le processus d'évaluation de sécurité et d'autorisation de la TI et l'autorisation d'exploitation doivent être mis à jour par la division de la Sécurité GI/TI.

L'équipe d'audit a testé deux modifications majeures récemment apportées à des applications essentielles afin de déterminer si leur impact sur la sécurité de la TI et s'ils étaient en conformité avec le processus de gestion des changements. Les deux modifications sélectionnées étaient les suivantes :

1. « InfoMédia » : intégration de Twitter (décembre 2018).
2. SGDDI : mise à niveau du SGDDI (juillet 2019).

L'audit a permis de constater que les modifications à InfoMédia ont été mises en œuvre sans prévenir ou aviser la division de la Sécurité GI/TI, et donc l'impact potentiel de la modification du système InfoMédia n'a pas été évalué.

En ce qui concerne la mise à niveau du SGDDI, un représentant de la sécurité informatique était présent lors de la discussion avec le conseil de gestion des changements, mais aucune analyse documentée des impacts sur la sécurité informatique ni aucune autorisation d'exploitation n'ont été trouvées.

Le non-respect du processus établi pourrait donc signifier que les modifications apportées aux systèmes et aux applications informatiques ont été mises en œuvre sans tenir pleinement compte des incidences qu'elles peuvent avoir sur la sécurité informatique, ce qui pourrait entraîner l'introduction de vulnérabilités relatives à la sécurité dans les systèmes et applications informatiques existants.

Recommandation 2

Le SMA du SGM devrait, en adoptant une approche fondée sur les risques, effectuer des examens et une surveillance continus des activités clés suivantes en matière de sécurité des TI, afin de s'assurer qu'elles respectent les processus établis pour la protection des informations ministérielles de nature délicate :

- gestion de l'accès aux systèmes informatiques;
- processus permettant de déterminer, d'évaluer et de signaler les incidents de sécurité informatique;
- prévention et gestion de toute perte de données, de tout dommage aux données ou de toute compromission des données de l'organisation;
- considérations liées à la sécurité dans le cycle de vie de l'élaboration des systèmes.

2.3 Constatation 3 : Sécurité publique Canada a défini les composantes d'un programme de formation et de sensibilisation à la sécurité informatique; des améliorations sont nécessaires afin de s'assurer que les employés comprennent mieux leurs responsabilités en matière de protection de la confidentialité, de la disponibilité et de l'intégrité des informations.

Tous les employés, pas seulement ceux de la Division de la sécurité de la GI/TI, sont responsables de la sécurité des technologies de l'information et de l'information qu'elles contiennent. La nouvelle *Politique du gouvernement sur la sécurité* du CT et la *Directive sur la gestion de la sécurité du SCT* exigent que chaque ministère définisse, documente et tienne à jour les exigences et les pratiques ministérielles en matière de sensibilisation et de formation à la sécurité, conformément aux exigences de la politique pangouvernementale. Les ministères doivent élaborer, donner, consigner et tenir à jour des activités et des produits de sensibilisation à la sécurité pour renseigner les personnes au sujet des menaces et des risques pour la sécurité et leur rappeler leurs propres responsabilités en matière de sécurité. Les ministères doivent également fournir ou organiser une formation sur la sécurité pour tous les employés, y compris une formation spécialisée en matière de sécurité pour les personnes ayant des responsabilités spécifiques en matière de sécurité, comme le gardien COMSEC.

En 2019-2020, l'ASM a élaboré une stratégie de sensibilisation à la sécurité qui exige que tous les employés suivent deux cours sur la sécurité dès leur arrivée au Ministère. Le premier cours obligatoire s'intitule Sensibilisation à la sécurité (A230) et est offert par l'École de la fonction publique du Canada. L'équipe d'audit a obtenu la confirmation que, en août 2019, 87 % des employés de PS avaient suivi ce cours obligatoire. Le deuxième cours est une vidéo obligatoire sur la sécurité d'une durée de 20 minutes que tous les membres du personnel (employés et contractuels) doivent regarder pendant leur période d'orientation avant de recevoir leur laissez-passer pour l'édifice.

Bien qu'ils ne soient pas spécifiquement axés sur la sécurité informatique, ces deux cours obligatoires couvrent les éléments de base de la sécurité informatique et sont bien présentés. SP n'a mis en place aucun programme de formation et de sensibilisation sur la sécurité informatique, et n'a pas non plus établi d'obligation en ce qui concerne la mise en place d'une formation d'appoint sur la sensibilisation à la sécurité, offerte à intervalles réguliers, afin d'informer les membres du personnel des nouvelles menaces et tendances en matière de sécurité informatique.

SP n'organise pas non plus pour ses employés d'exercices pratiques sur la sensibilisation à la sécurité qui pourraient les sensibiliser à la façon de réagir en cas d'incidents de sécurité présumés (par exemple, des exercices sur l'hameçonnage). La procédure de ratissage de sécurité n'inclut aucune évaluation des principales mesures de contrôle de sécurité, comme les dispositifs USB non surveillés et non protégés ou les ordinateurs portables sans câble de sécurité laissés sans surveillance. On consigne

cependant, lors des ratissages, tout ordinateur sur lequel la session est ouverte et qui a été laissé déverrouillé par un utilisateur.

La formation sur la sensibilisation à la sécurité devrait être donnée de façon systématique et exhaustive afin de s'assurer que toutes les personnes connaissent leurs responsabilités sur ce plan et qu'elles maintiennent les connaissances et les compétences nécessaires pour s'acquitter efficacement de leurs fonctions. Ceci permettrait également de donner une assurance raisonnable que les employés de SP ne compromettront pas volontairement la sécurité et qu'ils comprennent les conséquences possibles du non-respect de ces responsabilités en matière de sécurité.

Recommandation 3

Le SMA du SGM devrait veiller à ce qu'un programme de sensibilisation et de formation à la sécurité informatique soit élaboré pour la sécurité informatique et à ce qu'il soit mis en œuvre pour couvrir et évaluer de manière exhaustive les risques liés à la sécurité informatique et faire en sorte que les employés conservent les connaissances requises pour pouvoir s'acquitter de leurs responsabilités.

3 Conclusion

Des améliorations sont nécessaires pour que Sécurité publique Canada puisse établir un cadre de contrôle des activités de sécurité informatique qui soit bien défini et pleinement efficace, en plus d'être conforme à la *Politique sur la sécurité du gouvernement* révisée du Conseil du Trésor, ainsi qu'aux autres politiques, directives et normes pertinentes. Plus précisément, Sécurité publique Canada devra faire des efforts importants pour documenter et communiquer les pratiques de contrôle de la sécurité informatique exigées par le Conseil du Trésor et assurer leur application.

4 Plan d’action de la direction

Recommandation	Mesures prévues	Date d’achèvement cible
1. Le sous-ministre adjoint, Secteur de la gestion ministérielle devrait examiner le cadre de gouvernance actuel afin de s’assurer qu’il soit harmonisé avec les exigences de la nouvelle *Politique sur la sécurité du gouvernement* du Conseil du Trésor et d’améliorer la prise de décisions stratégiques en matière de sécurité des technologies de l’information, en particulier : • veiller à l’intégration systématique de la sécurité des TI au processus ministériel de gestion des risques liés à la sécurité; • clarifier les rôles et les responsabilités des personnes et des organes de gouvernance en ce qui concerne la gestion des activités de sécurité des TI; • veiller à ce que les instruments de politique internes, y compris les politiques, procédures et lignes directrices, soient mis à jour, approuvés,	Définir les rôles et désigner un agent de la cybersécurité (ACS) et un agent de la cybersécurité adjoint (ACSA), dans le cadre d’une clarification plus globale des rôles et responsabilités en matière de sécurité des TI au sein de la DGDPI et du SGM. Définir et distinguer les rôles et responsabilités respectifs en matière de sécurité des TI avec nos fournisseurs de services d’entreprise : Services partagés Canada (SPC), Centre de la sécurité des télécommunications Canada (CSTC), Services publics et Approvisionnement Canada (SPAC). Créer et tenir à jour un registre des risques pour la sécurité des TI basé sur le Plan de sécurité ministériel (PSM) et les risques ministériels. Revoir les contrôles de sécurité interne énoncés dans la publication ITSG-33. Faire un examen détaillé des politiques, procédures et lignes directrices de Sécurité publique	31/03/2021 31/03/2022 31/03/2021 31/03/2023 31/03/2023

communiqués et révisés régulièrement afin d'en assurer la pertinence continue.	Canada en matière de sécurité des TI. Examiner et harmoniser les processus d'évaluation et d'autorisation de sécurité (EAS) et les autorisations d'exploiter.	 31/03/2021
2. Le sous-ministre adjoint, Secteur de la gestion ministérielle devrait, en adoptant une approche fondée sur les risques, effectuer des examens et une surveillance continus des activités clés suivantes en matière de sécurité des TI, afin de s'assurer qu'elles respectent les processus établis pour la protection des informations ministérielles de nature délicate : • gestion de l'accès aux systèmes informatiques; • processus permettant de déterminer, d'évaluer et de signaler les incidents de sécurité informatique; • prévention et gestion de toute perte de données, de tout dommage aux données ou de toute compromission des données de l'organisation; • considérations liées à la sécurité dans le cycle de vie de l'élaboration des systèmes.	Élaborer un plan d'investissement décrivant les achats prévus de nouveaux outils de sécurité des TI de façon progressive, selon ce que dicteront les priorités et les ressources. Créer et maintenir une infrastructure distincte pour les employés affectés à la sécurité des TI et les dispositifs et les outils connexes. Demander au Conseil d'adoption stratégique et d'examen des projets (CASEP) de prendre en compte la sécurité des TI tout au long du cycle de vie des activités et des projets de GI/TI faisant l'objet d'un suivi. Registre de suivi des événements, incidents et compromissions en matière de sécurité. Mettre à jour ou exécuter le processus d'EAS et l'autorisation d'exploiter pour toutes les applications existantes de SP importantes	31/03/2023 31/03/2021 31/03/2021 31/03/2021 31/03/2023

	et critiques, en privilégiant celles qui sont critiques. Revoir régulièrement les droits d'administration et faire une vérification des activités des utilisateurs bénéficiant de privilèges élevés sur tous les systèmes. Créer et tenir à jour un calendrier intégré de toutes les activités liées à la sécurité des TI, afin de faciliter la planification et la surveillance, les analyses et les examens continus, et de garantir la conformité avec les politiques et les processus en place.	31/03/2021 31/03/2021
3. Le sous-ministre adjoint, Secteur de la gestion ministérielle devrait veiller à ce qu'un programme de sensibilisation et de formation à la sécurité informatique soit élaboré pour la sécurité informatique et à ce qu'il soit mis en œuvre pour couvrir évaluer de manière exhaustive les risques liés à la sécurité informatique et faire en sorte que les employés conservent les connaissances requises pour pouvoir s'acquitter de leurs responsabilités.	Élaborer une stratégie de communication et de sensibilisation à la sécurité. Instaurer un processus d'inspection du contenu numérique. Instaurer une surveillance spéciale des activités à haut risque des utilisateurs. Mettre en œuvre périodiquement des programmes de détection de l'hameçonnage et de tests de sécurité.	31/03/2021 31/03/2021 31/03/2021 31/03/2021

Remerciements

La Direction générale de l'audit interne et de l'évaluation tient à remercier toutes les personnes qui ont fourni des conseils et de l'aide pendant l'audit.

Annexe A : Critères de l’audit

Les critères suivants ont permis de garantir un contrôle suffisant et approprié favorisant ainsi l’atteinte de l’objectif de l’audit et aidant les vérificateurs à formuler leur opinion :

Critère 1	Une structure de gouvernance efficace est en place pour favoriser la planification, la prise de décisions et la surveillance en matière de sécurité informatique.
Critère 2	Des mesures de contrôle ministérielles suffisantes et opérationnelles sont en place pour atténuer les risques en matière de sécurité informatique, et ces contrôles fonctionnent comme prévu.

Annexe B : Acronymes

DPI	Dirigeant principal de l'information
SGM	Secteur de la gestion ministérielle
CSTC	Centre de la sécurité des télécommunications Canada
SECOM	Sécurité des communications
CS	Chef de la sécurité
CGM	Comité de gestion du Ministère
ASM	Agent de sécurité du Ministère
PSM	Plan de sécurité ministériel
ISGC	Infrastructure secrète du gouvernement du Canada
RCTS	Réseau canadien Très secret
GI	Gestion de l'information
TI	Technologie de l'information
CGTI	Contrôles généraux de la technologie de l'information
AMPTI	Avis de la mise en œuvre de la politique de TI
CSTI	Coordonnateur de la sécurité de la technologie de l'information
GSTI	Norme opérationnelle de sécurité du Conseil du Trésor – Gestion de la sécurité des technologies de l'information
NIST	National Institute of Standards and Technology
ICP	Infrastructure à clés publiques
EFVP	Évaluation des facteurs relatifs à la vie privée
SP	Sécurité publique Canada
CMR	Comité de gestion des ressources
EAS	Évaluation et d'autorisation de sécurité
ES	Énoncé de sensibilité
MTES	Matrice de traçabilité des exigences en matière de sécurité
SPC	Services partagés Canada
CT	Conseil du Trésor du Canada