AUDIT HORIZONTAL DE LA GESTION DE L'INFORMATION SENSIBLE

Division de l'audit interne et de l'évaluation

Avril 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 24 mars 2025.
Approuvé par le directeur des poursuites pénales le 24 avril 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 : J79-37/2025F-PDF

ISBN : 978-0-660-76651-5

TABLE DES MATIÈRES

SOMMAIRE

Contexte

Le Service des poursuites pénales du Canada (SPPC) est une autorité de poursuite, qui utilise et génère une quantité importante d'informations classifiées et sensibles. Le milieu de travail post-pandémique offre aux employés la souplesse de travailler à l'extérieur du bureau, tout en ayant accès à un large éventail d'informations protégés et/ou sensibles, qui sont contenues dans les dossiers de poursuite. La divulgation non autorisée (intentionnelle ou accidentelle) de ces informations pourrait avoir de sérieuses répercussions sur la réputation et l'intégrité de l'organisme.

L'équipe de Planification stratégique et mesure du rendement a désigné la protection des informations comme représentant l'un des principaux risques pour le SPPC, dans le cadre du plus récent exercice de profil de risque organisationnel. En outre, le nombre d'atteintes à la protection des renseignements liés aux poursuites qui sont signalées a augmenté dans l'ensemble de l'organisme, en particulier en ce qui concerne le caviardage incorrect/insuffisant des informations contenus dans les documents à communiquer et/ou les documents de la Cour.

Par conséquent, la haute direction a intérêt à obtenir l'assurance que des processus et des contrôles sont en place et fonctionnent comme prévu, afin de garantir la protection des informations sensibles et/ou classifiées (Protégé C, Secret, Très secret), contenues dans les dossiers de poursuites.

Objectif

L'Audit horizontal de la gestion de l'information sensible vise à assurer que des processus et des contrôles sont en place et fonctionnent comme prévu pour garantir la protection des informations sensibles et classifiées relatives aux poursuites, y compris les processus de caviardage des renseignements, qui sont contenus dans les documents de la Cour.

Conclusion de l'audit

Le SPPC dispose de processus et de contrôles adéquats et efficaces pour la gestion de l'information sensible. Toutefois, afin d'accroître l'efficacité, il convient de faciliter l'accès et de simplifier les processus physiques.

En outre, la transmission régulière de communications concises et adaptées aux publics cibles est nécessaire pour faciliter la compréhension des exigences relatives à la gestion des renseignements de nature délicate par les employés du SPPC et les mandataires. De plus, il convient de préciser les exigences des mandataires quant à l'utilisation de leurs outils et installations.

Des activités de formation et de sensibilisation sont organisées, mais il y a lieu d'offrir une formation régulière et ciblée pour mieux soutenir et promouvoir la connaissance de la gestion des informations sensibles.

On a mis en place une gestion efficace des autorisations de sécurité des mandataires. Néanmoins, le niveau des autorisations de sécurité délivrées aux employés du SPPC ne correspond pas toujours aux fonctions exercées et certaines n'ont pas été mises à jour en fonction des périodes de validité prescrites, ce qui est non conforme à la Norme sur le filtrage de sécurité du Conseil du Trésor (CT) du Canada. Les employés du SPPC sont responsables de mettre à jour leur autorisation de sécurité, et aucune surveillance n'est exercée à cet égard.

Des mécanismes de rapportage sur la gestion de l'information sensible sont en place. Néanmoins, pour atténuer les risques, il y a lieu d'adopter une approche plus proactive en matière de surveillance et de rapports, notamment en ce qui concerne les autorisations de sécurité et les outils et les installations des mandataires. Enfin, le renforcement des contrôles à l'égard du caviardage des renseignements contenus dans les documents de la Cour peut contribuer à réduire le nombre d'atteintes à la vie privée.

Sommaire des recommandations

1. Les instruments de politique du SPPC traitant de la gestion de l'information sensible doivent être rédigés en langage clair et préciser les rôles et responsabilités du personnel des opérations juridiques du SPPC et des mandataires. En outre, ils doivent être mis à la disposition des employés du SPPC et des mandataires. (Moyen)
2. Les communications traitant de la gestion des informations sensibles à l'intention des régions et des mandataires doivent être efficaces, cohérentes et transmises régulièrement. L'approche doit prévoir la transmission des communications par une source appropriée, s'inscrire dans un contexte adapté aux régions/mandataires et privilégier la concision. (Moyen)
3. La formation obligatoire à l'intention des employés du SPPC doit être définie, facilement accessible, offerte régulièrement et faire l'objet d'un suivi quant à la participation. En outre, il faut évaluer le besoin de définir des exigences en matière de formation obligatoire pour les mandataires. Il convient de tenir compte de la nécessité d'adapter la formation aux réalités de la gestion des informations sensibles liées aux dossiers de poursuite du SPPC. (Moyen)
4. La mise en œuvre de solutions numériques sécurisées pour le transfert d'information sensible devrait être envisagée afin d'améliorer l'efficacité et de réduire le risque pour le SPPC résultant d'actions non conformes. (Moyen)
5. Il convient d'assurer une sensibilisation et une conformité à l'égard des exigences du CT en ce qui concerne la délivrance d'attestations de sécurité dont le niveau correspond aux fonctions exercées. Les attestations de sécurité doivent être mises à jour en conformité avec la Norme sur le filtrage de sécurité du CT. (Élevé)

PROCESSUS DE GOUVERNANCE

Ce à quoi nous nous attendions

Nous nous attendions à ce que le SPPC ait consigné un cadre clair, y compris les rôles et responsabilités pertinents, pour soutenir la gestion de l'information sensible par les employés et les mandataires du SPPC.

En outre, nous nous attendions à constater la transmission régulière de communications visant à promouvoir la sensibilisation des employés du SPPC et des mandataires aux politiques, directives, normes et lignes directrices.

Conclusion

Les processus adéquats sont consignés, et la communication est assurée, mais il faut préciser les exigences des mandataires. De plus, la transmission régulière de communications concises et adaptées au public cible facilitera la compréhension des exigences en matière de gestion des informations sensibles par les employés du SPPC et les mandataires.

Constatations

Politiques et processus

Nous avons constaté la consignation de politiques et processus établis pour soutenir la gestion adéquate de l'information sensible par les employés du SPPC et les mandataires.

Les rôles et les responsabilités des avocats à l'interne ont été définis, mais pas ceux des membres du personnel de soutien juridique, qui participent également au traitement de l'information sensible liée aux dossiers de poursuite.

Les politiques et processus à l'intention des mandataires, notamment les Conditions d'ententes à terme fixe des mandataires, ne fournissent pas suffisamment de précisions sur les rôles et responsabilités, la préservation/conservation et l'élimination des renseignements, ainsi que sur les outils et les installations. Dans les régions, les équipes de supervision des mandataires (ESM) ont indiqué fournir aux mandataires des mises à jour à cet égard à mesure que celles-ci sont disponibles. Cependant, toutes ont omis de fournir aux mandataires la Directive sur la gestion de l'information du SPPC, contrairement aux Conditions d'ententes à terme fixe des mandataires. En outre, au moment de l'accueil et de l'intégration, ce ne sont pas toutes les ESM qui ont remis aux mandataires les politiques et processus centralisés du SPPC, même si les mandataires sont chargés, au même titre que les employés du SPPC, de gérer les dossiers de poursuite.

Communication

Nous avons constaté que les Services de sécurité et les bureaux régionaux du SPPC transmettent régulièrement des communications aux employés de l'organisme pour favoriser la connaissance des instruments de politique pertinents, et l'ensemble des ESM ont indiqué qu'elles s'occupent d'acheminer ces communications aux mandataires.

En outre, contrairement aux mandataires, les employés du SPPC ont accès aux politiques et processus publiés sur iNet[A]. Cependant, les instruments de politique ne sont pas facilement accessibles sur iNet, ce qui peut nuire à la sensibilisation des employés aux exigences.

Bien que les employés et les mandataires aient indiqué que la communication était suffisante, les commentaires recueillis signalent la nécessité d'une communication plus proactive, claire et cohérente de la part de l'administration centrale, des bureaux régionaux et des ESM. La transmission régulière de communications concises et adaptées au public cible peut contribuer à accroître la mobilisation des intervenants.

Recommandation 1

Le directeur adjoint des poursuites pénales et le directeur général principal des Services ministériels doivent veiller à ce que les instruments de politique du SPPC traitant de la gestion de l'information sensible soient rédigés en langage clair et précisent les rôles et responsabilités du personnel des opérations juridiques du SPPC et des mandataires et qu'ils soient mis à la disposition des employés du SPPC et des mandataires. (Moyen)

Recommandation 2

Le directeur adjoint des poursuites pénales et le directeur général principal des Services ministériels doivent veiller à la transmission régulière de communications efficaces et cohérentes sur la gestion de l'information sensible aux régions et aux mandataires. L'approche adoptée doit prévoir :

- *la transmission des communications par une source appropriée (p. ex., les procureurs fédéraux en chef pour les communications régionales);*
- *l'ajout de contexte destiné aux régions/mandataires pour centraliser les communications avant la transmission aux régions/mandataires;*
- *la présentation concise et directe des principaux points. (Moyen)*

[A] Il s'agit du site Intranet du SPPC, utilisé pour communiquer aux employés les informations et les ressources informatiques de l'organisme en toute sécurité.

Ce à quoi nous nous attendions

Nous nous attendions à ce que des programmes de formation soient mis en place efficacement, afin d'accroître les connaissances et la compréhension des employés et des mandataires en ce qui concerne leurs responsabilités en matière de protection des informations sensibles.

Conclusion

Bien que divers types de formations et d'activités de sensibilisation soient offerts, il y a lieu d'offrir une formation régulière et ciblée pour mieux soutenir et promouvoir la connaissance de la gestion des informations sensibles. Accroître la sensibilisation à cet égard peut permettre de réduire les risques de non-conformité.

Formation

Le SPPC a désigné pour les employés deux cours obligatoires sur la gestion de l'information sensible : le cours Sensibilisation à la sécurité (COR310), offert à tous les employés par l'École de la fonction publique du Canada, et le cours Les poursuites – principes fondamentaux (niveau 1), donné aux procureurs dans le cadre du Programme de perfectionnement des procureurs fédéraux du SPPC. Ce dernier porte notamment sur le caviardage des renseignements contenus dans les documents à communiquer, qui s'apprend également dans le cadre de la formation en cours d'emploi.

Toutefois, seulement environ 60 % des employés du SPPC possèdent des documents indiquant qu'ils ont suivi le cours obligatoire Sensibilisation à la sécurité. En outre, certains employés nous ont mentionné que l'accès à la formation sur les principes fondamentaux pouvait être retardé en raison du nombre limité de places disponibles et des réductions du budget de voyage. Le fait de ne pas appliquer l'exigence quant à la formation obligatoire n'est pas efficace.

Il n'y a pas de formation obligatoire sur la gestion de l'information sensible pour les mandataires. De plus, nous avons constaté un manque de clarté et de cohérence dans le matériel de formation fourni par les ESM aux mandataires dans les différentes régions.

Les mandataires et les employés du SPPC qui ont répondu à un sondage ont indiqué recevoir une formation suffisante. Cependant, les employés ont souligné avoir besoin d'une formation plus régulière, de formations de recyclage et de formations ciblées, en particulier sur le caviardage des renseignements contenus dans les documents à communiquer. En outre, certains employés ont mentionné qu'une formation dirigée par un formateur leur apporterait plus de clarté que la lecture de procédures et de lignes directrices.

Recommandation 3

Le directeur général principal des Services ministériels doit veiller à ce que la formation obligatoire fournie aux employés du SPPC soit définie, facilement accessible, offerte régulièrement et qu'elle fasse l'objet d'un suivi en ce qui concerne l'achèvement. Il convient d'évaluer le besoin de définir des exigences en matière de formation obligatoire pour les mandataires. Il faut envisager d'élaborer et/ou de fournir une formation qui tient compte des réalités de la gestion de l'information sensible contenue dans les dossiers de poursuite du SPPC. (Moyen)

EFFICACITÉ ET EFFICIENCE OPÉRATIONNELLES

Ce à quoi nous nous attendions

Nous nous attendions à ce que des installations et des outils adéquats soient en place pour permettre aux employés et aux mandataires de gérer efficacement l'information sensible.

Nous nous attendions à ce que le niveau des attestations de sécurité délivrées corresponde aux fonctions exercées par les mandataires et les employés du SPPC.

Conclusion

En assurant la prestation de formation additionnelle afin de favoriser la compréhension des processus et des outils, il est possible de renforcer l'efficacité opérationnelle.

Le SPPC dispose d'installations et d'outils qui permettent à ses employés de gérer les informations sensibles, bien qu'il y ait lieu de faciliter l'accès et de simplifier les processus physiques afin d'accroître l'efficience. Les rapports sur les outils et les installations des mandataires peuvent permettre de confirmer le respect des exigences.

Le SPPC dispose d'outils et de processus de gestion des attestations de sécurité, mais il y a lieu d'assurer la clarté et la compréhension à l'égard de la correspondance entre le niveau des attestations de sécurité et les fonctions exécutées. La surveillance des attestations de sécurité délivrées aux employés du SPPC peut atténuer la non-conformité du SPPC à la Norme sur le filtrage de sécurité du CT.

Constatations

Installations et outils

En général, les installations et les outils mis à la disposition des employés du SPPC répondent aux exigences en matière de gestion de l'information sensible, à l'exception de certaines régions qui ne disposent pas de salles Très secret. S'il existe un processus permettant de s'assurer que les cabinets de mandataires disposent des outils et des installations nécessaires, nous n'avons pas pu vérifier si les mandataires respectent les exigences fixées en raison de l'absence de la consignation de documents à cet égard. Nous n'avons pas été en mesure de déterminer si cela est dû à une mauvaise gestion des documents ou au fait que le processus prévu pour recueillir et vérifier les informations pertinentes n'a pas été suivi.

Nous avons constaté que le SPPC ne dispose pas d'un réseau sécurisé pour stocker et transmettre les informations Protégé C et de niveaux supérieurs. Les processus suivis reposent plutôt sur une approche physique, qui prévoit notamment de se rendre dans un organisme partenaire pour recueillir/consulter les renseignements et d'utiliser des ordinateurs portables hors réseau pour stocker et consulter les informations. Ces processus peuvent prendre du temps et contribuer à un manque d'efficacité.

Les situations suivantes illustrent le manque de compréhension des employés en ce qui concerne les installations et les outils à utiliser et/ou la manière de les utiliser :

- désigner les salles de préparation des dossiers comme étant des salles Très secret;
- laisser des outils électroniques sans surveillance dans des espaces publics alors que les mots de passe y sont joints;
- utiliser des outils/processus inadéquats pour sécuriser les informations sur support matériel pendant les déplacements;
- accepter que de l'information sensible soit transmise par l'intermédiaire des réseaux du SPPC, parce que les distances géographiques sont grandes ou qu'il faut du temps pour se déplacer et remettre les renseignements en mains propres.

Environ 20 % des employés du SPPC qui ont répondu au sondage estiment que les processus actuels sont inadéquats. Selon les commentaires recueillis, l'absence d'un réseau sécurisé, l'accès restreint aux salles protégées, le temps nécessaire pour remettre les documents en mains propres et accéder aux ordinateurs portables autonomes, les processus peu clairs et le manque de formation contribuent aux inefficacités.

Attestations de sécurité

Nous avons examiné un échantillon des attestations de sécurité délivrées aux employés du SPPC et aux mandataires. Le processus de renouvellement des attestations de sécurité des mandataires fonctionne comme prévu. En effet, les mandataires faisant l'objet de l'échantillon examiné détiennent des attestations de sécurité valides et d'un niveau qui correspond aux fonctions exécutées.

Cependant, nous avons constaté un manque de clarté dans certaines régions quant à la correspondance entre le niveau des attestations de sécurité délivrées aux employés du SPPC et les fonctions exécutées, et ce ne sont pas tous les employés faisant l'objet de l'échantillon examiné qui disposent d'une attestation de sécurité d'un niveau qui correspond aux fonctions qu'ils doivent exécuter. En outre, étant donné que certains employés n'ont pas mis à jour leur attestation de sécurité, conformément à la Norme sur le filtrage de sécurité du CT, le SPPC est non conforme à la Norme. L'employé est responsable de mettre à jour son attestation de sécurité, et il n'existe pas de processus de suivi pour garantir la conformité à cet égard

EFFICACITÉ ET EFFICIENCE OPÉRATIONNELLES

Ce à quoi nous nous attendions

Nous nous attendions à ce que des mécanismes de surveillance et de rapportage soient en place pour garantir la gestion adéquate de l'information sensible.

Surveillance et rapportage

Nous avons constaté que le Comité sur la gestion de la sécurité, du savoir et du numérique assurait une surveillance adéquate à l'égard de la gestion des informations sensibles et qu'il veille à l'exécution de son mandat.

La surveillance est exercée par les ESM, qui effectuent la visite des lieux de travail des mandataires, et par les Services de sécurité, qui mènent des inspections dans les bureaux régionaux du SPPC. Néanmoins, les activités de surveillance ont cessé en raison de la pandémie de COVID-19 et les réductions du budget de voyage, limitant ainsi la visibilité sur la gestion des informations sensibles.

Le fait de signaler les atteintes à la vie privée et les incidents de sécurité est une composante essentielle de la gestion des informations sensibles et repose sur la décision des employés du SPPC et des mandataires d'en rendre compte. Nous avons constaté que des processus ont été établis pour rendre compte des atteintes à la vie privée auprès de l'équipe de l'accès à l'information et de la protection des renseignements personnels (AIPRP) et des incidents de sécurité auprès des Services de sécurité. Les processus sont réactifs et reposent sur la sensibilisation et la volonté des employés ou des mandataires à signaler la situation. Les régions qui affichent un nombre supérieur d'incidents et/ou d'atteintes peuvent en attribuer la cause à une lacune dans leurs processus, bien que cela puisse être attribuable aussi au fait que certaines régions ne signalent pas tous les incidents et/ou atteintes. Toutefois, en 2022, l'équipe de l'AIPRP a noté une hausse de la tendance à signaler les atteintes à la vie privée découlant du caviardage des renseignements contenus dans les documents de la Cour. À l'époque une recommandation avait été formulée à l'intention du directeur des poursuites pénales pour la mise en œuvre de mesures préventives aux fins du renforcement des contrôles en matière de caviardage. Néanmoins, ce type d'atteinte à la vie privée se reproduit et continue d'être signalé..

Aucune surveillance n'est exercée en ce qui concerne le caviardage par les mandataires des informations sensibles. Cependant, quatre ESM régionales ont indiqué fournir une orientation et une rétroaction à cet égard et/ou examiner les informations caviardées par les mandataires.

Finalement, il n'est pas possible d'extraire des données au moyen du module de sécurité du logiciel utilisé pour consigner les attestations de sécurité, mais on peut le faire à l'aide du module de ressources humaines. Par conséquent, cela peut contribuer à améliorer la capacité d'assurer le suivi efficace de la concordance et de la validité des attestations de sécurité et la conformité du SPPC.

Conclusion

Le SPPC a mis en œuvre des mécanismes de rapportage sur la gestion de l'information sensible, mais il convient d'apporter des améliorations afin d'adopter une approche proactive à l'égard de la surveillance et des rapports, notamment en ce qui concerne les attestations de sécurité. Le renforcement des contrôles liés au caviardage des informations contenues dans les documents de la Cour peut contribuer à la réduction des atteintes à la vie privée.

Recommandation 4

Le directeur adjoint des poursuites pénales et le directeur général principal des Services ministériels devraient envisager la mise en œuvre des solutions numériques sécurisées pour le transfert d'informations, afin d'améliorer l'efficience et de réduire le risque pour le SPPC résultant d'actions non conformes. (Moyen)

Recommandation 5

Le directeur adjoint des poursuites pénales et le directeur général principal des Services ministériels doivent veiller à la connaissance des exigences du CT, relativement à la délivrance d'attestations de sécurité d'un niveau qui correspond aux fonctions exercées. Il faut notamment veiller à ce que le niveau des attestations de sécurité délivrées soit en conformité avec les fonctions exercées et à ce que les attestations soient mises à jour selon la Norme sur le filtrage de sécurité du CT (cycle de mise à jour, section 5, annexe B). (Élevé)

PLAN D'ACTION DE LA DIRECTION

No.	Recommandation	Risque	Plan d'action de la direction	Bureau de première responsabilité	Date cible
1	Le directeur adjoint des poursuites pénales et le directeur général principal des Services ministériels doivent veiller à ce que les instruments de politique du SPPC traitant de la gestion de l'information sensible soient rédigés en langage clair et précisent les rôles et responsabilités du personnel des opérations juridiques du SPPC et des mandataires et qu'ils soient mis à la disposition des employés du SPPC et des mandataires.	Moyen	La direction approuve cette recommandation. Actions à prendre : • Les instruments de politique seront examinés par l'équipe de gestion de l'information et l'équipe de sécurité, et mis à jour, le cas échéant, notamment en définissant les rôles et les responsabilités du personnel et des mandataires des opérations juridiques. • Les documents seront disponibles sur iNet pour les employés et, pour les mandataires, sur le site web de la Gestion du savoir ou sur le site web du SPPC.	Directeur, Sécurité et gestion des installations	31 mars 2026
2	Le directeur adjoint des poursuites pénales et le directeur général principal des Services ministériels doivent veiller à la transmission régulière de communications efficaces et cohérentes sur la gestion de l'information sensible aux régions et aux mandataires. L'approche adoptée doit prévoir : • la transmission des communications par une source appropriée (p. ex., les procureurs fédéraux en chef pour les communications régionales); • l'ajout de contexte destiné aux régions/mandataires pour centraliser les communications avant la transmission aux régions/mandataires; • la présentation concise et directe des principaux points.	Moyen	La direction approuve cette recommandation. Actions à prendre : • Un plan de communication sera mis en œuvre pour assurer des communications régulières concernant la gestion de l'information sensible, tant pour les employés que pour les mandataires. Ce plan indiquera quelle méthode sera utilisée pour la diffusion des informations et par qui. • Si un contexte régional est nécessaire, il sera obtenu lors de l'élaboration du matériel. • Un gabarit sera créé pour les matériels de communication pour s'assurer que les points clés sont communiqués à l'avant.	Directeur, Sécurité et gestion des installations	31 mars 2026
3	Le directeur général principal des Services ministériels doit veiller à ce que la formation obligatoire fournie aux employés du SPPC soit définie, facilement accessible, offerte régulièrement et qu'elle fasse l'objet d'un suivi en ce qui concerne l'achèvement. Il convient d'évaluer le besoin de définir des exigences en matière de formation obligatoire pour les mandataires. Il faut envisager d'élaborer et/ou de fournir une formation qui tient compte des réalités de la gestion de l'information	Moyen	La direction est partiellement d'accord avec cette recommandation. La direction considère que la formation disponible est suffisante pour répondre aux besoins des employés du SPPC et n'élaborera pas/ne fournira pas de formation supplémentaire adaptée au SPPC. Les gestionnaires sont responsables de s'assurer que les employés ont suivi la formation obligatoire. Les Ressources humaines assurent le suivi de la formation suivie par les employés et envisageront un processus permettant de fournir aux gestionnaires les données d'achèvement de la formation.	Directeur, Sécurité et gestion des installations et Directeur, Programme de coordination des	30 novembre 2025

	sensible contenue dans les dossiers de poursuite du SPPC.		Actions à prendre : • Les informations sur la formation et les guides disponibles sur iNet seront inclus dans le plan de communication. • Les mandataires seront informés qu'ils sont tenus de suivre le cours COR310. La section 7.2 du contrat d'agent sera modifiée. Les unités régionales de supervision des mandataires surveilleront pour l'achèvement.	mandataires	
4	Le directeur adjoint des poursuites pénales et le directeur général principal des Services ministériels devraient envisager la mise en œuvre des solutions numériques sécurisées pour le transfert d'informations, afin d'améliorer l'efficience et de réduire le risque pour le SPPC résultant d'actions non conformes.	Moyen	La direction approuve cette recommandation. Actions à prendre : • Le chef de la sécurité collaborera avec nos partenaires, Services partagés Canada et le Centre de la sécurité des télécommunications, afin de trouver des solutions numériques pour un réseau sécurisé distinct. Cela permettrait au SPPC d'envoyer, de recevoir, de consulter et de manipuler des informations protégés C, secrets, très secrets et SIGNIT au sein du gouvernement du Canada et avec des organismes d'enquête (ex. : la GRC, le ministère des Pêches et des Océans, Environnement et Changement climatique Canada, l'Agence des services frontaliers du Canada, Justice Canada), y compris les courriels sécurisés, le transfert de données et le stockage numérique des informations hautement classifiés. • Étant donné que ce travail nécessitera un financement, des options seront déterminées et un dossier conceptuel sera soumis à la décision du Comité des hauts responsables. • Déterminer des solutions, dans le cadre du projet de divulgation électronique, qui nous permettront de recueillir des éléments de preuve auprès des organismes d'enquête, de les partager avec les avocats de la défense et de les stocker, jusqu'au niveau Protégé B.	Directeur, Sécurité et gestion des installations	31 mars 2026
5	Le directeur adjoint des poursuites pénales et le directeur général principal des Services ministériels doivent veiller à la connaissance des exigences du CT, relativement à la délivrance d'attestations de sécurité d'un niveau qui correspond aux fonctions exercées. Il faut notamment veiller à ce que le niveau des attestations de sécurité délivrées soit en conformité avec les fonctions exercées et à ce que les attestations soient mises à jour selon la Norme sur le filtrage de sécurité du CT (cycle de mise à jour, section 5, annexe B).	Élevé	La direction approuve cette recommandation. Une nouvelle directive sur le filtrage de sécurité est entrée en vigueur le 6 janvier 2025, ce qui nécessite une mise à jour des niveaux de sécurité pour de nombreux employés du SPPC. Le SCT a prévu deux ans pour la mise en œuvre. Actions à prendre : • De l'information sera communiquée aux gestionnaires concernant les niveaux de sécurité - à la fois les changements qui découleront de la Directive et un rappel de n'assigner du travail qu'en fonction du niveau d'autorisation de sécurité de l'employé. • Des instructions seront fournies aux gestionnaires pour qu'ils examinent les niveaux de sécurité de tous les postes.	Directeur, Sécurité et gestion des installations	6 avril 2027

			• Un nouvel outil sera mis en œuvre pour déterminer le niveau de sécurité requis pour tout nouveau poste. • Les courriels de rappel de PeopleSoft seront mis à jour pour inclure un avertissement concernant la gravité du non-renouvellement de l'habilitation de sécurité. • Les gestionnaires des employés dont l'habilitation est en retard seront inclus dans les courriels de rappel générés par PeopleSoft. • Pour ceux qui approchent de la date de renouvellement et qui n'ont pas agi, l'équipe de sécurité transmettra leur dossier à leur supérieur hiérarchique (délai de notification à déterminer).		

ANNEXE A – RENSEIGNEMENTS SUR L'AUDIT

Énoncé 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 horizontal visait les informations Protégé C, Secret et Très secret, contenus dans les dossiers de poursuite, traités par les employés du SPPC et les mandataires de tous les bureaux du SPPC, à l'exception de ceux installés dans les régions du Nord (Nunavut, Territoire du Nord-Ouest et Yukon).

Méthodologie

Les activités suivantes s'inscrivent dans la méthodologie appliquée :

- entretiens et sondages menés auprès des employés de l'administration centrale, du personnel et de la direction des régions et des membres des équipes de supervision des mandataires;
- sondages menés auprès des mandataires;
- examen et analyse de données et des politiques, pratiques, procédures et directives consignées.

Critères de l'audit

1	Le SPPC a mis en œuvre un cadre défini et consigné afin de soutenir la gestion adéquate de l'information sensible (Protégé C et niveaux supérieurs).
2	L'organisme dispose d'installations et d'outils et exerce une surveillance aux fins de la gestion efficace et efficiente de l'information sensible.
3	Des programmes de formation et de sensibilisation sont mis en œuvre de manière efficace pour améliorer la compréhension et les connaissances des employés et des mandataires à l'égard de leurs responsabilités en matière de protection de l'information sensible.

ANNEXE B – LISTE DES ACRONYMES/ABRÉVIATIONS

AIPRP	Accès à l'information et protection des renseignements personnels
ESM	Équipes de supervision des mandataires
SPPC	Service des poursuites pénales du Canada
CT	Conseil du Trésor du Canada