Audit de la gestion de la sécurité matérielle

Division de l'audit interne
Conseil de recherches en sciences naturelles et en génie du Canada
Conseil de recherches en sciences humaines du Canada

Approuvé par le président le 18 mars 2015

N^{o} de catalogue CR22-50/2015F-PDF
ISBN 978-0-660-03877-3

TABLE DES MATIÈRES

Ceci est une version abrégée du rapport d'audit. La publication de l'information contenue dans la version complète du rapport peut représenter une menace et un risque pour la sécurité du

CRSNG ou du CRSH. L'information a été retenue en vertu de l'article 16(2)(c) de la *Loi sur l'accès à l'information*.

1 CONTEXTE

Le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG) et le Conseil de recherches en sciences humaines du Canada (CRSH)[1] appuient la réalisation de travaux érudits dans les établissements d'enseignement postsecondaire du Canada et relèvent du Parlement par l'entremise du ministre de l'Industrie. La fonction de sécurité matérielle est exercée au sein de la Direction des services administratifs communs (DSAC), qui épaule les deux organismes. L'équipe des Services de sécurité comprend deux employés, soit l'agent de sécurité de l'organisme (l'ASO) et l'ASO adjoint. L'ASO relève du dirigeant principal de l'information (DPI) et du vice-président de la DSAC par l'intermédiaire du dirigeant principal adjoint de l'information.

La Politique sur la sécurité du gouvernement publiée par le Secrétariat du Conseil du Trésor (SCT) définit la sécurité matérielle comme étant « l'assurance que l'information, les biens et les services ne sont pas compromis et que les personnes sont protégées contre la violence en milieu de travail[2] » et indique que les ministères et organismes doivent mettre en œuvre un programme de sécurité en vue d'obtenir les résultats suivants[3] :

- l'information, les biens et les services ne sont pas compromis et les employés sont protégés contre la violence en milieu de travail;
- les structures, mécanismes et ressources de gouvernance sont en place pour assurer la gestion efficace et efficiente de la sécurité, tant au sein d'un ministère que dans l'ensemble du gouvernement;
- la gestion des incidents de sécurité est efficacement coordonnée au sein des ministères et dans l'ensemble du gouvernement;
- l'interopérabilité et l'échange de renseignements sont assurés au moyen de pratiques efficaces et uniformes de gestion de la sécurité et de l'identité;
- la continuité des activités et des services du gouvernement est assurée en cas d'incidents de la sécurité, de perturbations ou de situations d'urgence.

Les organisations doivent s'assurer que la gestion de la sécurité est concertée, coordonnée et surveillée, établir un cadre réunissant les diverses fonctions responsables des éléments de la sécurité[4] et veiller à ce que tous les employés, à tous les échelons de l'organisation, connaissent et comprennent leurs responsabilités[5]. Le succès global d'un programme de gestion de la sécurité d'une organisation repose sur l'efficacité de la planification, de la communication, de la collaboration à l'échelle de l'organisation et de la surveillance.

2 JUSTIFICATION DE L'AUDIT

Dans le cadre du processus de planification de l'audit interne basé sur le risque, la Division de l'audit interne (DAI) a déterminé que la fonction de sécurité matérielle nécessite un examen. L'audit était prévu dans le Plan d'audit axé sur les risques de 2014-2017 (PAAR) car :

[1] Dans les rapports, le CRSNG et le CRSH sont appelés « les organismes ».
[2] Politique sur la sécurité du gouvernement, le 1er juillet 2009, section 3.1.
[3] Politique sur la sécurité du gouvernement, le 1er juillet 2009, section 5.2.
[4] Politique sur la sécurité du gouvernement, le 1er juillet 2009, section 3.3.
[5] Directive sur la gestion de la sécurité ministérielle, le 1er juillet 2009, section 6.1.2.

- les organismes n'avaient jamais effectué d'audit de la sécurité matérielle;
- la Politique sur la sécurité du gouvernement du SCT précise que tous les ministères et organismes doivent examiner leur conformité périodiquement;
- l'audit était mentionné dans le PAAR de 2014-2017 du CRSNG et du CRSH, lequel avait été approuvé par les présidents en mars 2014.

3 OBJECTIF ET PORTÉE DE L'AUDIT

Objectif

Cet audit vise à donner l'assurance que les pratiques de gouvernance et de gestion du risque et les contrôles internes concernant la gestion de la sécurité matérielle sont adéquates et efficaces. L'audit a évalué l'efficacité et la pertinence des mesures de sécurité et des contrôles de gestion mis en place par les organismes. Il comprend une évaluation :

- de la gouvernance, des rôles et des responsabilités de toutes les parties concernées;
- des processus et des pratiques de gestion des risques d'atteinte à la sécurité matérielle;
- de l'accès physique aux installations, à l'information et aux biens;
- de la sensibilisation et de la conformité des employés aux politiques et directives sur la sécurité matérielle.

Portée

L'audit visait toutes les installations de l'administration centrale du CRSNG et du CRSH situées à Constitution Square au centre-ville d'Ottawa ainsi que deux des cinq bureaux régionaux du CRSNG. Il visait également l'information et les biens s'y trouvant. L'audit ne portait ni sur la conformité au *Règlement sur la santé et la sécurité au travail* ni sur les pratiques, contrôles et processus en matière de sécurité gérés par les responsables des bâtiments qui abritent le CRSNG et le CRSH.

4 MÉTHODE DE L'AUDIT

L'audit a été mené conformément aux Normes internationales pour la pratique professionnelle de l'audit interne de l'Institut des auditeurs internes (IAI), énoncées dans le Cadre international de référence des pratiques professionnelles (CIPP), et conformément aux Normes relatives à la vérification interne au sein du gouvernement du Canada, appuyées par les résultats du programme d'assurance et d'amélioration de la qualité.

L'étape de planification de l'audit comprenait des entrevues préliminaires ainsi que la collecte et l'examen des documents pour comprendre l'état actuel de la gestion de la sécurité au sein des organismes. Le programme d'audit, y compris les procédures et les critères d'audit détaillés, a ensuite été conçu à la lumière de l'information recueillie au cours de la planification. Il était axé sur les objectifs et les secteurs d'intérêt susmentionnés.

Par la suite, à l'étape de l'audit proprement dit, les auditeurs ont interrogé les spécialistes de la sécurité, les gestionnaires de programme et les employés; vérifié les mesures de protection matérielle dans différents secteurs et endroits; et examiné et évalué les pratiques actuelles en matière de sécurité par rapport aux pratiques exemplaires et aux orientations fournies par le SCT.

5 ÉQUIPE DE L'AUDIT

Dirigeant principal de l'audit : Benjamin Cyr

Responsable de l'audit : Patricia Morrell

6 RÉPONSE DE LA DIRECTION AUX RECOMMANDATIONS DE L'AUDIT

POINT	RECOMMANDATION	PLAN D'ACTION	DATE CIBLE
1.	Il est recommandé aux organismes de s'assurer que l'ASO coordonne le programme de sécurité et les divers secteurs fonctionnels responsables de la sécurité et d'officialiser son rôle dans la gouvernance et la supervision du programme de sécurité.	Acceptée. Les Solutions d'information et d'innovation (SII) examineront et officialiseront le rôle de l'ASO dans la gouvernance et la supervision du programme de sécurité afin d'assurer une coordination efficace de ce programme, notamment les secteurs fonctionnels de la sécurité.	Septembre 2015
2.	Il est recommandé aux organismes de mettre d'abord à jour leurs évaluations de la conjoncture, de la menace et des risques de manière à valider ou à cerner les principaux risques ou menaces pour leur environnement opérationnel (y compris les bureaux satellites) puis d'élaborer, d'achever et de mettre en œuvre un Plan de sécurité de l'organisme et d'autres documents et plans comme le Plan de continuité des activités et le Plan de reprise après sinistre.	Acceptée. Dans le cadre du Plan de sécurité de l'organisme (PSO), les SII valident les menaces et les risques cernés dans les évaluations des menaces et des risques (EMR) antérieures et effectuent une analyse de la conjoncture afin de mieux définir les menaces et les risques pour les organismes dans l'environnement de sécurité actuel. Le PSO a indiqué que l'achèvement des EMS des bureaux régionaux constitue une importante activité d'atténuation des risques pour la sécurité en 2015-2016. Les recommandations découlant du PSO et des EMR permettront de mettre à jour des documents clés sur la sécurité des organismes, notamment le PCA et le PRAS.	Achèvement du PSO : avril 2015 Achèvement des EMR des bureaux régionaux : mars 2016

3.	Il est recommandé aux organismes de veiller à mener des enquêtes de sécurité conformément aux exigences énoncées dans la Politique sur la sécurité du gouvernement, qui définit les exigences s'appliquant non seulement aux employés, mais aussi aux tiers ayant accès aux installations, aux biens et à l'information.	Acceptée. Les SII présenteront des options aux comités de gestion des organismes pour s'assurer que les organismes mènent des enquêtes de sécurité du personnel conformément à la Politique sur la sécurité du gouvernement tout en continuant de satisfaire aux exigences opérationnelles des organismes.	Septembre 2015
4.	Il est recommandé aux organismes d'effectuer une évaluation officielle de la menace et des risques pour toutes les installations (y compris les bureaux régionaux) afin de s'assurer que les contrôles de l'accès et les outils de surveillance sont déployés dans les secteurs en fonction du niveau de risque ou des besoins liés au degré de sensibilité.	Acceptée. Les SII effectueront une EMR dans les environnements physiques (notamment les bureaux régionaux du CRSNG) pour s'assurer que les organismes mettent en œuvre des contrôles et mesures de sécurité matérielle conformément au niveau de risque et aux exigences relatives aux zones d'accès contrôlé.	Mars 2016
5.	Il est recommandé aux organismes d'examiner et de mettre en œuvre les directives et processus pour l'étiquetage, le traitement et la protection de leurs données et de leurs dossiers électroniques et papier.	Acceptée. Les SII examineront les lignes directrices en vigueur sur la classification de l'information pour les besoins de la sécurité et passeront en revue diverses approches de mise en œuvre pour maximiser le résultat.	Mars 2016
6.	Il est recommandé aux organismes de s'assurer que les exigences en matière de gestion et de protection des données et de l'information de tiers sont clairement définies dans les accords sur les niveaux de service et les protocoles d'entente conclus avec d'autres organismes.	Acceptée. Les SII élaboreront un processus et mettront en œuvre une procédure pour s'assurer que les ententes conclues avec d'autres organisations (c'est-à-dire ENS et protocoles d'entente) prévoient des exigences en matière de sécurité pour gérer et protéger les données et l'information des tiers.	Mars 2016

7.	Il est recommandé aux organismes d'élaborer une directive claire sur la gestion des biens (notamment la reddition de comptes, les processus, les procédures et les lignes directrices) et de mettre en œuvre un système central ou intégré permettant la gestion adéquate des biens à toutes les étapes de leur cycle de vie (achat, inscription à l'inventaire, attribution, récupération, élimination, etc.).	Acceptée. La Division des finances et de l'administration des octrois élaborera un processus de gestion des biens permettant une gestion adéquate des biens à toutes les étapes de leur cycle de vie. Les procédures élaborées dans le cadre de ce processus définiront clairement les rôles et responsabilités concernant l'établissement des obligations redditionnelles, les types de biens assujettis à la politique ainsi que les moyens et la fréquence du suivi à l'aide du nouveau système centralisé.	Mars 2016
8.	Il est recommandé aux organismes d'élaborer et de mettre en œuvre un programme obligatoire de sensibilisation à la sécurité conforme au PSO (une fois que sa version finale aura été établie) faisant état des exigences des organismes en matière de sécurité et des risques liés aux activités, aux installations, aux biens et à l'information	Acceptée. Les SII élaboreront et mettront en œuvre un vaste programme obligatoire de sensibilisation à la sécurité adapté aux besoins des organismes en matière de sécurité et à leurs niveaux de risque.	Septembre 2016

7 ANNEXE I – Critères de l'audit

Les critères de l'audit ont été établis d'après la Politique sur la sécurité du gouvernement (2009) et de la Directive ministérielle sur la gestion de la sécurité (2009) du SCT et les Contrôles de gestion de base du BCG (2011).

1. **Les rôles et les responsabilités en matière de sécurité matérielle sont clairement définis et assumés par l'employé concerné; et l'information ou les problèmes sont communiqués à l'échelon approprié.**
   - La structure de gouvernance à l'appui de la gestion de la sécurité matérielle est clairement définie et respectée.
   - Les rôles et les responsabilités des personnes chargées de la gestion de la sécurité matérielle sont clairement définis et couvrent tous les aspects obligatoires.
   - Les rôles et les responsabilités des comités et de la haute direction relativement à la sécurité matérielle sont définis, documentés et assumés.
   - L'information sur la sécurité matérielle, les rapports d'incident et les résultats des évaluations sont communiqués à la direction ou aux comités de gestion, qui en assurent la surveillance, aux fins de discussion ou de décision.

2. **L'accès physique aux installations, aux biens et à l'information des organismes est limité aux personnes autorisées qui ont fait l'objet d'une enquête de sécurité au niveau approprié et qui ont besoin de cet accès.**
   - Des périmètres et des zones d'accès réservé ont été déterminés et sont dûment contrôlés.
   - Les organismes limitent aux personnes compétentes et autorisées l'accès aux biens et ont mis en place des contrôles pour protéger ces biens.
   - Les organismes ont établi un protocole de classification de l'information pour relever, étiqueter et stocker adéquatement l'information sensible et protégée.
   - Les personnes qui ont accès à l'information classifiée, aux biens et aux zones d'accès contrôlé font l'objet d'une enquête de sécurité et leur accès est fonction de leur cote de sécurité et de leurs besoins.
   - Les organismes ont établi des procédures, des lignes directrices et des mécanismes de surveillance de la sécurité (information, biens et locaux) à l'appui d'une saine gestion de la sécurité matérielle dans les bureaux satellites et dans le cadre du télétravail.
   - Le niveau de sécurité des réseaux des organismes permet de protéger adéquatement les fonds de renseignements.

3. **Les employés connaissent et assument leurs rôles et leurs responsabilités en matière de sécurité matérielle.**
   - Les employés des organismes connaissent les exigences en matière de sécurité matérielle.
   - Les employés des organismes, à tous les échelons, comprennent et assument complètement leurs rôles et leurs responsabilités en matière de sécurité matérielle.
   - L'information sur la sécurité matérielle est disponible et communiquée régulièrement à l'ensemble des employés.
   - Le respect des exigences en matière de sécurité matérielle est surveillé et les problèmes sont réglés.

4. **Des processus adéquats et efficaces sont en place pour cerner les menaces et gérer les risques pour la sécurité matérielle et ils fonctionnent comme prévu.**
   - Les organismes ont défini et documenté un processus de gestion des risques d'atteinte à la sécurité matérielle.

- Le processus de gestion des risques est continu et les menaces ou risques éventuels font l'objet d'une surveillance systématique visant à s'assurer que l'on donne suite aux risques émergents.
- Les risques ou menaces pour la sécurité matérielle cernés antérieurement ont été communiqués à la haute direction et analysés et des mesures adéquates ont été prises pour les gérer.
- Les organismes ont approuvé des plans de sécurité interne documentés qu'ils passent régulièrement en revue pour s'assurer qu'ils demeurent pertinents et à jour.

8 ANNEXE II – Définitions

On trouvera des variantes des définitions des termes suivants dans les politiques, directives, normes et guides du SCT ainsi que dans le Guide pour la planification de la gestion des urgences 2010-2011 publié par Sécurité publique Canada.

Analyse de la conjoncture : Processus d'identification des principaux facteurs et risques internes et externes qui influent sur le programme de politiques et de gestion d'une organisation.

Évaluation des risques : Processus consistant à recueillir de l'information et à attribuer une valeur aux risques en vue de documenter les priorités, d'élaborer ou de comparer des plans d'action et de renseigner les décideurs.

Évaluation des menaces : Processus d'identification ou d'évaluation d'entités, des mesures ou des cas, qu'ils soient naturels ou causés par l'homme, qui ont nui ou pourraient nuire à la vie, à l'information, aux activités ou aux biens.

Évaluation des menaces et des risques (EMR) : Processus consistant :

- à recenser les biens et les ressources et à évaluer le niveau de risque connexe;
- à évaluer les menaces, notamment la motivation, l'intention et la capacité d'un agent de menace et la possibilité, la probabilité et la conséquence des actes de menace qui pourraient poser un risque pour les services essentiels;
- à examiner et à évaluer les interruptions possibles et les événements en vue de déterminer les vulnérabilités et la mise en œuvre de contre-mesures afin de les atténuer.

Analyse des répercussions sur les activités (ARA) : Processus consistant à analyser la mesure dans laquelle un ministère est exposé à des risques et à des répercussions susceptibles d'entraver son fonctionnement ou sa capacité d'assurer en continu les services essentiels. Le processus comprend plusieurs étapes : déterminer les services essentiels et les priorités qui s'y rapportent; déterminer les niveaux de service minimaux et les temps d'arrêt maximaux autorisés; schématiser les dépendances à l'égard des services essentiels; évaluer les risques et les capacités de reprise des activités; et formuler des stratégies de reprise des activités.

Plan de sécurité de l'organisme (PSO) : Plan énonçant en détail les décisions de gestion des risques d'atteinte à la sécurité et définissant les stratégies, les buts, les objectifs, les priorités et les délais pour améliorer la sécurité de l'organisme et appuyer sa mise en œuvre.

Planification de la continuité des activités (PCA) : Élaboration et exécution en temps opportun de plans, de mesures, de procédures et d'ententes visant à éviter ou à réduire toute interruption des services et de la disponibilité de biens essentiels. Le programme de PCA comprend quatre étapes :

- établissement de la gouvernance du programme de PCA;
- conduite d'une ARA;
- élaboration de plans de continuité des activités et d'ententes;
- maintien de l'état de préparation du programme de PCA.

Plan de gestion des urgences (PGU) : Élaboration et mise en œuvre de plans pour gérer les situations d'urgence concernant tous les dangers, notamment toutes les activités et les mesures de gestion des risques se rapportant à la prévention, à l'atténuation, à l'état de préparation, à l'intervention et à la reprise des activités.