VÉRIFICATION DE LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

Division de la vérification interne
Conseil de recherches en sciences naturelles et en génie du Canada
Conseil de recherches en sciences humaines du Canada
20 septembre 2012

Table des matières

1 Sommaire

1.1 Introduction

Le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG) et le Conseil de recherches en sciences humaines du Canada (CRSH) (ci-après les « organismes ») sont deux organismes fédéraux épaulés par la Direction des services administratifs communs (DSAC), qui gère pour leur compte les technologies de l'information (TI) et la sécurité des TI. Les organismes sont assujettis à la Politique sur la sécurité du gouvernement du Conseil du Trésor et à ses directives, normes et lignes directrices connexes qui indiquent que l'information, les biens et les services ne doivent pas être compromis.

Une vérification de la sécurité des TI des organismes a été réalisée pour les raisons suivantes :

- La sécurité des TI figurait parmi les aspects nécessitant un examen plus approfondi dans le plan de vérification interne axé sur les risques de 2011-2014;
- La Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) du Secrétariat du Conseil du Trésor (SCT) exige que la sécurité des TI soit incluse dans le plan de vérification interne axé sur les risques;
- Aucune vérification de la sécurité des TI n'a été réalisée au sein des organismes au cours des dix dernières années;
- Les conséquences d'une atteinte à la sécurité des TI pourraient être graves pour les organismes.

La présente vérification a porté sur le programme conjoint de sécurité des TI des organismes, notamment l'état du programme de sécurité des TI et les activités connexes entre le 1er avril 2011 et la fin du mois de décembre de la même année. La vérification a commencé par une évaluation globale de la sécurité des TI et une évaluation connexe des risques, à partir desquelles l'équipe de vérification a établi un plan de vérification mettant l'accent sur les éléments du programme comportant un risque plus élevé.

1.2 Contexte

Souvent, l'information est considérée comme un élément ou un bien indispensable pour la plupart, voire l'ensemble des organisations du fait que la majorité d'entre elles ne peuvent fonctionner si l'information manque ou si elle n'est pas fiable. De nos jours, la disponibilité, l'intégrité et la confidentialité de l'information sont au cœur des préoccupations, et c'est pourquoi les organismes sont assujettis à la Politique sur la sécurité du gouvernement (PSG) et à ses directives, normes et lignes directrices connexes.

Puisque les organismes mènent et continueront de mener de plus en plus leurs activités par voie électronique, ils ont manifestement fait d'énormes progrès pour ce qui est de renforcer les compétences entourant la sécurité des TI. Par exemple, les organismes ont récemment rédigé des politiques sur la sécurité des TI et ont acheté et mis en œuvre des outils automatisés pour améliorer continuellement leurs systèmes et les protéger

contre les failles de la sécurité. Il sera important que les organismes poursuivent dans la voie de l'amélioration continue de la sécurité des TI. Le présent rapport renferme des recommandations additionnelles à cet égard.

1.3 Objectifs et portée

La présente vérification interne visait à évaluer l'efficacité de certains contrôles de sécurité des TI des organismes et d'en rendre compte. Plus précisément, cette vérification donne une assurance quant à la pertinence et à l'efficacité des principaux contrôles de sécurité des TI en place au sein des organismes dans les domaines suivants :

- gouvernance du programme de sécurité des TI;
- cadre du programme de sécurité des TI;
- défense des frontières et du périmètre;
- contrôles d'accès logique et accès privilégié aux systèmes (p. ex., systèmes de gestion des octrois);
- processus de gestion des changements et des configurations;
- gestion des vulnérabilités;
- sécurité physique de la salle de serveurs.

1.4 Points forts

Les vérificateurs ont observé pendant la vérification plusieurs activités se rapportant au programme de sécurité des TI qui découlaient de l'importance accrue accordée par les organismes à la sécurité des TI. Au nombre des points forts en matière de sécurité des TI, mentionnons les suivants :

- Rédaction d'une politique et d'une directive sur la sécurité des TI et amélioration d'autres documents sur la sécurité;
- Création d'un poste d'agent ministériel de la sécurité (AMS);
- Réalisation d'examens indépendants de la sécurité pendant la période de vérification, notamment une évaluation indépendante de la sécurité par la Division de la technologie de l'information et des services de soutien (TISS) en avril 2011 et une évaluation de la protection et de la sécurité des biens des organismes en décembre 2011;
- Importantes améliorations à la gestion des correctifs;
- Établissement du Comité de contrôle des changements (CCC) officiel;
- Mise en place d'une politique exigeant que les changements susceptibles de compromettre la sécurité soient soumis à l'approbation du coordonnateur de la sécurité des TI;
- Mise en place d'une architecture de sécurité et d'un accès à distance protégé qui comprennent un pare-feu du périmètre configuré selon plusieurs zones, un service d'accès à distance (par l'entremise d'un réseau privé virtuel) qui exige

une authentification à deux facteurs et un système de détection des intrusions dans le réseau. Par ailleurs, la mise en œuvre d'une solution d'accès à distance plus récente et plus sûre était en cours au moment de la vérification;

- Procédures dûment documentées pour la gestion des utilisateurs réseau ou par accès à distance des applications du SIGBS ou d'AMIS[1];
- Adoption des principales pratiques relatives aux mots de passe de certains systèmes.

1.5 Principales constatations de la vérification

Même si les organismes ont récemment déployé des efforts en ce qui concerne la sécurité des TI, l'équipe de vérification a relevé quelques secteurs où elle recommande d'autres améliorations à cet égard :

Gouvernance du programme de sécurité des TI

Les postes d'agent ministériel de la sécurité et de coordonnateur de la sécurité des TI ont été créés; toutefois, il n'y a aucun comité de surveillance supérieur ni aucun conseil supérieur qui examine régulièrement l'état et le rendement du programme de sécurité des TI. Les deux organismes n'ont établi aucun plan de sécurité des TI, alors que le Conseil du Trésor l'exige.

Cadre du programme de sécurité des TI

L'équipe de vérification a constaté qu'une politique sur la sécurité des TI et certains documents d'appui avaient été rédigés, mais qu'ils n'avaient pas été approuvés par la direction ou communiqués au personnel. Elle a remarqué par ailleurs l'absence d'un cadre global définissant les volets du programme de sécurité des TI. Les procédures, directives et normes connexes n'ont pas été définies. Pour l'instant, elles sont officieuses ou inexistantes.

Processus et procédures officiels en matière de sécurité des TI

Les vérificateurs ont constaté que des processus et procédures non officiels sont en place dans de nombreux domaines, notamment la défense des frontières et du périmètre, le contrôle de l'accès et la gestion des changements et des configurations.

Les organismes ont mis en place quelques procédures rigoureusement documentées comme la gestion des utilisateurs réseau ou par accès à distance des applications du SIGSB ou d'AMIS. Lorsque des procédures officielles sont en place et que des contrôles internes ont été mis en œuvre, les vérificateurs ont remarqué que l'on ne conserve pas toujours les données confirmant que les procédures ont été suivies. Sans documents adéquats montrant la piste de vérification, il est difficile de déterminer si les contrôles fonctionnent comme prévu.

[1] SIGSB : Système informatisé de gestion des subventions et bourses du CRSNG; AMIS : Système informatisé de gestion des subventions et bourses du CRSH.

Contrôles de l’accès

L’équipe de vérification a relevé des possibilités d’amélioration dans le domaine du contrôle de l’accès. Pour certains systèmes, les processus en place pour la gestion des utilisateurs sont non officiels. Dans d’autres cas, les procédures officielles ont été documentées, mais l’équipe a remarqué qu’elles n’étaient pas suivies systématiquement. Les vérifications effectuées sur des échantillons ont mis au jour des exemples de documents inadéquats pour corroborer l’approbation de l’accès accordé aux utilisateurs, notamment les utilisateurs privilégiés, et des comptes d’employés ayant quitté leur emploi qui n’avaient pas été supprimés dans les délais requis. L’équipe de vérification a également constaté l’utilisation de comptes d’administrateur partagés. De plus, aucune norme officielle concernant les mots de passe n’était en place au sein des organismes. Par conséquent, la fiabilité des mots de passe (longueur minimale, complexité, délai d’expiration, etc.) variait d’un système à l’autre. Pour certains systèmes, les paramètres des mots de passe respectaient les principales pratiques à cet égard. Outre l’accès logique, les vérificateurs ont relevé des possibilités d’amélioration dans les contrôles de l’accès physique visant la salle de serveurs.

Programme de gestion des vulnérabilités

L’équipe de vérification a constaté que d’importantes améliorations avaient été apportées récemment à la gestion des correctifs dans l’infrastructure, notamment la mise en œuvre d’un outil automatisé de gestion des correctifs. Elle a également observé qu’un programme non officiel de gestion des vulnérabilités était en place; toutefois, aucune suite n’avait été donnée à une cyberalerte importante, en partie à cause d’un manque de communication entre le personnel responsable de la sécurité et des gestionnaires de la TI. Par ailleurs, aucune preuve n’a pu être fournie pour déterminer si l’on avait donné suite à des cyberavertissements particuliers. Aucun programme interne d’évaluation technique de la vulnérabilité n’a été mené pendant la vérification et on ne disposait d’aucune donnée faisant état de procédures, de constatations ou de mesures correctives connexes.

1.6 Recommandations

1. Nous recommandons aux organismes de réexaminer la structure de gouvernance du programme de sécurité des TI et d’inclure la surveillance du programme par la haute direction dans le mandat de l’un des organes de surveillance ou comités supérieurs en place. Celui-ci devra examiner régulièrement les priorités, les plans et le rendement en matière de sécurité des TI et faire valoir l’importance de la fonction pour l’organisme. De plus, nous recommandons qu’un plan de sécurité de l’organisme soit élaboré, comme l’exige la Directive sur la gestion de la sécurité ministérielle du Conseil du Trésor, et qu’il prévoie des examens systématiques du programme de sécurité des TI.
2. Nous recommandons aux organismes de peaufiner, d’approuver et de communiquer la politique sur la sécurité des TI à tous les employés comme prévu par la direction. Par ailleurs, nous leur recommandons d’examiner minutieusement leur cadre de sécurité des TI, à savoir la politique sur la sécurité des TI, les directives, les normes et les lignes directrices ainsi que les

procédures et les processus requis pour les mettre en œuvre dans le contexte opérationnel des organismes. Cet examen devrait être réalisé dans le contexte des dernières politiques, directives, normes et lignes directrices des organismes principaux responsables de la sécurité et du Conseil du Trésor. De plus, il devrait vérifier que les objectifs de contrôle de la sécurité, les contrôles ainsi que la gestion des risques sont intégrés au programme de sécurité des TI des organismes.

3. Nous recommandons aux organismes d'officialiser leurs mécanismes de gestion de la sécurité et de changement, et d'élaborer des documents sur la procédure à suivre à l'appui des activités afin d'avoir l'assurance que les processus et procédures sont suivis systématiquement. De plus, nous recommandons de conserver la documentation des contrôles clés (p. ex., approbations, examens de la sécurité et documentation de la gestion des changements) pour les besoins de la piste de vérification.
4. Nous recommandons aux organismes d'officialiser toutes les procédures de gestion des utilisateurs, y compris celles concernant l'accès physique, et de communiquer au personnel les procédures en place afin d'assurer leur respect systématique. Les procédures de gestion des utilisateurs devraient exiger un examen périodique de tous les comptes et documenter l'utilisation des comptes privilégiés et d'administrateur. De plus, il faudrait définir une norme régissant les mots de passe qui soit conforme aux principales pratiques à cet égard, passer en revue les mots de passe existants et faire en sorte qu'ils soient conformes à cette norme. Il faudrait aussi élaborer et mettre en œuvre une procédure de surveillance de l'accès physique à la salle de serveurs.
5. Nous recommandons aux organismes d'examiner le processus de gestion des vulnérabilités et de l'harmoniser avec les principales pratiques à cet égard, notamment le processus d'élévation des privilèges et de communication des vulnérabilités ainsi que de documentation des décisions en matière de gestion des risques. Le processus d'évaluation technique de la vulnérabilité devrait également être examiné, officialisé et appliqué de façon régulière. Il faudrait conserver les données probantes témoignant de l'évaluation et du suivi de la vulnérabilité pour les besoins de la piste de vérification. Par ailleurs, nous recommandons d'examiner le processus de gestion des correctifs, de l'officialiser et de l'étendre à toutes les composantes du réseau et à tous les systèmes d'application.

1.7 Conclusion

Les organismes déploient des efforts dans le domaine de la sécurité des TI et apportent actuellement plusieurs améliorations à leur programme de sécurité des TI. Néanmoins, il convient de souligner que le programme exige des éléments de gouvernance cruciaux, une politique complète et un cadre de gestion, et requiert l'officialisation et la documentation des processus et procédures non officiels afin de réduire le risque d'atteinte à la sécurité des TI.

2 À propos de la vérification

2.1 Contexte

Une vérification de la sécurité des TI des organismes a été réalisée pour les raisons suivantes :

- La sécurité des TI figurait parmi les aspects nécessitant un examen plus approfondi dans le plan de vérification interne axé sur les risques de 2011-2014;
- La Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) du Secrétariat du Conseil du Trésor (SCT) exige que la sécurité des TI soit incluse dans le plan de vérification interne axé sur les risques;
- Aucune vérification de la sécurité des TI n'a été réalisée au sein des organismes au cours des dix dernières années;
- Les conséquences d'une atteinte à la sécurité des TI pourraient être graves pour les organismes.

Les organismes sont assujettis à la Politique sur la sécurité du gouvernement (PSG) du Conseil du Trésor et à ses directives, normes et lignes directrices connexes. La PSG requiert la protection de l'information, des biens et des services contre toute compromission et celle des personnes contre la violence en milieu de travail.

En vertu de la PSG et des directives et lignes directrices connexes, la gestion de la sécurité exige une évaluation continue des risques ainsi que la mise en place, la surveillance et le maintien de mécanismes appropriés de contrôle de gestion interne en matière de prévention (atténuation), de détection, d'intervention ou de rétablissement. La gestion de la sécurité recoupe d'autres fonctions de gestion, dont l'accès à l'information, la protection des renseignements personnels, la gestion du risque, la gestion des urgences et de la continuité des activités, les ressources humaines, la santé et la sécurité au travail, l'immobilier, la gestion du matériel, la gestion de l'information, les technologies de l'information et les finances. La sécurité est assurée lorsqu'elle est appuyée par la haute direction, une dimension qui fait partie intégrante de la planification stratégique et opérationnelle, et qu'elle est intégrée aux cadres, à la culture, aux activités courantes des organismes et aux comportements des employés.

La PSG inclut des documents clés normatifs comme la Directive sur la gestion de la sécurité ministérielle (2009) et la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) du Conseil du Trésor ainsi que d'autres directives, normes et lignes directrices fédérales.

La Directive sur la gestion de la sécurité ministérielle définit les rôles et les responsabilités des fonctionnaires de ministères qui assistent les administrateurs généraux dans la gestion de la sécurité ministérielle. Ces responsabilités sont à la base d'un processus décisionnel et redditionnel efficace lié aux activités de sécurité ministérielle. Cette directive établit aussi les objectifs minimaux de contrôle de la sécurité qu'un ministère doit atteindre pour s'assurer de remplir son mandat, de mener ses activités et de respecter ses priorités et exigences en matière de sécurité.

La sécurité des TI devient, sans aucun doute, l'un des éléments les plus importants de la planification et de la mise en œuvre des TI. Comme les organismes mènent et continueront de mener de plus en plus leurs activités par voie électronique, ils accordent manifestement la priorité au renforcement des compétences entourant la sécurité des TI, ce qui a été mis en valeur au début de la présente vérification. Par exemple, les politiques sur la sécurité des TI viennent d'être rédigées, et certains outils automatisés ont été achetés et mis en œuvre pour aider à protéger les systèmes des organismes contre les vulnérabilités. Il sera important que les organismes poursuivent dans la voie de l'amélioration continue.

2.2 Objectif et portée

La présente vérification interne visait à évaluer l'efficacité de certains contrôles de sécurité des TI du CRSNG et du CRSH et d'en rendre compte. Plus précisément, cette vérification donne une assurance quant à la pertinence et à l'efficacité des principaux contrôles de sécurité des TI en place au sein des organismes dans les domaines suivants :

- gouvernance du programme de sécurité des TI;
- cadre du programme de sécurité des TI;
- défense des frontières et du périmètre;
- contrôles d'accès logique et accès privilégié aux systèmes (p. ex., systèmes de gestion des octrois);
- processus de gestion des changements et des configurations;
- gestion des vulnérabilités;
- sécurité physique de la salle de serveurs.

2.3 Méthode

L'équipe de vérification a utilisé une approche et une méthode conformes aux normes de vérification interne établies par l'Institut des vérificateurs internes et à la Politique de vérification interne du gouvernement du Canada.

La vérification a commencé par une étude préparatoire, dans le cadre de laquelle les vérificateurs ont réalisé des entrevues préliminaires et examiné des documents afin de comprendre l'état actuel des risques et des contrôles de la sécurité des TI. Cette étape a débouché sur une évaluation des risques pour la sécurité des TI.

Le programme de vérification, incluant des procédures et critères de vérification détaillés, a ensuite été conçu à la lumière de cette étude. Il portait sur les sept secteurs clés définis plus haut.

Outre la norme GSTI, l'établissement des critères de vérification a pris en compte les normes en vigueur dans l'industrie, notamment ISO 27002, laquelle constitue un code de pratique pour la sécurité de l'information qui établit des lignes directrices et des principes généraux pour amorcer, mettre en œuvre, maintenir et améliorer la gestion de la sécurité de l'information au sein d'une organisation. La norme fournit également des orientations pour l'élaboration de normes sur la sécurité organisationnelle et des pratiques de gestion efficace de la sécurité.

Les méthodes suivantes ont été utilisées pour recueillir des éléments probants :

- Entrevues et examen de la documentation;
- Recensement des contrôles internes clés et examen des processus de sécurité et des procédures de fonctionnement normalisées;
- Révision structurée des contrôles et processus clés;
- Vérification de l'efficacité opérationnelle des contrôles au moyen de requêtes, appuyée par l'observation et l'examen de la documentation.

L'application de ces procédures a permis de déterminer si les critères de vérification avaient été respectés, partiellement respectés ou n'avaient pas été respectés. Des données probantes ont été recueillies conformément à la politique, aux directives et aux normes du Conseil du Trésor sur la vérification interne, et les procédures employées étaient conformes aux normes professionnelles de l'Institut des vérificateurs internes. Les vérificateurs ont vérifié si l'information était suffisante, fiable, pertinente et utile, puis ils ont tiré des conclusions quant à la question de savoir si les preuves documentées répondaient aux objectifs de la vérification.

3 Observations et recommandations

3.1 Points forts

Les vérificateurs ont observé pendant la vérification plusieurs activités se rapportant au programme de sécurité des TI qui découlaient de l'importance accrue accordée par les organismes à la sécurité des TI. Au nombre des points forts en matière de sécurité des TI, mentionnons les suivants :

- Rédaction d'une politique et d'une directive sur la sécurité des TI et amélioration d'autres documents sur la sécurité;
- Création d'un poste d'agent ministériel de la sécurité (AMS);
- Réalisation d'examens indépendants de la sécurité pendant la période de vérification, notamment une évaluation indépendante de la sécurité par la Division de la technologie de l'information et des services de soutien (TISS) en avril 2011 et une évaluation de la protection et de la sécurité des biens des organismes en décembre 2011;
- Importantes améliorations à la gestion des correctifs;
- Établissement du comité de contrôle des changements(CCC) officiel;
- Mise en place d'une politique exigeant que les changements susceptibles de compromettre la sécurité soient soumis à l'approbation du coordonnateur de la sécurité des TI;
- Mise en place d'une architecture de sécurité et d'un accès à distance protégé qui comprennent un pare-feu du périmètre configuré selon plusieurs zones, un service d'accès à distance (par l'entremise d'un réseau privé virtuel) qui exige une authentification à deux facteurs et un système de détection des intrusions dans le réseau. Par ailleurs, la mise en œuvre d'une solution d'accès à distance plus récente et plus sûre était en cours au moment de la vérification;

- Procédures dûment documentées pour la gestion des utilisateurs réseau ou par accès à distance des applications du SIGBS ou d'AMIS;
- Adoption des principales pratiques relatives aux mots de passe de certains systèmes.

3.2 Améliorations à apporter

3.2.1 Gouvernance du programme de sécurité des TI

Afin de gérer efficacement les risques pour la sécurité, il faut établir une structure de gouvernance de la sécurité des TI, définir clairement les mandats et assurer une surveillance de la sécurité des TI, notamment l'examen des priorités, des plans et du rendement à cet égard. Par ailleurs, la Directive sur la gestion de la sécurité ministérielle du Secrétariat du Conseil du Trésor exige l'élaboration d'un plan de sécurité de l'organisme.

L'équipe de vérification a constaté qu'un coordonnateur de la sécurité des TI et qu'un agent ministériel de la sécurité avaient été nommés dans des documents préliminaires sur la sécurité. Toutefois, il n'existe aucun organe de surveillance de la haute direction qui se réunit régulièrement et examine l'information se rapportant aux priorités et aux plans liés à la sécurité des TI, fournit des avis sur des problèmes, examine le rendement de la fonction de sécurité des TI et communique ses décisions à l'organisme en temps opportun. Bien qu'il existe plusieurs comités de la haute direction, notamment le Comité directeur de GI-TI des deux Conseils, la responsabilité d'assurer la sécurité des TI ne relève pas de leur mandat. Même si l'élaboration d'un plan de sécurité de l'organisme est mentionnée dans un document préliminaire sur les priorités en matière de protection et de sécurité des biens, ce plan n'a pas été établi. En outre, certaines activités liées à l'examen de la sécurité des TI ont été entreprises (la plus récente étant une évaluation de la menace et des risques qui demeure préliminaire), mais aucun processus officiel n'est en place pour déterminer les types d'examens qui devraient être réalisés et leur fréquence.

Recommandation : Nous recommandons aux organismes de réexaminer la structure de gouvernance du programme de sécurité des TI et d'inclure la surveillance du programme par la haute direction dans le mandat de l'un des organes de surveillance ou comités supérieurs en place pour que celui-ci examine régulièrement les priorités, les plans et le rendement en matière de sécurité des TI et fasse valoir l'importance de la fonction pour l'organisme. De plus, nous recommandons qu'un plan de sécurité de l'organisme soit élaboré, comme l'exige la Directive sur la gestion de la sécurité ministérielle du Conseil du Trésor, et qu'il prévoie des examens systématiques du programme de sécurité des TI.

3.2.2 Cadre de sécurité des TI

Un cadre complet de sécurité des TI comprend une politique claire sur la sécurité des TI qui a été approuvée et qui est appuyée par des procédures, normes et directives clés et respecte la politique du Secrétariat du Conseil du Trésor. Les organismes ont une politique préliminaire sur la sécurité des TI mais elle n'a pas été approuvée par la direction ni communiquée à tous les employés. Cette politique n'inclut aucun cadre pour l'établissement d'objectifs en matière de contrôle de la sécurité des TI et la gestion des contrôles ou des risques. Par ailleurs, des directives, normes et procédures connexes

limitées ont été définies. Plus précisément, les processus et procédures requis à l'appui de la norme GSTI sont généralement non officiels ou non documentés. Il est possible d'améliorer les exigences en matière d'éducation, de formation ou de sensibilisation portant sur la sécurité, la gestion de la continuité des activités, la détermination des conséquences des infractions à la politique sur la sécurité de l'information et la définition des rôles et des responsabilités, notamment le signalement des incidents de sécurité.

Recommandation : Nous recommandons aux organismes de peaufiner, d'approuver et de communiquer la politique sur la sécurité des TI à tous les employés comme prévu par la direction. Par ailleurs, nous leur recommandons d'examiner minutieusement leur cadre de sécurité des TI, à savoir la politique sur la sécurité des TI, les directives, les normes et les lignes directrices ainsi que les procédures et les processus requis pour les mettre en œuvre dans le contexte opérationnel des organismes. Cet examen devrait être réalisé dans le contexte des dernières politiques, directives, normes et lignes directrices des principaux organismes responsables de la sécurité et du Conseil du Trésor. De plus, cet examen devrait vérifier que les objectifs de contrôle de la sécurité, et les contrôles eux-mêmes, ainsi que la gestion des risques sont intégrés au programme de sécurité des TI des organismes.

3.2.3 Procédures et processus officiels en matière de sécurité des TI

Les procédures et processus documentés officiels constituent un élément clé de la sécurité des TI, car ils contribuent à assurer le respect systématique des processus et la prise en charge des risques pour la sécurité. L'équipe de vérification a constaté que dans de nombreux domaines de la sécurité des TI, seuls des processus et procédures non officiels sont en place, notamment :

- le processus d'établissement et de maintien des frontières et du périmètre afin d'assurer la sécurité;
- le processus d'examen et d'approbation des répercussions des changements apportés à l'infrastructure sur la sécurité;
- les procédures et les listes de vérification pour l'administration des composantes de sécurité clés, comme les pare-feu;
- les lignes directrices sur le raffermissement des infrastructures;
- le processus d'évaluation technique de la vulnérabilité.

Le caractère non officiel et limité des processus et procédures accroît le risque d'erreurs de gestion ou d'omissions susceptibles de compromettre la sécurité des TI.

Les organismes ont mis en place certaines procédures documentées de manière officielle, notamment la gestion des utilisateurs réseau ou par accès à distance des applications du SIGSB ou d'AMIS. Dans les cas où des procédures officielles sont en place et où des contrôles internes ont été mis en œuvre, les vérificateurs ont constaté que les données confirmant le respect des procédures n'étaient pas toujours conservées. Voici des exemples relevés pendant la vérification :

- Une politique exige que les changements susceptibles de compromettre la sécurité soient soumis à l'approbation du coordonnateur de la sécurité des TI, mais les données probantes attestant les examens de la sécurité effectués par le coordonnateur ou l'approbation des changements n'ont pas pu être fournies pour un échantillon de changements à l'infrastructure et aux applications;

- Des procédures officielles de création de comptes sont en place pour le réseau et certaines applications, mais les données attestant l'approbation n'ont pu être fournies pour un échantillon de nouveaux comptes;
- Certaines évaluations techniques de la vulnérabilité sont réalisées, mais aucune donnée attestant ces évaluations et les mesures correctives prises n'a pu être fournie.

Sans documents suffisants à l'appui de la piste de vérification, il est difficile de déterminer si les contrôles fonctionnent comme prévu.

Recommandation : Nous recommandons aux organismes d'officialiser leurs processus de gestion de la sécurité et des changements, et d'élaborer des documents sur la procédure à suivre à l'appui des activités afin d'avoir l'assurance que les processus et procédures sont suivis systématiquement. De plus, nous recommandons de conserver la documentation des contrôles clés (p. ex., approbations, examens de la sécurité et documentation de la gestion des changements) pour les besoins de la piste de vérification.

3.2.4 Contrôles de l'accès

Les éléments clés d'un contrôle efficace de l'accès logique incluent un processus d'autorisation officielle pour accorder et retirer l'accès aux systèmes, un examen régulier de l'accès des utilisateurs aux systèmes, un contrôle des comptes d'administrateur et des paramètres de mot de passe rendant le mot de passe difficile à deviner conformément à la politique. Un contrôle efficace de l'accès physique comprend la restriction de l'accès à la salle de serveurs aux personnes autorisées et la surveillance de cet accès.

Les vérificateurs ont observé que les organismes utilisent des processus non officiels ou non documentés pour accorder et retirer l'accès à certains systèmes. Pour d'autres systèmes, des procédures officielles étaient documentées, mais l'équipe de vérification a constaté qu'elles n'étaient pas suivies systématiquement. La vérification effectuée sur des échantillons a mis au jour des cas d'approbation non documentée ou inadéquate à l'appui de l'accès accordé aux utilisateurs, notamment aux utilisateurs privilégiés, et des comptes appartenant à des employés ayant quitté leur emploi qui n'avaient pas été supprimés dans les délais requis. Par ailleurs, aucun examen régulier des comptes des utilisateurs et des privilèges d'accès n'était exigé, ce qui accroît le risque que l'accès non autorisé passe inaperçu. L'équipe de vérification a également constaté l'existence de comptes d'administrateur partagés et la possibilité d'accéder à la console de l'administrateur à partir de postes de travail non administratifs.

Par ailleurs, les organismes n'ont aucune norme officielle concernant les mots de passe. Une « norme » régissant les mots de passe figure dans un document sur la procédure à suivre, mais il est difficile de savoir si elle vise toutes les applications et l'infrastructure, puisqu'elle n'est pas définie dans le document. Par conséquent, les paramètres rendant les mots de passe difficiles à deviner (longueur minimale, complexité, délai d'expiration, etc.) varient en fonction des applications et de l'infrastructure. Même si certains systèmes vont au-delà des normes minimales ou utilisent des paramètres de mots de passe configurés conformément aux principales pratiques à cet égard, plusieurs autres ne les respectaient pas.

L'équipe de vérification a constaté que certains employés, de même qu'une société externe, avaient accès à la salle de serveurs malgré l'absence d'éléments prouvant

l'approbation de cet accès et qu'il n'existe aucun processus documenté concernant la suppression des droits d'accès à la salle de serveurs. De surcroît, cette salle et les alentours immédiats ne sont pas surveillés.

Recommandation : Nous recommandons aux organismes d'officialiser toutes les procédures de gestion des utilisateurs, y compris celles concernant l'accès physique, et de communiquer au personnel les procédures en place afin d'assurer leur respect systématique. Les procédures de gestion des utilisateurs devraient exiger un examen périodique de tous les comptes et documenter l'utilisation des comptes privilégiés et d'administrateur. De plus, il faudrait définir une norme régissant les mots de passe qui soit conforme aux principales pratiques, passer en revue les mots de passe existants et faire en sorte qu'ils soient conformes à cette norme. Il faudrait aussi élaborer et mettre en œuvre une procédure de surveillance de l'accès physique à la salle de serveurs.

3.2.5 Gestion des vulnérabilités

Les vulnérabilités devraient être gérées au moyen d'un processus de découverte continue et de mise en œuvre des solutions. Les vérificateurs ont constaté que même si les alertes de sécurité sont surveillées et que des mesures sont prises pour remédier aux vulnérabilités, il n'existe aucun registre des mesures prises en réponse aux cyberalertes et il n'a pas toujours été possible de déterminer si les mesures d'atténuation recommandées par les principaux organismes responsables de la sécurité[2] avaient été prises. Certaines alertes ou mesures d'atténuation dans les alertes pourraient facilement passer inaperçues. La vérification par sondages a mis en évidence un problème de sécurité critique auquel aucune suite n'a été donnée. Même si un processus de gestion des risques est énoncé dans le document sur la gouvernance de l'infrastructure de la Division de la technologie de l'information et des services de soutien (TISS), la documentation des décisions de gestion des risques se rapportant aux vulnérabilités ne fait l'objet d'aucune exigence particulière.

La Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) du Secrétariat du Conseil du Trésor indique qu'une évaluation de vulnérabilité (c'est-à-dire évaluation technique de la vulnérabilité) devrait être effectuée « régulièrement pour les systèmes très délicats ou assortis de risques importants, et à la discrétion [des ministères], pour les autres systèmes ». Même si le personnel responsable des TI a expliqué que la vulnérabilité était soumise périodiquement à une évaluation technique, l'équipe n'a observé pendant la vérification technique aucun processus ni aucun résultat de ces évaluations.

Les vérificateurs ont constaté que d'importantes améliorations avaient été apportées à la gestion des correctifs dans l'infrastructure, notamment la mise en œuvre d'un outil automatisé de gestion des correctifs. Cela étant dit, aucun correctif n'est actuellement appliqué à certaines composantes du réseau et les correctifs ne sont pas appliqués de manière régulière aux applications.

Recommandation : Nous recommandons aux organismes d'examiner le processus de gestion des vulnérabilités et de l'harmoniser avec les principales pratiques à cet égard, notamment le processus d'acheminement et de communication des vulnérabilités ainsi que de documentation des décisions en matière de gestion des risques. Le processus

[2] Le rôle des principaux organismes responsables de la sécurité est défini dans la Politique sur la sécurité du gouvernement. Ils fournissent des conseils, de l'orientation et des services pour appuyer les activités courantes de sécurité des ministères et organismes. Mentionnons notamment le Centre de la sécurité des télécommunications Canada et Sécurité publique Canada.

d’évaluation technique de la vulnérabilité devrait également être examiné, officialisé et appliqué de façon régulière. Il faudrait conserver les données probantes témoignant de l’évaluation et du suivi de la vulnérabilité pour les besoins de la piste de vérification. Par ailleurs, nous recommandons d’examiner le processus de gestion des correctifs, de l’officialiser et de l’étendre à toutes les composantes du réseau et à tous les systèmes d’application.

4 Conclusion

Les organismes déploient des efforts dans le domaine de la sécurité des TI et apportent actuellement plusieurs améliorations à leur programme de sécurité des TI. Néanmoins, il convient de souligner que le programme exige des éléments de gouvernance cruciaux, une politique complète et un cadre de gestion, et requiert l’officialisation et la documentation des processus et procédures non officiels afin de réduire le risque d’atteinte à la sécurité des TI.

5 ANNEXE A – Critères de vérification

Critères de vérification	
Gouvernance du programme de sécurité des TI	
1.1	Une structure de gouvernance est établie pour la sécurité des TI. Les organes responsables de la gouvernance sont investis de mandats clairement définis, jouent un rôle actif, exercent une grande influence et surveillent les processus de gestion. L'organe de surveillance se réunit régulièrement et examine l'information se rapportant aux priorités et plans de sécurité des TI, donne des avis sur les problèmes, examine le rendement de la fonction de sécurité des TI et communique ses décisions à l'organisme sans tarder.
1.2	Un plan de sécurité des TI à jour a été défini et est conforme à la stratégie et aux attentes opérationnelles ainsi qu'aux capacités en matière de TI. Les plans tactiques sont élaborés à partir du plan stratégique.
1.3	L'approche adoptée par l'organisme pour gérer la sécurité des TI et sa mise en œuvre sont examinées de manière indépendante à des intervalles réguliers, ou quand des changements importants sont apportés à la mise en œuvre de la sécurité.
Cadre du programme de sécurité des TI	
2.1	Une politique sur la sécurité des TI a été définie et approuvée par la direction, publiée et communiquée à tous les employés.
2.2	La politique sur la sécurité des TI fait état de l'engagement de la direction et décrit l'approche adoptée par l'organisme pour gérer la sécurité de l'information.
2.3	La politique sur la sécurité des TI est appuyée par des procédures, normes et directives clés et elle respecte la politique du Secrétariat du Conseil du Trésor du Canada.
Défense des frontières et du périmètre	
3.1	Des zones frontalières et périmétriques ont été définies. Elles sont gérées et contrôlées adéquatement afin de les protéger contre les menaces et d'assurer la sécurité des systèmes et des applications.
3.2	Des zones de sécurité des TI interne ont été définies. Elles sont gérées et contrôlées adéquatement afin de les protéger contre les menaces et d'assurer la sécurité des systèmes et des applications.
Contrôles de l'accès et accès privilégié aux systèmes	
4.1	Un processus d'autorisation officiel est en place pour accorder et retirer l'accès des utilisateurs aux systèmes; les droits d'accès des utilisateurs au SIGSB, à AMIS, à SharePoint et aux systèmes et aux données connexes sont conformes aux besoins opérationnels définis et documentés, sont demandés par le gestionnaire de l'utilisateur et sont approuvés par le propriétaire du système.
4.2	La direction examine régulièrement tous les comptes et les privilèges connexes.
4.3	Les paramètres des mots de passe pour les applications et les réseaux sont gérés conformément aux politiques approuvées en matière de sécurité.
4.4	L'accès aux comptes privilégiés d'applications, de bases de données et de réseaux est limité et les activités effectuées à l'aide de ces comptes sont surveillées.
Gestion des changements et des configurations	
5.1	Un processus de gestion des configurations est établi et dûment tenu à jour.
5.2	Un processus de gestion des changements aux systèmes est établi et tenu à jour, avec l'apport des responsables de la sécurité des TI.
Gestion des vulnérabilités	
6.1	Les vulnérabilités sont gérées grâce à un processus de découverte continue et de mise en œuvre des solutions.
6.2	Un système de gestion des correctifs exploité dans l'infrastructure permet d'installer rapidement les

Critères de vérification	
	correctifs de sécurité cruciaux pour le SIGSB, AMIS et SharePoint ainsi que pour les systèmes et bases de données et l'infrastructure connexes.
Sécurité physique de la salle de serveurs	
7.1	Les restrictions à l'accès physique sont mises en œuvre et administrées afin que seules les personnes autorisées aient accès à la salle de serveurs. L'approbation de la direction est requise avant que l'accès ne soit accordé.

6 Réponse de la direction aux recommandations découlant de la vérification

Sommaire

La direction du CRSNG et du CRSH accepte les constatations découlant de la vérification.

La direction est d'accord avec le thème central de la vérification, c'est-à-dire qu'il faut apporter et officialiser d'importantes améliorations à la sécurité des TI afin de contribuer à l'instauration d'une culture de l'amélioration continue pour fournir ainsi de manière durable des résultats positifs et accroître la valeur des activités des organismes.

La vérification met au jour des améliorations à apporter au cadre stratégique sur la politique sur la sécurité des TI et propose plusieurs façons de s'y prendre. La présente réponse de la direction aborde les recommandations une à une et énonce les mesures générales propres à assurer l'amélioration continue de la position des organismes en matière de sécurité.

La direction du CRSNG et du CRSH reconnaît le thème prédominant des recommandations découlant de la vérification, mais il convient de noter clairement que, dans le cas de chaque recommandation, les problèmes avaient déjà été relevés et que des mesures précises étaient en cours en vue de combler toute lacune. Par suite de l'évaluation indépendante de la sécurité effectuée en avril 2011, un cadre stratégique sur la politique sur la sécurité des TI a été élaboré, puis utilisé comme guide pour combler certaines lacunes. Par ailleurs, pendant la vérification, une politique sur la sécurité des TI et des directives ont été élaborées (novembre 2011), présentées à la haute direction et approuvées officiellement par les présidents (juillet 2012).

La direction du CRSNG et du CRSH continue d'accorder une grande priorité à l'état de préparation des organismes en matière de sécurité.

Contexte

La Division de la vérification interne du CRSNG et du CRSH a procédé à la vérification du programme conjoint de sécurité des TI des organismes. La vérification a porté sur l'état du programme de sécurité des TI et les activités connexes entre le 1er avril 2011 et la fin de décembre de cette même année. La vérification interne visait à évaluer

l'efficacité de certains contrôles de sécurité des TI du CRSNG et du CRSH et d'en rendre compte.

Au cours des 20 derniers mois, la Direction des services administratifs communs s'est intéressée de très près à la position des organismes en matière de sécurité, en particulier la sécurité des TI. À cette fin, une évaluation indépendante de la sécurité des TI a été réalisée en avril 2011 et une évaluation ministérielle de la menace et des risques a été menée à bien en décembre de la même année. Ces deux initiatives font ressortir la nécessité de poursuivre l'officialisation des processus de sécurité des TI, d'examiner les contrôles d'accès des utilisateurs et de mettre en œuvre un programme de gestion des vulnérabilités.

En juillet 2012, une politique des deux organismes sur la sécurité des TI a été approuvée par les présidents. La responsabilité générale des futures directives et normes a été déléguée au vice-président de la DSAC, tandis que la responsabilité de la tenue à jour continue, du parrainage et de la coordination des politiques sur les TI, notamment la politique sur la sécurité des TI, incombe au dirigeant principal de l'information (DPI).

Point	Recommandation	Plan d'action	Date cible
1	A) Réexaminer la structure de gouvernance du programme de sécurité des TI et inclure la surveillance du programme par la haute direction dans le mandat de l'un des organes de surveillance ou comités supérieurs en place pour que celui-ci examine régulièrement les priorités, les plans et le rendement en matière de sécurité des TI et fasse valoir l'importance de la fonction pour l'organisme.	• Toutes les politiques sur la GI et les TI sont examinées et leur approbation est recommandée par les présidents des organismes au Comité directeur de GI-TI des deux Conseils. • La gestion de l'information est actuellement un point permanent à l'ordre du jour des réunions du Comité directeur de GI-TI des deux Conseils. • La sécurité des TI deviendra un point permanent à l'ordre du jour de toutes les futures réunions du comité des deux organismes. • En concertation avec l'agent ministériel de la sécurité, les organismes élaborent actuellement une stratégie officielle de communication sur la sécurité qui vise à renseigner le personnel et à lui rappeler l'importance de la sécurité.	MENÉE À BIEN Février 2012 T4 2012-2013

	B) Élaborer un plan de sécurité de l'organisme, comme l'exige la Directive sur la gestion de la sécurité ministérielle du Conseil du Trésor et prévoir des examens stratégiques du programme de sécurité des TI.	• L'élaboration d'un plan de sécurité de l'organisme a été amorcée en mars 2010 sous l'égide du l'agent ministériel de la sécurité. • Le plan de sécurité de l'organisme prévoira un examen annuel du programme de sécurité des TI.	T4 2012-2013
2	A) Peaufiner, approuver et communiquer la politique sur la sécurité des TI à tous les employés.	• La politique des organismes sur la sécurité des TI et les directives connexes ont été approuvées par les présidents des organismes en 2012.	MENÉE À BIEN Juillet 2012
	B) Examiner minutieusement le cadre de sécurité des TI, à savoir la politique sur la sécurité des TI, les directives, les normes et les lignes directrices ainsi que les procédures et processus requis pour les mettre en œuvre dans le contexte opérationnel des organismes. Cet examen devrait être réalisé dans le contexte des dernières politiques, directives, normes et lignes directrices des principaux organismes responsables de la sécurité et du Conseil du Trésor et vérifier que les objectifs de contrôle de la sécurité et les contrôles ainsi que la gestion des risques sont intégrés au programme de sécurité des TI des organismes.	• Le cadre stratégique sur la politique sur la sécurité, établi en novembre 2011 a servi de guide pour l'élaboration de l'actuelle politique sur la sécurité des TI et des directives connexes. • Ce cadre a été élaboré conformément aux dispositions sur la sécurité des TI de la Politique sur la sécurité du gouvernement du gouvernement du Canada et la Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI). • La norme GSTI définit les exigences de base en matière de sécurité que les organismes fédéraux doivent respecter pour protéger l'information et les biens de TI placés sous leur contrôle. • Le cadre utilise également la structure organisationnelle de la norme ISO 27002 − chacune des 11 catégories mentionnées en constitue un volet.	T4 2012-2013

3	A) Officialiser les mécanismes de gestion de la sécurité et des changements et élaborer des documents sur la procédure à suivre à l'appui des activités afin d'avoir l'assurance que les processus et procédures à suivre sont suivis systématiquement.	• Un processus officiel de contrôle des changements est actuellement mis en œuvre au sein de la Division des solutions d'information et d'innovation (SII) et tous les changements proposés sont surveillés par le Comité de contrôle des changements (CCC) selon un processus officiel de demande de changement. • Les documents sur la procédure à suivre à l'appui du processus de gestion de la sécurité sont en cours d'élaboration en vue de leur mise en œuvre.	MENÉE À BIEN Août 2011 T4 2012-2013
	B) Conserver la documentation des contrôles clés (p. ex., approbations, examens de la sécurité et documentation de la gestion des changements) pour les besoins de la piste de vérification.	• Les organismes mettent la dernière main aux documents sur la procédure à suivre et les processus pour toutes les activités relatives à la sécurité et aux changements aux fins de vérification.	T4 2012-2013
4	A) Officialiser toutes les procédures de gestion des utilisateurs, y compris celles concernant l'accès physique, et communiquer au personnel les procédures en place afin d'assurer leur respect systématique. Les procédures de gestion des utilisateurs devraient exiger un examen périodique de tous les comptes et documenter l'utilisation des comptes privilégiés et d'administrateur.	• Considérées comme une exigence clé de la mise en œuvre du Système de gestion des relations avec la clientèle et de SharePoint, toutes les procédures de gestion des utilisateurs sont examinées et officialisées parallèlement à l'évaluation de la menace et des risques. • Deux nouveaux outils de surveillance ont été mis en œuvre dans l'environnement de production afin de vérifier l'utilisation des comptes d'administration privilégiés. De plus, un archivage central des mots de passe a été mis en œuvre afin de vérifier et de suivre de près l'utilisation de tous les comptes privilégiés du système et de surveiller les activités.	Janvier 2013 MENÉE À BIEN Avril 2012

	B) Il faudrait définir une norme régissant les mots de passe qui soit conforme aux principales pratiques à cet égard, passer en revue les mots de passe existants et faire en sorte qu'ils soient conformes à cette norme. Il faudrait aussi élaborer et mettre en œuvre une procédure de surveillance de l'accès physique à la salle de serveurs.	• Considérées comme une exigence clé de la mise en œuvre du Système de gestion des relations avec la clientèle et de SharePoint, des normes régissant les mots de passe ont été établies conformément aux pratiques exemplaires en vigueur au sein de l'industrie. • En concertation avec l'agent ministériel de la sécurité, les organismes élaborent actuellement des procédures pour la surveillance de l'accès physique à la salle de serveurs.	MENÉE À BIEN Mai 2012 T4 2012-2013
5	A) Examiner le processus de gestion des vulnérabilités et l'harmoniser avec les principales pratiques, notamment le processus d'acheminement et de communication des vulnérabilités ainsi que de documentation des décisions en matière de gestion des risques.	• Dans le cadre de la mise en œuvre du cadre stratégique sur la politique sur la sécurité des TI, des travaux ont commencé en vue d'officialiser le processus de gestion des vulnérabilités, notamment les pratiques exemplaires du point de vue de la vérification et des documents.	T1 2013-2014
	B) Examiner, officialiser et appliquer de façon régulière le processus d'évaluation technique de la vulnérabilité. Conserver les données probantes témoignant de l'évaluation et du suivi de la vulnérabilité pour les besoins de la piste de vérification.	• La mise en œuvre de nouveaux outils et procédures d'évaluation à l'appui des évaluations de vulnérabilité devrait débuter au quatrième trimestre et se poursuivre l'an prochain.	T1 2013-2014
	C) Examiner le processus de gestion des correctifs, l'officialiser et l'étendre à toutes les composantes du réseau et à tous les systèmes d'application.	• Le processus de gestion des correctifs a été officialisé et automatisé à l'aide d'outils de surveillance et de correction nouvellement automatisés. • Un nouveau poste d'agent de la conformité a été créé. Le titulaire surveillera et examinera de façon indépendante la conformité des correctifs et des licences d'utilisation de l'infrastructure des organismes.	MENÉE À BIEN Mars 2011 Janvier 2012