Rapport d'audit interne — La gestion de la sécurité des technologies de l'information

Janvier 2018

Revue des pratiques et audit interne

Bureau du vérificateur général du Canada

Office of the Auditor General of Canada

This document is also available in English.

Cat. No. FA3-130/2017F-PDF
ISBN 978-0-660-23571-4

Table des matières

Sommaire

Objectif

L'audit visait à déterminer si le Bureau du vérificateur général du Canada disposait d'un cadre adéquat et efficace pour assurer la sécurité des technologies de l'information (TI).

L'audit interne a porté sur la période allant du 1er janvier 2016 au 30 novembre 2016. Nous avons prolongé cette période jusqu'au 31 mars 2017, mais uniquement pour examiner le plan d'action sur la gestion de la sécurité des TI établi par la direction de la sécurité des TI à la suite de son autoévaluation. La direction a transmis ce plan à la fonction d'audit interne le 24 mars 2017.

Importance de cet audit interne

Cet audit interne est important parce que le Bureau a reconnu qu'un programme de sécurité des TI efficace et efficient était essentiel pour protéger les renseignements sensibles et les actifs de valeur dont il est responsable. Or, pour s'acquitter de cette obligation, il est primordial que le Bureau dispose d'un **cadre de sécurité des TI** adéquat et efficace.

Conclusion

Nous avons conclu que le Bureau avait conçu un cadre adéquat pour assurer la sécurité de ses systèmes de TI. Cependant, la gestion du cadre de sécurité des TI a nui à son efficacité. Plus particulièrement, la direction de la sécurité des TI n'a pas systématiquement revu ses politiques, procédures et directives. Elle n'a pas non plus mis en œuvre bon nombre des contrôles exigés par les lignes directrices et instruments de politique pertinents du Conseil du Trésor en matière de sécurité des TI.

La direction de la sécurité des TI accepte nos recommandations. Une réponse détaillée suit chacune des recommandations du rapport.

Nous avons demandé à la direction de nous remettre un plan d'action, ce qu'elle a fait le 20 juillet 2017.

Cadre de sécurité des TI — Toutes les ressources d'une organisation, y compris les politiques, le personnel, les processus, les pratiques et les technologies, qui sont utilisées pour évaluer les risques et les attaques en matière de TI, et les atténuer.

Introduction

Objet de l'audit interne

1. Le présent audit interne visait à déterminer si le Bureau du vérificateur général du Canada disposait d'un cadre adéquat et efficace pour assurer la sécurité des technologies de l'information (TI).

2. Un cadre de sécurité des TI bien établi :

- est conforme aux politiques et lignes directrices pertinentes du gouvernement en matière de sécurité des TI;
- contient une structure de gouvernance assortie de rôles et de responsabilités précis à l'égard de la sécurité des TI;
- prévoit des mécanismes adéquats de rapport pour les fonctions des TI qui sont clairs, pertinents, compréhensibles, utiles et opportuns;
- prévoit des contrôles de gestion ou des mesures techniques destinés à protéger les actifs de TI et l'information et à assurer un service sécuritaire et ininterrompu;
- contient un plan d'action, décrivant les produits attendus et les échéances, pour mettre en œuvre ses contrôles de gestion de la sécurité ou mesures de protection techniques et évaluer les progrès réalisés dans la mise en œuvre du plan.

3. Cet audit interne a porté sur la période allant du 1er janvier 2016 au 30 novembre 2016. Nous avons prolongé cette période au 31 mars 2017, mais uniquement pour examiner la version définitive du plan d'action sur la gestion de la sécurité des TI établi par la direction de la sécurité des TI à la suite de son autoévaluation. La direction a transmis le plan à la fonction d'audit interne le 24 mars 2017.

4. La section intitulée **À propos de l'audit interne**, à la fin du présent rapport, donne des précisions sur l'objectif de l'audit, les moyens et méthodes examinés et les critères de l'audit.

Importance de cet audit interne

5. Cet audit interne est important parce que le Bureau a reconnu qu'un programme de sécurité des TI efficace et efficient était essentiel pour protéger les renseignements sensibles et les actifs de valeur dont il est responsable. Or, pour s'acquitter de cette obligation, il est primordial que le Bureau dispose d'un cadre de sécurité des TI adéquat et efficace.

Constatations, recommandations et réponses

Autoévaluation de la sécurité des technologies de l'information

Résumé des constatations

6. Le Bureau du vérificateur général du Canada a élaboré un cadre adéquat de sécurité des technologies de l'information (TI). Il a ainsi établi des politiques, des procédures et des directives sur la sécurité des TI qui sont en grande partie conformes aux exigences de la *Politique sur la sécurité du gouvernement* et de la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information* (GSTI) du Conseil du Trésor.

7. Le Bureau devait réaliser des autoévaluations annuelles de ses programmes et pratiques de sécurité des TI, mais la direction de la sécurité des TI n'a pas été en mesure de confirmer qu'elle avait procédé à ces autoévaluations avant 2016. Nous avons constaté que l'autoévaluation réalisée en 2016 avait été exhaustive et avait abouti à un plan d'action complet.

8. Par ailleurs, dans le cadre de sa gestion de la sécurité des TI, le Bureau n'a pas mis en œuvre, ou a partiellement mis en œuvre, bon nombre des exigences prévues dans la norme GSTI du Conseil du Trésor et dans ses propres politiques, procédures et directives en matière de sécurité des TI.

L'autoévaluation de la sécurité des TI du Bureau a été exhaustive

Importance de cette constatation

9. Cette constatation est importante parce qu'il est impératif de procéder à une autoévaluation annuelle des programmes et pratiques de sécurité des TI du Bureau et de les actualiser si l'on veut recenser et atténuer des risques qui sont en constante évolution.

Ce que nous avons examiné

10. Au début de l'audit interne, la direction de la sécurité des TI nous a fait savoir qu'elle amorçait une autoévaluation des contrôles de sécurité. La direction et la fonction d'audit interne ont alors convenu de ce qui suit :

- La direction définirait un plan de travail relatif à l'autoévaluation pour tester les principaux contrôles de sécurité des TI, analyserait les résultats obtenus et établirait un plan d'action.
- La fonction d'audit interne examinerait les travaux réalisés par la direction et formulerait des commentaires et des recommandations.

11. Dans un premier temps, nous avons discuté avec la direction de la méthode qu'elle comptait utiliser pour réaliser l'autoévaluation. Nous avons vérifié si la méthode retenue donnerait à la direction du Bureau l'assurance voulue. Nous avons tenu compte des exigences relatives aux autoévaluations du Conseil du Trésor et de ses directives sur les contrôles devant être testés.

12. Nous avons examiné tous les tests conçus et réalisés par la direction de la sécurité des TI. Nous avons aussi fait par sondage les tests réalisés. Nous avons examiné les conclusions tirées par la direction sur tous les tests.

13. Nos constatations portent sur :

- la stratégie d'autoévaluation de la direction.

Ce que nous avons constaté

14. **La stratégie d'autoévaluation de la direction** — La norme GSTI prévoit que « [l]es ministères doivent effectuer une évaluation annuelle de leur programme et de leurs pratiques de sécurité des TI afin de vérifier leur conformité aux politiques et normes de sécurité du gouvernement et du ministère […] ». Or, rien ne prouve que le Bureau ait réalisé une autoévaluation de son programme et de ses pratiques de sécurité des TI avant l'automne 2016. C'est donc dire que le Bureau n'a pas satisfait à cette exigence de la GSTI.

15. Vu les contraintes de temps et de ressources, la direction a décidé que l'autoévaluation de l'automne 2016 porterait sur des systèmes sélectionnés, conformément au guide *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33) du Centre de la sécurité des télécommunications.

16. La direction a eu recours aux contrôles de sécurité et aux améliorations des contrôles proposés dans le guide ITSG-33. Celui-ci propose aux organisations un choix de plus de 900 contrôles possibles. La direction a choisi les contrôles à tester en se fondant sur une stratégie adaptée à son environnement de risque.

17. Nous avons examiné la décision prise par la direction de faire porter l'autoévaluation uniquement sur une sélection de systèmes du Bureau. Nous comprenons qu'en raison de ressources limitées, il était difficile de procéder à une autoévaluation exhaustive de tous les systèmes de TI du Bureau. La direction nous a fait savoir que, conformément à l'esprit de l'ITSG-33, elle évaluerait systématiquement les autres systèmes par rotation. À notre avis, cette stratégie est raisonnable.

18. Pour chaque test de contrôle effectué, la direction a consigné ses travaux dans un ou plusieurs scripts de test, qui résument l'étendue des travaux, les procédures, les résultats et les conclusions.

19. Nous avons fait ce qui suit :

- Nous avons vérifié si la direction avait réalisé tous les tests décrits dans sa stratégie adaptée.
- Nous avons examiné tous les scripts pour vérifier si la direction avait effectué les tests selon les exigences du guide ITSG-33 et si des éléments probants étayaient les conclusions de la direction pour chacun des tests.
- Nous avons vérifié si tous les scripts avaient été soumis à une revue de contrôle qualité adéquate.
- Nous avons sélectionné au hasard 25 scripts pour effectuer nous-mêmes les tests afin de voir si nos conclusions étaient les mêmes que celles de la direction.

20. Nous n'avons constaté aucun écart à la suite de la réalisation des travaux décrits ci-dessus. À notre avis, la stratégie de la direction lui a permis de réaliser une autoévaluation exhaustive d'une sélection de systèmes du Bureau.

Le cadre de sécurité des TI du Bureau était adéquat, mais des faiblesses dans la mise en œuvre des politiques et pratiques du Bureau relatives aux TI ont nui à son efficacité

Importance de cette constatation

21. Conformément aux exigences du Conseil du Trésor, le Bureau doit établir un cadre de gouvernance clair et se conformer aux lignes directrices et instruments de politique pertinents du Conseil du Trésor en matière de sécurité des TI pour assurer la sécurité de l'information et des actifs de TI dont il a la charge.

Ce que nous avons examiné

22. Nous avons examiné les résultats de l'autoévaluation de la sécurité des TI du Bureau. Plus particulièrement, nous avons examiné le cadre de sécurité des TI du Bureau et vérifié s'il était bien établi, bien mis en œuvre et conforme aux politiques et aux normes pertinentes du gouvernement en matière de sécurité des TI.

23. Nous avons examiné la structure de gouvernance du Bureau et évalué si elle était conforme aux lignes directrices et instruments de politique pertinents du Conseil du Trésor en matière de sécurité des TI. Nous avons vérifié si le Bureau disposait d'un mécanisme de rapport clair, pertinent, compréhensible, utile et opportun pour faire rapport sur les incidents liés à la sécurité des TI aux parties externes (par exemple Services partagés Canada).

24. Nos constatations portent sur :

- les résultats de l'autoévaluation;
- le cadre de sécurité des TI du Bureau;
- la gouvernance;
- la mise en œuvre du cadre de sécurité des TI.

Ce que nous avons constaté

25. **Les résultats de l'autoévaluation** — Après avoir terminé son autoévaluation, la direction de la sécurité des TI a conclu que la gestion des risques liés à la sécurité des TI comportait de nombreuses faiblesses. Nous partageons cet avis. Les constatations présentées ci-après décrivent en détail ces faiblesses.

26. **Le cadre de sécurité des TI du Bureau** — Le cadre de sécurité des TI du Bureau est généralement conforme aux lignes directrices et instruments de politique pertinents du Conseil du Trésor en matière de sécurité des TI. Il manquait cependant certains éléments obligatoires dans la politique du Bureau

par rapport à ces lignes directrices et instruments de politique. Ainsi, la politique du Bureau ne prévoit pas les exigences suivantes :

- la réalisation d'une autoévaluation annuelle;
- une description appropriée des rôles et responsabilités du dirigeant principal de l'information du Bureau;
- une description des rapports hiérarchiques entre le coordonnateur de la sécurité des TI et le dirigeant principal de l'information.

27. La fonction d'audit interne a noté que, exception faite de la revue de la politique effectuée lors de l'autoévaluation, le Bureau n'avait pas procédé à un examen systématique de chacun des éléments de sa politique de sécurité des TI. Par conséquent, la structure de gouvernance de la sécurité des TI n'a pas été actualisée dans la politique du Bureau.

28. La direction a indiqué à l'équipe d'audit interne que le Bureau adoptera toute nouvelle politique ou ligne directrice pertinente publiée par le Conseil du Trésor. Elle nous a aussi indiqué que le Bureau définirait des procédures, des normes et des directives au besoin.

29. **La gouvernance** — La fonction d'audit interne a examiné en profondeur les questions liées à la gouvernance. Nous avons examiné les descriptions de poste du personnel chargé de la sécurité des TI, le cas échéant. Nous avons constaté que les trois descriptions de poste étaient désuètes, n'étaient pas conformes à la norme GSTI, ou ne concordaient pas avec les responsabilités actuelles du titulaire du poste. Il n'y avait aucune description pour un des postes.

30. Nous avons constaté un manque de surveillance dans les secteurs suivants :

- Conseil de gestion des changements liés aux TI — Un employé de la sécurité des TI avait été choisi pour présider les réunions de ce conseil. Il n'a pas assisté à environ un tiers des réunions au cours de la période visée par notre audit. Aucun autre membre de l'équipe de la sécurité des TI n'a été délégué pour remplacer cet employé en son absence. De plus, le mandat du conseil n'était pas à jour.
- Comité de l'équipe de la sécurité virtuelle — Nous n'avons pas trouvé le mandat de ce comité et il n'y avait que quelques comptes rendus de décisions. À notre avis, peu d'éléments probants prouvaient que le comité avait exercé une surveillance suffisante pour garantir que l'information liée aux priorités, aux plans et aux résultats dans le secteur de la sécurité des TI avait été régulièrement examinée et que des conseils avaient été formulés en temps opportun lorsqu'il y avait des problèmes.

31. Nous avons aussi constaté que les outils automatisés du Bureau qui envoient des messages d'alerte pour surveiller les incidents de sécurité des TI devaient être améliorés.

32. Pour ce qui est de la communication, nous avons constaté que le Bureau n'avait pas officiellement avisé le personnel de la nomination du nouvel agent de sécurité ministériel du Bureau et du nouveau dirigeant principal de l'information, ni de la création du poste d'agent de sécurité adjoint ministériel. Au cours de

notre audit, le Bureau a également nommé un nouveau coordonnateur de son plan de continuité des activités. La direction du Bureau nous a fait savoir qu'elle voulait communiquer ces nominations à la suite de l'autoévaluation de la sécurité des TI, lorsqu'elle serait mieux placée pour créer un cadre efficient de gouvernance de la sécurité des TI.

33. La norme GSTI du Conseil du Trésor oblige la haute direction à approuver les politiques, normes et lignes directrices ministérielles relatives à la sécurité des TI. Or, nous n'avons trouvé aucun élément démontrant que la direction du Bureau avait approuvé les politiques de sécurité des TI du Bureau.

34. **La mise en œuvre du cadre de sécurité des TI** — Le Bureau n'a pas mis en œuvre un grand nombre d'exigences de ses propres politiques et procédures, ou il les a mises en œuvre en partie seulement.

35. Selon les constatations de l'autoévaluation, 31 % des processus de sécurité des TI du Bureau satisfaisaient aux exigences. Le reste des processus (69 %) satisfaisait en partie, satisfaisait en grande partie ou ne satisfaisait pas aux exigences.

36. La fonction d'audit interne a obtenu une assurance étayant la conclusion de la direction de la sécurité des TI, à savoir que les résultats des tests indiquaient que les systèmes sélectionnés du Bureau n'avaient pas été protégés de manière à ramener le risque à un niveau acceptable.

37. Vu que la conclusion de la direction découlant de l'autoévaluation ne visait que les systèmes sélectionnés, la fonction d'audit interne a aussi voulu savoir si elle pouvait tirer la même conclusion sur le cadre de sécurité des TI du Bureau dans son ensemble. Elle a donc vérifié si la même conclusion valait pour d'autres systèmes. Nous avons de fait constaté qu'un bon nombre de ces observations s'appliquaient aussi à d'autres systèmes. La direction a également indiqué que la plupart des contrôles testés ne s'appliquaient pas seulement aux systèmes sélectionnés et que son plan d'action comprenait des solutions visant tous les systèmes et applications du Bureau.

38. En 2015, l'équipe du Service du contrôleur du Bureau a aussi évalué l'efficacité du système de contrôle interne visant les rapports financiers. Certaines observations de l'équipe étaient similaires à celles formulées dans l'autoévaluation des systèmes sélectionnés. L'équipe du Service du contrôleur avait fait des recommandations en fonction de ses observations et la direction y avait donné suite en établissant un plan d'action. Les observations du Service du contrôleur venaient étayer le point de vue selon lequel les problèmes relevés dans les systèmes sélectionnés n'étaient pas propres à ces systèmes. Ces observations ont confirmé la nécessité pour le Bureau de procéder à une autoévaluation de tous ses systèmes de TI.

39. ***Plan de sécurité ministérielle*** — Les organisations fédérales sont tenues de définir un plan de sécurité ministérielle prévoyant des objectifs, des buts, des stratégies, des priorités et des échéances pour améliorer la sécurité. Le plan doit aussi donner des précisions sur les décisions relatives à la gestion des risques de sécurité.

40. Selon la *Directive sur la gestion de la sécurité ministérielle*, l'agent de sécurité ministériel doit mettre à jour le plan de sécurité ministérielle à la lumière des résultats de la mesure du rendement, de l'évaluation ainsi que des évaluations de risque. Nous avons constaté que même si le Bureau avait périodiquement mis à jour son profil de risques liés à la sécurité des TI, il n'avait pas mis à jour son plan de sécurité ministérielle en fonction de ces nouveaux risques depuis le 20 décembre 2013. L'agent de sécurité adjoint ministériel nous a indiqué que le Bureau comptait diffuser un nouveau plan de sécurité ministérielle au cours de l'exercice 2017-2018.

41. ***Évaluations des menaces et des risques*** — Les évaluations des menaces et des risques aident les organisations à évaluer les éléments qui pourraient nuire à leur sécurité. La norme GSTI du Conseil du Trésor recommande de procéder à une évaluation des menaces et des risques pour chacun des systèmes de TI tout au long de leur cycle de vie (préparation, conception et développement, mise en œuvre, fonctionnement, élimination). Comme les technologies et les menaces sont en constante évolution, les ministères et les organismes doivent examiner régulièrement les risques liés à la sécurité et adapter les exigences en conséquence.

42. Le Bureau n'a pas régulièrement actualisé ses évaluations des menaces et des risques pour un grand nombre de ses systèmes. La direction a depuis mis en œuvre un plan pour régler cette question.

43. ***Plan de continuité des activités*** — En janvier 2014, le Bureau a terminé la rédaction de son plan de continuité des activités. Ce plan vise à garantir la poursuite des activités essentielles du Bureau de sorte qu'il dispose des structures et des processus requis pour reprendre la prestation des services après une interruption inopinée de ses activités. Tester et revoir régulièrement le plan de continuité des activités est utile pour confirmer qu'il fonctionne comme prévu afin de garantir une interruption minimale ou nulle des services et du fonctionnement des actifs de TI essentiels.

44. Pour garantir que le plan de continuité des activités fonctionne comme prévu, le Bureau a réalisé certains tests, dont deux **exercices de simulation sur maquette**. Cependant, le Bureau n'a pas testé son **centre de reprise des activités en cas de sinistre**. Un test a été effectué sur celui-ci à la suite de l'audit interne.

45. ***Rapports externes*** — Aux termes de la *Politique sur la sécurité du gouvernement* du Conseil du Trésor, les ministères doivent signaler à l'instance appropriée (par exemple le Secrétariat du Conseil du Trésor du Canada ou Services partagés Canada) les enjeux importants concernant la conformité à la politique et les incidents liés à la sécurité. La direction de la sécurité des TI a élaboré et consigné un processus pour signaler les incidents liés à la sécurité des TI.

Exercice de simulation sur maquette — Une simulation sur papier qui permet de tester les capacités de réponse d'une organisation.

Centre de reprise des activités en cas de sinistre — Une unité que peut utiliser une organisation pour récupérer et rétablir son infrastructure et ses activités des TI lorsque son centre de données principal n'est plus disponible.
Source : TechTarget, Inc.

Le processus original date du 1er janvier 2013. Au fil des ans, la direction a souvent modifié ce document. Les derniers changements y ont été apportés le 10 septembre 2015. Nous avons constaté que le document était clair, pertinent et compréhensible. Cependant, il s'agissait encore d'une ébauche, qui ne reflétait pas la structure de gouvernance actuelle de la fonction de sécurité des TI du Bureau. Le document était donc, de ce fait, d'une utilité limitée. La direction nous a fait savoir qu'elle s'employait à revoir celui-ci. Elle nous a aussi indiqué qu'il n'y avait eu aucune infraction à la sécurité importante.

46. ***Contrats*** — Avant de passer un contrat, les ministères doivent déterminer si la sécurité des TI est un élément pertinent de la prestation de biens et de services par le fournisseur. Si tel est le cas, les ministères doivent tenir compte des exigences relatives à la sécurité des TI à toutes les étapes du processus de passation du contrat. Au Bureau, c'est le coordonnateur de la sécurité des TI qui doit effectuer les contrôles de sécurité des TI avant la passation d'un contrat. Nous avons appris que jusqu'en mai 2016, le processus de passation des contrats ne comprenait pas de vérification automatique des exigences relatives à la sécurité des TI.

47. ***Risques liés au piratage psychologique*** — Dans tous les systèmes de sécurité des TI, il y a des risques associés aux facteurs humains. Les attaquants exploitent souvent la vulnérabilité des personnes pour accéder à des données sécurisées. Les **tests de piratage psychologique** constituent un excellent outil pour évaluer les réactions du personnel à des cyberattaques par piratage psychologique. Nous avons constaté que le Bureau n'avait pas procédé à ce genre de test depuis 2011 en vue de déterminer ce que ses employés feraient en cas d'attaques extérieures. La direction analyse actuellement la meilleure façon de procéder à de tels tests.

Recommandations

48. La direction de la sécurité des TI devrait surveiller la mise en œuvre des lignes directrices et instruments de politique pertinents du Conseil du Trésor en matière de sécurité des TI dès qu'ils sont publiés et, au besoin, prendre des mesures correctives en temps opportun.

Réponse de la direction — *Recommandation acceptée. Dans le cadre du plan d'action du Bureau du vérificateur général du Canada établi à la suite de l'autoévaluation de la sécurité des TI, l'équipe de la sécurité des TI a recensé toutes les mesures correctives qui doivent être prises pour assurer la conformité aux lignes directrices et instruments de politique pertinents du Conseil du Trésor en matière de sécurité des TI dès qu'ils sont publiés.*

49. La direction de la sécurité des TI devrait évaluer tous les ans les procédures, normes et directives relatives à la sécurité des TI pour veiller à ce qu'elles restent à jour et soient conformes aux lignes directrices et instruments

Tests de piratage psychologique — Exercices visant à tester les réactions du personnel à une cyberattaque, dans le cadre de laquelle une personne de l'extérieur obtient de l'information sensible ou un accès inapproprié en établissant une relation de confiance avec des personnes à l'interne ou des employés ou en les bernant.

de politique pertinents du Conseil du Trésor en matière de sécurité des TI dès qu'ils sont publiés. Cette évaluation devrait comprendre une surveillance de la conformité aux exigences.

***Réponse de la direction** — Recommandation acceptée. Dans le cadre du plan d'action établi à la suite de l'autoévaluation de la sécurité des TI, de nouvelles procédures, normes et directives sont en cours d'élaboration. Un processus est aussi en voie d'être établi pour veiller à ce que les politiques, procédures et directives du Bureau en matière de sécurité des TI soient revues annuellement afin qu'elles restent actuelles et conformes aux lignes directrices et instruments de politique pertinents du Conseil du Trésor en matière de sécurité des TI.*

50. La direction de la sécurité des TI devrait :

- définir, consigner, actualiser et approuver les rôles et responsabilités pour tous les postes qui contribuent à la sécurité des TI, notamment pour le personnel de soutien qui appuie le travail des titulaires des postes clés;
- toujours communiquer rapidement le cadre de gouvernance de la sécurité des TI à tout le personnel dès que la direction a approuvé les changements qui y sont apportés.

***Réponse de la direction** — Recommandation acceptée. Les rôles et les responsabilités de tous les postes qui contribuent à la sécurité des TI ont maintenant été préparés, définis, consignés, actualisés et approuvés par la direction de la sécurité des TI. Celle-ci a communiqué le nouveau cadre de gouvernance de la sécurité des TI à l'ensemble du personnel le 30 juin 2017 et elle le tiendra informé de tout changement apporté à la structure de gouvernance.*

La direction s'est penchée sur les risques relevés

Importance de cette constatation

51. Il importe de disposer de contrôles de sécurité des TI efficaces pour que le Bureau puisse protéger ses actifs et l'information sensible. Vu les faiblesses décrites précédemment, il est primordial que la direction de la sécurité des TI mette son plan d'action en œuvre pour renforcer les contrôles visant les risques connus.

Ce que nous avons examiné

52. Nous avons vérifié si le Bureau disposait d'un processus d'établissement des rapports internes qui était clair, pertinent, compréhensible, utile et opportun pour faire rapport sur la sécurité des TI.

53. Nous avons examiné le plan d'action de la direction de la sécurité des TI visant à donner suite aux observations formulées dans l'autoévaluation. Nous avons vérifié si les mesures proposées cadraient avec les observations et si la direction avait prévu de les mettre en œuvre rapidement.

54. Nos constatations portent sur :

- l'évaluation des risques et les rapports internes;
- le plan d'action.

Ce que nous avons constaté

55. **L'évaluation des risques et les rapports internes** — Nous avons examiné le registre des risques du Service des systèmes et technologies de l'information de l'automne 2015 et de l'automne 2016. Les risques liés à la sécurité des TI recensés à l'automne 2015 sont restés les mêmes pendant la majeure partie de la période visée par l'audit. Nous avons aussi examiné les risques relevés à l'automne 2016, puisqu'ils faisaient partie de la période considérée.

56. À l'automne 2015, la direction de la sécurité des TI a déterminé que la sécurité des TI comportait un **risque inhérent** élevé. Elle a cependant déterminé que les contrôles en place permettaient de ramener ce risque à un **risque résiduel** acceptable. Par la suite, à la lumière des résultats préliminaires de l'autoévaluation, la direction a noté que, dans plusieurs cas, les contrôles ne semblaient pas efficaces. Résultat, la direction a révisé les résultats de l'évaluation des risques pour 2016. La sécurité des TI comportait donc toujours un risque inhérent élevé mais, en réalisant l'inefficacité de certains contrôles, la direction a relevé le risque résiduel lié à la sécurité des TI à un niveau élevé.

57. Nous avons constaté que la direction de la sécurité des TI avait rapidement informé la direction du Bureau des changements apportés à l'évaluation du risque résiduel lié à la sécurité des TI. De plus, la direction de la sécurité des TI a rapidement informé la direction du Bureau des premiers résultats de l'autoévaluation. À l'automne 2016, l'agent de sécurité adjoint ministériel a confirmé à la direction du Bureau que la sécurité des TI n'était pas à un niveau acceptable pour le Bureau. En janvier 2017, l'agent de sécurité adjoint ministériel a aussi communiqué les résultats de l'autoévaluation aux membres du Comité d'audit du Bureau.

58. La direction du Bureau a décidé d'inscrire le risque lié à la sécurité des TI comme un risque important dans le registre des risques de 2016 du Bureau. Le Bureau a par ailleurs intégré la sécurité des TI à ses priorités stratégiques de 2017-2018 et il s'est engagé à en assurer la surveillance.

59. Tous les ans, la direction de la sécurité des TI présente à la direction du Bureau un rapport sur les incidents de sécurité ou les cas de non-conformité aux politiques de sécurité des TI. Il n'y a eu aucun incident de sécurité des TI pendant la période visée par l'audit interne. La direction de la sécurité des TI a appliqué le même processus pour faire rapport à l'interne sur les incidents de sécurité des TI que celui utilisé pour présenter des rapports externes (voir le paragraphe 45). Comme nous l'avons déjà indiqué, le processus était encore à l'état d'ébauche et

Risque inhérent — Le risque évalué sans tenir compte des contrôles existants et de toutes les mesures prises pour le contrer.

Risque résiduel — Le risque évalué après avoir tenu compte des mesures d'atténuation et des contrôles mis en place.

n’avait pas été actualisé. L’agent de sécurité ministériel nous a fait savoir qu’il communiquerait rapidement à la direction du Bureau toute atteinte importante à la sécurité des TI, le cas échéant.

60. Nous avons aussi noté que la direction de la sécurité des TI avait rapidement communiqué des renseignements pertinents, compréhensibles et précis sur la sécurité des TI aux employés du Bureau lorsque la sécurité des TI pouvait avoir une incidence sur leur travail au quotidien.

61. **Le plan d’action** — Pour chacune des déficiences relevées dans son autoévaluation, la direction de la sécurité des TI a défini un plan d’action, en désignant un responsable de la mise en œuvre des mesures prévues et en précisant une échéance pour corriger la situation. La direction de la sécurité des TI a aussi présenté son plan d’action à la direction du Bureau.

62. Nous avons examiné le plan d’action de la direction de la sécurité des TI. À la lumière de cet examen, nous estimons qu’il permettra de corriger les faiblesses relevées par la direction dans l’autoévaluation. En raison de ces faiblesses, il importe que la direction mette en œuvre son plan d’action comme prévu. Nous surveillerons la mise en œuvre du plan.

Conclusion

63. Nous avons conclu que le Bureau du vérificateur général du Canada avait mis au point un cadre adéquat pour appuyer la sécurité de ses systèmes de TI. Cependant, la façon dont le Bureau a géré son cadre de sécurité des TI a nui à son efficacité. Plus particulièrement, la direction de la sécurité des TI n’a pas systématiquement revu ses politiques, procédures et directives. Elle n’a pas non plus mis en œuvre un grand nombre des contrôles exigés aux termes des lignes directrices et instruments de politique pertinents du Conseil du Trésor en matière de sécurité des TI.

À propos de l'audit interne

L'Équipe de la revue des pratiques et de l'audit interne du Bureau du vérificateur général du Canada fournit en toute indépendance de l'information, une assurance et des avis objectifs au vérificateur général. Les travaux de l'équipe sont une source de valeur ajoutée pour le Bureau, car ils améliorent les pratiques d'audit et favorisent l'apprentissage et le perfectionnement continu.

L'audit interne a été réalisé selon les *Normes relatives à la vérification interne au sein du gouvernement du Canada*, qui sont conformes aux normes de l'Institute of Internal Auditors. Le Bureau prévoit réaliser une inspection professionnelle avant le 31 mars 2018.

Dans le cadre de notre processus normal d'audit, nous avons obtenu la confirmation de la direction que les constatations figurant dans le présent rapport étaient fondées sur des faits.

Objectif

L'audit interne visait à déterminer si le Bureau du vérificateur général du Canada disposait d'un cadre adéquat et efficace pour assurer la sécurité des technologies de l'information (TI).

Moyens et méthodes examinés et critères

Au début de l'audit interne, nous avons présenté au Comité d'audit du Bureau un sommaire du plan d'audit qui recensait les moyens et méthodes, de même que les critères connexes, que nous avions jugés essentiels pour examiner la gestion de la sécurité des TI par le Bureau.

Le tableau ci-après présente les moyens et méthodes examinés, de même que les critères utilisés, dans le cadre de notre audit interne.

Nous avons choisi les critères de l'audit interne en fonction des lignes directrices et instruments de politique pertinents du Conseil du Trésor en matière de sécurité des TI et en nous fondant sur nos normes professionnelles et nos connaissances de l'objet considéré.

La direction a examiné les critères de l'audit interne et elle en a reconnu la validité.

Critères

Critères	Sources
Pour déterminer si le Bureau du vérificateur général du Canada avait un cadre adéquat et efficace pour assurer la sécurité des technologies de l'information (TI), nous avons utilisé les critères suivants :	
Le cadre de sécurité des TI du Bureau est bien établi et conforme aux politiques et directives pertinentes du gouvernement en matière de sécurité des TI.	• Conseil du Trésor, *Politique sur la sécurité du gouvernement*

Critères	Sources
Pour déterminer si le Bureau du vérificateur général du Canada avait un cadre adéquat et efficace pour assurer la sécurité des technologies de l'information (TI), nous avons utilisé les critères suivants : (suite)	
Le Bureau a une structure de gouvernance qui décrit clairement les rôles et responsabilités relatifs à la sécurité des TI : • Les obligations de rendre compte, les délégations de pouvoirs, les rapports hiérarchiques et les rôles et responsabilités sont définis, consignés et communiqués aux personnes concernées. • Les responsables de la gouvernance ont des mandats qui sont clairement communiqués; ils jouent un rôle actif et ils surveillent les processus de gestion. • L'organe de surveillance se réunit régulièrement et examine l'information liée aux priorités et aux plans en matière de sécurité des TI; il formule des avis sur les problèmes relevés; il examine le rendement de la fonction de la sécurité des TI; et il communique ses décisions à l'organisation en temps opportun.	• Conseil du Trésor, *Politique sur la sécurité du gouvernement*
La fonction des TI du Bureau possède des mécanismes de rapport qui sont clairs, pertinents, compréhensibles, utiles et opportuns.	• Conseil du Trésor, *Politique sur la sécurité du gouvernement*
Le Bureau dispose de contrôles de gestion de la sécurité des TI ou de mesures techniques destinés protéger les actifs de TI et l'information et à assurer un service sécuritaire et ininterrompu.	• Conseil du Trésor, *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information* (GSTI)
Le Bureau dispose d'un plan d'action, décrivant les produits attendus et les échéances, pour mettre en œuvre ses contrôles de gestion de la sécurité ou mesures de protection techniques, et évaluer les progrès réalisés dans la mise en œuvre du plan.	

Période visée par l'audit interne

L'audit interne a porté sur les moyens et méthodes qui étaient en place entre le 1er janvier 2016 et le 30 novembre 2016. Nous avons prolongé cette période jusqu'au 31 mars 2017, mais uniquement pour examiner le plan d'action transmis par la direction de la sécurité des TI le 24 mars 2017.

Équipe d'audit

Responsable de l'audit interne : Louise Bertrand

Directeur : Marc Gauthier

Tableau des recommandations

Le tableau qui suit regroupe les recommandations et les réponses apparaissant dans le présent rapport. Le numéro qui précède chaque recommandation correspond au numéro du paragraphe de la recommandation dans le rapport.

Recommandation	Réponse
48. La direction de la sécurité des TI devrait surveiller la mise en œuvre des lignes directrices et instruments de politique pertinents du Conseil du Trésor en matière de sécurité des TI dès qu'ils sont publiés et, au besoin, prendre des mesures correctives en temps opportun.	**Réponse de la direction** — Recommandation acceptée. Dans le cadre du plan d'action du Bureau du vérificateur général du Canada établi à la suite de l'autoévaluation de la sécurité des TI, l'équipe de la sécurité des TI a recensé toutes les mesures correctives qui doivent être prises pour assurer la conformité aux lignes directrices et instruments de politique pertinents du Conseil du Trésor en matière de sécurité des TI dès qu'ils sont publiés.
49. La direction de la sécurité des TI devrait évaluer tous les ans les procédures, normes et directives relatives à la sécurité des TI pour veiller à ce qu'elles restent à jour et soient conformes aux lignes directrices et instruments de politique pertinents du Conseil du Trésor en matière de sécurité des TI dès qu'ils sont publiés. Cette évaluation devrait comprendre une surveillance de la conformité aux exigences.	**Réponse de la direction** — Recommandation acceptée. Dans le cadre du plan d'action établi à la suite de l'autoévaluation de la sécurité des TI, de nouvelles procédures, normes et directives sont en cours d'élaboration. Un processus est aussi en voie d'être établi pour veiller à ce que les politiques, procédures et directives du Bureau en matière de sécurité des TI soient revues annuellement afin qu'elles restent actuelles et conformes aux lignes directrices et instruments de politique pertinents du Conseil du Trésor en matière de sécurité des TI.
50. La direction de la sécurité des TI devrait : • définir, consigner, actualiser et approuver les rôles et responsabilités pour tous les postes qui contribuent à la sécurité des TI, notamment pour le personnel de soutien qui appuie le travail des titulaires des postes clés; • toujours communiquer rapidement le cadre de gouvernance de la sécurité des TI à tout le personnel dès que la direction a approuvé les changements qui y sont apportés.	**Réponse de la direction** — Recommandation acceptée. Les rôles et les responsabilités de tous les postes qui contribuent à la sécurité des TI ont maintenant été préparés, définis, consignés, actualisés et approuvés par la direction de la sécurité des TI. Celle-ci a communiqué le nouveau cadre de gouvernance de la sécurité des TI à l'ensemble du personnel le 30 juin 2017 et elle le tiendra informé de tout changement apporté à la structure de gouvernance.