Service | Innovation | Rentabilité

Audit de la sécurité ministérielle

Rapport d’audit

Bureau de la vérification et de l’évaluation
Mars 2015

Services partagés Canada
Shared Services Canada

Canada

TABLE DES MATIÈRES

Sommaire

Points examinés

Le présent audit visait à déterminer si Services partagés Canada (SPC) mettait en œuvre un cadre de politique de sécurité qui était conforme aux politiques du Conseil du Trésor (CT) concernant la sécurité et si les processus d'évaluation et d'autorisation de sécurité (EAS) étaient en place comme prévu.

L'audit portait sur le cadre stratégique de sécurité de SPC et le processus d'EAS, du 1er avril 2012 au 31 octobre 2013.

Importance de l'audit

La sécurité de l'information, des biens et des services est essentielle pour empêcher que les renseignements ne soient compromis et veiller à ce que les personnes soient protégées contre la violence en milieu de travail. Le CT a établi des politiques spécifiques concernant la gestion de la sécurité ministérielle.

SPC a été créé le 4 août 2011 et sa fonction de sécurité a été établie en janvier 2012. L'audit porte sur la fonction de la sécurité ministérielle de SPC.

Constatations

Nous avons constaté que SPC a élaboré un cadre de politique de sécurité qui est conforme à la plupart des politiques gouvernementales clés, bien que des exceptions mineures ont été relevées. La direction a convenu de les rectifier une fois que l'examen des normes relatives à la gestion de la sécurité de la technologie de l'information serait achevé.

Pour se conformer aux exigences du CT relatives à la direction des activités liées à la gestion du risque, SPC a documenté et approuvé le Cadre de gestion des risques pour la sécurité de la technologie de l'information (le Cadre) qui régit le processus d'EAS. Toutefois, l'appartenance du document n'a pas été déterminée.

Les rôles et les responsabilités pour la direction de l'EAS ont été définis dans le Cadre, ainsi que dans le Guide sur le processus d'EAS de SPC (le Guide). Le Cadre et le Guide étaient disponibles aux employés de SPC.

Aucune des applications ministérielles de la technologie de l'information mises en œuvre au cours de la période visée par l'audit n'avait complété le processus d'EAS. Les gestionnaires de projet ont confirmé avoir mis en œuvre les applications sans compléter l'EAS, car le processus était considéré trop long pour répondre aux exigences de mise en œuvre.

Les gestionnaires de projet ont indiqué trois raisons clés pour ne pas avoir réalisé l'EAS pour l'application ministérielle : manque de compréhension envers le processus, le processus n'était pas inclus dans les calendriers de mise en œuvre des projets et le niveau d'effort n'était pas adapté aux risques liés aux applications.

Yves Genest
Dirigeant principal de la vérification et de l'évaluation

Contexte

1. Aux termes de la *Directive sur la gestion de la sécurité ministérielle* du Conseil du Trésor (CT), la gestion de la sécurité est une composante essentielle de la gestion efficace d'un ministère et du gouvernement dans son ensemble. Cette directive précise également que les activités de sécurité ministérielle doivent être coordonnées centralement et systématiquement intégrées aux activités courantes afin de s'assurer que les personnes, les informations, les biens et les services sont protégés, que les ministères ne font pas courir un risque accru aux autres ministères ni à l'ensemble du gouvernement, et que les activités et les services critiques se poursuivent en cas d'urgence.

2. Services partagés Canada (SPC) a été créé le 4 août 2011 afin de moderniser la façon dont le gouvernement fédéral gère son infrastructure de la technologie de l'information (TI) pour mieux soutenir les programmes et services offerts à la population canadienne. La première étape vers l'établissement d'une fonction de sécurité officielle à SPC a été prise en janvier 2012, avec la nomination d'un dirigeant principal de l'information et de la sécurité (DPIS), qui était aussi l'agent de sécurité du ministère et directeur de la sécurité. Avant ces nominations, il n'y avait aucune structure officielle en matière de sécurité pour SPC.

3. La Sécurité ministérielle, une division du Bureau du DPIS, était responsable de la gestion et de l'exploitation du Programme de sécurité interne du Ministère. La Division était formée de trois sections, chacune responsable de leurs fonctions respectives : sécurité de la TI, sécurité opérationnelle et sécurité interne.

4. La Sécurité ministérielle était responsable de la conception de mesures pour protéger la sécurité et l'intégrité des programmes, de l'information, des biens, du personnel et de l'environnement de travail de SPC. Ces mesures étaient liées à :

    - la sécurité physique;
    - aux questions de sécurités et aux enquêtes;
    - la sécurité de la TI;
    - aux politiques de gestion en matière de sécurité et d'urgences;
    - la sensibilisation à la sécurité;
    - la gestion des urgences et continuité des activités;
    - l'organisation de secours de l'immeuble;
    - la sécurité-incendie;
    - la sécurité du personnel;
    - aux formulaires.

5. L'équipe d'audit interne a examiné les politiques et les procédures élaborées par les représentants de la sécurité afin de veiller à ce qu'elles respectent les politiques gouvernementales. Parmi ces politiques, il y avait le processus d'évaluation et autorisation de sécurité (EAS), (anciennement connu sous le terme « processus de certification et d'accréditation ») qui était requis pour s'assurer que les systèmes et les applications étaient protégés adéquatement pour répondre au niveau de risques acceptable. L'examen du processus d'EAS a été réalisé pour déterminer si les risques liés aux systèmes informatiques organisationnels pour appuyer les activités opérationnelles ont été traités à SPC.

Objectif

6. L'objectif de cet audit consistait à déterminer si :

    - SPC mettait en place un cadre d'une politique de sécurité qui était conforme aux politiques du CT en matière de sécurité;
    - des processus d'EAS étaient en place et s'ils fonctionnaient comme prévu.

Portée

7. L'audit portait sur le cadre de politique de sécurité de SPC et le processus d'EAS, du 1er avril 2012 au 31 octobre 2013.

8. L'audit visait la totalité des politiques, des guides, des documents et des données concernant la sécurité ministérielle à SPC durant cette période. Ceci ne comprenait pas la sécurité associée aux services fournis aux organisations partenaires et aux clients.

Méthodologie

9. Durant l'audit, nous avons :

    - interrogé les cadres supérieurs, les gestionnaires de projet et les experts techniques;
    - examiné les documents du CT, du gouvernement du Canada et de SPC;
    - réalisé l'examen du processus opérationnel d'EAS.

10. Le travail mené sur le terrain pour les besoins de cet audit a été achevé en grande partie le 1er avril 2014.

Énoncé d'assurance

11. Des procédures suffisantes et appropriées ont été suivies, et des données probantes ont été réunies afin de soutenir l'exactitude des conclusions de l'audit. Les constatations et les conclusions de l'audit ont été basées sur une comparaison des conditions qui existaient au moment de l'audit selon des critères établis convenus avec la direction. Cet engagement a été réalisé conformément aux Normes relatives à l'audit interne au sein du gouvernement du Canada et aux Normes internationales pour la pratique professionnelle de l'audit interne. Une inspection des pratiques professionnelles n'a pas été effectuée.

Constatations détaillées et recommandations

Documents et processus en matière de sécurité

12. Nous nous attendions à ce que SPC respecte les politiques et directives relatives à la sécurité du gouvernement. Nous avons examiné les produits de SPC conçus pour respecter les exigences du CT, notamment le plan de sécurité ministériel (PSM) de SPC et l'ébauche de la Politique sur la sécurité ministérielle (PSSM). SPC respectait les exigences clés relatives à la sécurité du CT. Des exceptions mineures ont été relevées concernant la Norme relative à la gestion de la sécurité de la technologie de l'information (NGSTI) du CT et la direction a convenu de les rectifier une fois que l'examen des NGSTI serait achevé.

13. Tout au long de l'élaboration du PSM, on a mené des consultations à l'interne et à l'externe afin de s'assurer de la validité de l'information présentée. Le processus consultatif a permis de dresser la liste des plus hauts risques auxquels fait face SPC, ainsi qu'à une analyse approfondie pour mesurer la probabilité et l'incidence de ces risques liés à la sécurité, et la façon dont ils pourraient toucher l'atteinte des résultats stratégiques et opérationnels de SPC. Ce travail a conduit à l'établissement d'un plan de mise en œuvre comprenant les contrôles recommandés pour pallier cet écart, les ressources requises et la date d'achèvement prévue.

14. Conformément à la *Politique sur la sécurité du gouvernement* du CT, le Ministère a élaboré et approuvé un PSM qui a décrit les objectifs de contrôle de la sécurité, les lacunes et leurs plans d'action, ainsi que les rôles et les responsabilités liés à la mesure du rendement et à l'établissement de rapports. Nous avons constaté que SPC a mis en œuvre la plupart des contrôles de sécurité dont la mise en œuvre était prévue pour la fin de l'exercice financier 2013-2014. Ces contrôles, bien qu'ils n'aient pas été mis en œuvre au moment de l'audit, étaient à jour pour l'achèvement de leurs échéances.

15. Le Ministère possédait un PSSM documenté et approuvé. Le PSSM était le principal instrument pour communiquer les rôles, les responsabilités et les obligations redditionnelles concernant la sécurité à SPC. Bien que la communication du PSSM n'était pas obligatoire, la direction prévoyait communiquer la politique aux employés.

16. Nous avons conclu que SPC avait élaboré des politiques et des procédures qui étaient conformes aux exigences décrites dans la plupart des politiques du CT. Les rôles et les responsabilités étaient définis dans le cadre de politique et des plans de communication au personnel avaient été établis. On surveillait les mesures de sécurité et on établissait des rapports connexes. Des progrès étaient réalisés pour que la mise en œuvre complète soit achevée en temps opportun. De plus, on communiquait régulièrement avec les représentants du Secrétariat du Conseil du Trésor du Canada pour veiller au respect continu des politiques de sécurité gouvernementales.

Le processus d'EAS

17. Dans le cadre des activités de gestion des risques requises par la *Politique sur la sécurité du gouvernement* du CT, nous nous attendions à ce que SPC mette en œuvre les activités de gestion du risque pour les applications de la TI. Nous nous attendions également à ce que SPC applique le processus d'EAS à mesure que les systèmes de la TI ministériels étaient mis en œuvre.

18. Nous avons noté que SPC avait mis en œuvre un cadre de gestion des risques, conformément à la politique du CT. Le Cadre de gestion des risques pour la sécurité de la technologie de l'information (le Cadre) a été approuvé le 1er avril 2012 par le DPIS et le directeur principal, Sécurité et gestion de l'identité. Le Cadre a été élaboré par SPC, en collaboration avec le CT et le Centre de la sécurité des télécommunications Canada (CSTC), afin de mettre en œuvre un cadre de gestion continue des risques, conformément au guide de sécurité ITSG-33 du CSTC. L'ancien processus de certification et d'accréditation a été renommé le processus d'EAS. Un guide élaboré par la sécurité de la TI a été transmis aux employés afin qu'ils l'utilisent avec le Cadre.

19. Il n'était pas clair de qui relevait le Cadre de SPC. Le DPIS, qui était responsable des applications ministérielles, et le directeur général, directeur général, Transformation cybernétique et sécurité de la TI (DG TCSTI), qui était responsable de toutes les applications non-ministérielles, ont indiqué être responsables du Cadre. Le manque de clarté quant à l'appartenance du Cadre pourrait avoir une incidence sur les communications liées au processus d'EAS, ainsi qu'à son application et sa surveillance. De plus, cette question pourrait donner lieu à deux processus d'EAS au sein de SPC, ce qui entrainerait davantage de confusions.

20. Nous avons déterminé qu'il y avait 23 applications ministérielles de la TI qui ont été mises en œuvre pendant la période visée par le présent audit. Ces applications étaient requises pour que l'EAS soit réalisée conformément à la *Politique sur la sécurité du gouvernement* du CT. Nous avons constaté que le processus d'EAS n'a été appliqué pour aucune de ces applications.

21. Nous avons rencontré les six gestionnaires de projet responsables de la mise en œuvre de ces 23 applications. Les gestionnaires de projet ont indiqué trois raisons clés pour expliquer pourquoi l'EAS n'avait pas été réalisée pour ces applications : manque de compréhension envers le processus, le processus d'EAS n'était pas inclus dans les calendriers de mise en œuvre des projets et le niveau d'effort n'était pas adapté aux risques liés aux applications.

22. Nous avons remarqué que les communications de la haute direction sur les exigences relatives au processus d'EAS étaient limitées. Le premier message concernant le processus d'EAS datait de septembre 2013 et provenait du gestionnaire de la sécurité de la TI. Avant ce message, un seul des six gestionnaires interrogés avait reçu de l'information concernant le processus d'EAS à SPC. La teneur du processus prévu à SPC n'était pas claire pour les gestionnaires, bien que certains d'entre eux possédaient déjà de l'expérience relative au processus d'EAS avant de se joindre à SPC. Certains ont indiqué que des messages clairs de la part de la haute direction auraient fait en sorte que le processus aurait été appliqué de manière plus uniforme.

23. Le Cadre de SPC, ainsi que le Guide, indiquait que les gestionnaires de projet devaient appliquer le processus d'EAS dans le cadre du cycle de vie des projets. Bien que SPC a défini et mis en œuvre un cadre de gouvernance de projet, nous avons remarqué que le processus d'EAS n'était pas intégré dans la méthodologie de gestion de projet existante. Une intégration précoce de l'EAS dans le cycle de vie du projet dans le cadre de la méthodologie de gestion de projet, permettrait d'améliorer les mesures de contrôle pour veiller à ce que le processus d'EAS soit achevé.

24. Au cours des consultations, des gestionnaires ont soulevé des préoccupations concernant le temps et les ressources nécessaires pour appliquer le processus d'EAS correctement. La nécessité de mettre en œuvre rapidement les applications ministérielles a parfois donné

lieu à des pressions pour que l'on contourne le processus de certification. Plusieurs des personnes interrogées ne croyaient pas pouvoir remplir les formalités administratives requises dans des délais si courts. Par conséquent, ils acceptaient les risques liés à la non-réalisation du processus. Nous avons observé qu'il y avait un manque de contrôles pour s'assurer que les applications aient été mises en œuvre après avoir achevé un processus d'EAS.

25. La haute direction et les gestionnaires de projets ont indiqué que le processus d'EAS devait être adapté aux risques connexes et qu'il fallait éviter d'appliquer le même processus pour chaque application sans tenir compte du niveau de risque. Par exemple, une application disponible sur le marché qui est utilisée par plusieurs autres ministères ne devrait pas nécessiter le même niveau d'examen qu'une nouvelle application développée à l'interne. Le processus d'EAS n'était pas jugé comme étant flexible. Plusieurs des applications mises en œuvre à SPC au cours de la période visée par l'audit étaient bien connues et étaient des applications plus couramment utilisées au sein du gouvernement comme Windows 7, PeopleSoft et SAP.

26. SPC a documenté et approuvé le Cadre qui exigeait le processus d'EAS. Les rôles et responsabilités pour réaliser l'EAS étaient définis dans le Cadre de SPC. L'exécution du processus d'EAS pour les applications ministérielles était limitée et toutes les applications ont été mises en œuvre sans avoir fait l'objet d'une EAS. À défaut de réaliser l'EAS, ceci a donné lieu au non-respect du Cadre de SPC. De plus, cela signifie que les activités de gestion des risques requises par la *Politique sur la sécurité du gouvernement* du CT n'ont pas été réalisées. Par conséquent, nous n'avons pas été en mesure de déterminer si les risques de sécurité de la TI liés à chaque application ont été déterminés et atténués.

Recommandation 1

La sous-ministre adjointe principale, Services ministériels, devrait préciser et communiquer l'appartenance du Cadre de gestion des risques pour la sécurité de la technologie de l'information, ainsi que les rôles et les responsabilités connexes, entre le Dirigeant principal de l'information et de la sécurité et le Directeur général, Transformation cybernétique et sécurité de la technologie de l'information.

Réponse de la direction :

La Sous-ministre adjointe principale (SMAP), Services ministériels (SM), est d'accord avec cette recommandation.

Le DPIS et le DG TCSTI, de la Direction générale de la transformation, de la stratégie de service et de la conception discutent fréquemment des questions liées aux risques liés à la sécurité et à l'évaluation de la sécurité.

L'Annexe C de la Politique sur la sécurité ministérielle de SPC, publiée le 21 mai 2014, contient les rôles et les responsabilités en matière de sécurité de la TI des trois directions générales qui ont des responsabilités en matière de sécurité de la TI. En outre, une matrice RACI[i] *est* en cours d'élaboration.

[i] Matrice RACI (responsable, agent comptable, consulté, informé)

Recommandation 2

La sous-ministre adjointe principale, Services ministériels, devrait élaborer et mettre en œuvre un plan de communication, indiquant notamment l'engagement des niveaux appropriés de gestion, aux intervenants participant à la mise en œuvre de systèmes ministériels de la technologie de l'information.

Réponse de la direction :

La SMAP SM est d'accord avec cette recommandation.

Il est important que les gestionnaires de projet comprennent les risques en matière de sécurité inhérents au déploiement d'applications et de systèmes et que l'autorisateur accepte ou n'accepte pas le niveau de risque évalué. L'autorisateur est le Directeur général des SM responsable de la gestion de l'application ou du système ministériel évalué.

Recommandation 3

Le sous-ministre adjoint principal, Projets et relations avec les clients, devrait intégrer le processus d'évaluation et autorisation de sécurité pour les applications ministérielles dans la méthodologie de gestion de projet de Services partagés Canada.

Réponse de la direction :

Le SMAP, Projets et relations avec les clients (PRC) est d'accord avec cette recommandation.

Le Centre d'excellence en gestion de projet de la Direction générale des PRC a établi un processus rigoureux de gestion des projets de la technologie de l'information. L'adoption de cette méthode aux applications ministérielles devrait permettre de veiller à ce que le processus d'EAS soit suivi convenablement pour les projets de développement d'applications.

Recommandation 4

La sous-ministre adjointe principale, Services ministériels, devrait réviser le processus d'évaluation et autorisation de sécurité pour prendre en compte les risques liés à l'application mise en œuvre.

Réponse de la direction :

La SMAP SM est d'accord avec cette recommandation.

Le DPIS entreprend une stratégie de gestion du portefeuille des applications pour évaluer la liste des états finaux des applications ministérielles de SPC. Cette stratégie fournira une liste des applications qui nécessiteront un processus d'EAS.

Recommandation 5

La sous-ministre adjointe principale, Services ministériels, devrait mettre en œuvre des contrôles qui permettent de s'assurer que le processus d'évaluation et autorisation de sécurité est achevé de manière appropriée avant la mise en œuvre des applications ministérielles.

Réponse de la direction :

La SMAP SM est d'accord avec cette recommandation.

Conclusion

27. Le présent audit visait à déterminer si SPC mettait en œuvre un cadre de politique de sécurité qui était conforme aux politiques en matière de sécurité du CT et que les processus d'EAS étaient en place et fonctionnaient comme prévu.

28. SPC a élaboré un cadre de politique de sécurité qui était conforme avec la plupart des politiques gouvernementales clés, bien que des exceptions mineures ont été soulevées. Un PSM a été établi et décrit les rôles et responsabilités définis, les fonctions de surveillance et d'établissement de rapports, ainsi que les fonctions de mesure du rendement qui doivent faire l'objet d'une amélioration approfondie. Un PSSM a été élaboré et approuvé par la présidente de SPC. Un message à l'intention des employés de SPC était sur point d'être envoyé.

29. SPC a documenté et approuvé le Cadre qui exigeait l'application du processus d'EAS. L'appartenance de ce document n'ayant pas été déterminée entre le DPIS et le DG, a donné lieu à des répercussions sur la responsabilité relative à l'application du processus.

30. Nous avons constaté que les rôles et les responsabilités pour l'exécution de l'EAS ont été définis dans le Cadre de SPC, ainsi que dans le Guide. Le Cadre et le Guide étaient disponibles aux employés de SPC.

31. Aucune des applications ministérielles de la TI mises en œuvre au cours de la période visée par le présent audit n'avait complété le processus d'EAS. Nous avons seulement été capables de relever quelques applications pour lesquelles certains des documents étaient remplis. Les gestionnaires de projet ont confirmé qu'ils ont mis en œuvre les applications sans réaliser l'EAS, car le processus était considéré trop long pour répondre aux exigences de mise en œuvre.

32. Les personnes responsables du processus d'EAS ont suggéré qu'une activité de mise en œuvre appuyée par des messages du DPIS donnerait lieu à une augmentation de l'application du processus.

33. Il faut tenir compte de l'adaptabilité du processus et des ressources requises pour remplir les documents requis, ainsi que des contrôles pour veiller à l'achèvement du processus d'EAS avant la mise en œuvre d'une application ministérielle. Intégrer le processus d'EAS dans la méthodologie de gestion de projet pourrait augmenter le taux de conformité.

Réponse et plans d'action de la direction

Recommandation 1

La sous-ministre adjointe principale, Services ministériels devrait préciser et communiquer l'appartenance du Cadre de gestion des risques pour à la sécurité de la technologie de l'information, ainsi que les rôles et les responsabilités connexes, entre le Dirigeant principal de l'information et de la sécurité et le Directeur général, Transformation cybernétique et sécurité de la technologie de l'information.

PLAN D'ACTION DE LA DIRECTION	POSTE RESPONSABLE	DATE D'ACHEVEMENT
Des réunions trimestrielles trilatérales seront prévues avec le Dirigeant principal de l'information et de la sécurité, le Directeur général, Transformation cybernétique et sécurité de la technologie de l'information (TI), de la Transformation, stratégie de services et conception et le Directeur Général de la sécurité de la TI Opérations. Le Cadre de gestion des risques pour la sécurité de la TI constituera un point permanent à l'ordre du jour. Résultats attendus : Les rôles et les responsabilités en matière de gestion du risque pour la sécurité de la TI sont clairs.	Sous-ministre adjointe principale, Services ministériels	30 septembre 2014

Recommandation 2

La sous-ministre adjointe principale, Services ministériels devrait élaborer et mettre en œuvre un plan de communication, indiquant notamment l'engagement des niveaux appropriés de gestion, aux intervenants participant à la mise en œuvre de systèmes ministériels de la technologie de l'information.

PLAN D'ACTION DE LA DIRECTION	POSTE RESPONSABLE	DATE D'ACHEVEMENT
Le Dirigeant principal de l'information et de la sécurité collaborera avec les Communications internes afin de concevoir le plan de communication le plus efficace et le plus approprié, et de mettre celui-ci en œuvre rapidement. Résultats attendus : La sensibilisation à l'égard de l'importance de la gestion des risques pour la sécurité de la technologie de l'information est considérée comme un résultat de ce plan d'action et de celui qui correspond à la recommandation nº 3.	Sous-ministre adjointe principale, Services ministériels	31 mars 2015 et en cours

Recommandation 3

Le sous-ministre adjoint principal, Projets et relations avec les clients devrait intégrer le processus d'évaluation et autorisation de sécurité pour les applications ministérielles dans la méthodologie de gestion de projet de Service partagés Canada.

PLAN D'ACTION DE LA DIRECTION	POSTE RESPONSABLE	DATE D'ACHEVEMENT
Le Dirigeant principal de l'information et de la sécurité (DPIS) discutera avec le Centre d'excellence en gestion de projet (CEGP) afin de s'assurer que le processus d'Évaluation et autorisation de sécurité est intégré dans la méthode de gestion de projet de SPC pour les projets de développement d'applications. Le DPIS, par l'intermédiaire d'une communication continue, veillera à ce que la méthode du CEGP soit utilisée pour ses projets de développement d'applications. Résultats attendus : La gestion des risques liés à la sécurité est incluse dans le cycle de vie du projet de développement d'applications.	Sous-ministre adjointe principale, Projets et relations avec les clients	31 mars 2015

Recommandation 4

La sous-ministre adjointe principale, Services ministériels devrait réviser le processus d'évaluation et autorisation de sécurité pour prendre en compte les risques liés à l'application mise en œuvre.

PLAN D'ACTION DE LA DIRECTION	POSTE RESPONSABLE	DATE D'ACHEVEMENT
Le processus d'Évaluation et autorisation de sécurité sera conçu pour indiquer un niveau de risque faible, moyen ou élevé pour chacune des applications de la technologie de l'information. Le Dirigeant principal de l'information et de la sécurité fournira de l'expertise en matière d'EAS à l'appui des exigences d'EAS qui se rapportent aux clients. Résultats attendus : Les applications et les systèmes ministériels seront évalués et autorisés adéquatement avant d'être	Sous-ministre adjointe principale, Services ministériels	31 mars 2015

déployés.		

Recommandation 5

La sous-ministre adjointe principale, Services ministériels devrait mettre en œuvre des contrôles qui permettent de s'assurer que le processus d'évaluation et autorisation de sécurité est achevé de manière appropriée avant la mise en œuvre des applications ministérielles.

PLAN D'ACTION DE LA DIRECTION	POSTE RESPONSABLE	DATE D'ACHEVEMENT
Les plans d'action de gestion pour les recommandations 2, 3 et 4 donneront suite à cette observation. Le renforcement de la communication permettra de veiller à ce que les gestionnaires de projet comprennent le processus d'Évaluation et autorisation de sécurité (EAS). L'adoption de la méthode du Centre d'excellence en gestion de projet de la Direction générale des projets et des relations avec les clients établira le cadre et les mécanismes de contrôle nécessaires à chaque étape de développement des applications ministérielles. Résultats attendus : Des contrôles sont en place pour s'assurer que le processus d'EAS est suivi correctement, au besoin, avant que les applications ministérielles soient déployées.	Sous-ministre adjointe principale, Services ministériels	31 mars 2015

Annexe A : Critères d’audit

Les critères suivants ont servi à effectuer l’audit :

1. SPC a élaboré et mis en œuvre des politiques et des procédures qui veillent à ce que des activités liées à la sécurité soient établies en conformité avec les politiques gouvernementales existantes;
2. Par l’entremise de l’application du processus d’EAS, SPC a traité les risques de sécurité liés à l’utilisation des systèmes ministériels de la TI pour appuyer les activités opérationnelles de SPC.

Annexe B : Acronymes

Acronyme	Signification de l'acronyme
CEGP	Centre d'excellence en gestion de projet
CSTC	Centre de la sécurité des télécommunications Canada
CT	Conseil du Trésor du Canada
DG TCSTI	Directeur général, Transformation cybernétique et sécurité de la technologie de l'information
DPIS	Dirigeant principal de l'information et de la sécurité
EAS	Évaluation et autorisation de sécurité
NGSTI	Norme relative à la gestion de la sécurité de la technologie de l'information
PRC	Projets et relations avec les clients
PSM	Plan de sécurité ministériel
PSSM	Politique sur la sécurité ministérielle
SM	Services ministériels
SMAP	Sous-ministre adjoint(e) principal(e)
SPC	Services partagés Canada
TI	Technologie de l'information
TSSC	Transformation, stratégie de services et conception