Deloitte.

Vérification interne de la gouvernance de la GI-TI

Commissariat à la protection de la vie privée du Canada

Le 24 mars 2015
Rapport finale

Table des matières

1. Sommaire exécutif 1

Renseignements généraux et contexte 1

Résumé des constatations 2

Conclusion 2

Déclaration de conformité 3

2. Objectif, portée et méthodologie de la vérification 4

Contexte 4

Objectif et portée de la vérification 5

Méthodologie de la vérification 5

3. Constatations et recommandations 7

Forces relevées 7

Conclusions de la vérification 7

Conclusion n^{o} 1 : Planification stratégique de la GI-TI 7

Conclusion n° 2 : Surveillance des applications et des changements 9

Conclusion n° 3 : Gestion des projets liés à la GI-TI 12

Appendice A – Personnes interrogées 15

Appendice B – Critères de vérification 16

1. Sommaire exécutif

Renseignements généraux et contexte

Le Commissariat à la protection de la vie privée du Canada (le Commissariat) est chargé de surveiller le respect de la *Loi sur la protection des renseignements personnels*, qui porte sur les pratiques de traitement des renseignements personnels utilisées par les ministères et organismes fédéraux, ainsi que de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), la loi fédérale sur la protection des renseignements personnels dans le secteur privé.

Le commissaire à la protection de la vie privée du Canada est un haut fonctionnaire du Parlement qui relève directement de la Chambre des communes et du Sénat. Il enquête sur les plaintes qui sont déposées par des personnes à l'endroit du gouvernement du Canada et d'entreprises du secteur privé de manière indépendante de tout autre secteur du gouvernement.

Le Commissariat a élaboré une stratégie de gestion de l'information et de la technologie de l'information (GI-TI) pour 2014-2017, ainsi qu'un plan de GI-TI distinct et plus détaillé pour 2015. Les organismes de gouvernance en place aux fins de la GI-TI sont le Comité de direction (CD) du Commissariat, regroupant un représentant de chaque direction générale (DG), ainsi que le Comité de suivi des changements (CSC), composé de représentants du niveau des gestionnaires. Le directeur de la GI-TI agit à titre de dirigeant principal de l'information, sous l'autorité du directeur général de la Gestion intégrée du Commissariat. Ce groupe comprend 22 équivalents temps plein (ETP), et il est doté d'un budget annuel d'environ 1,7 million de dollars en salaires. Son budget de fonctionnement s'élève à 1,1 million de dollars.

Même si l'organisation est relativement petite, en raison de la nature de son travail et de son mandat stratégique, le Commissariat a indiqué qu'il estimait pouvait compter sur une solide infrastructure de TI qui fait la promotion d'activités hautement efficaces tout en assurant la solidité du positionnement en matière de TI.

Le Commissariat a connu une très forte croissance au cours de la dernière décennie, et des événements d'importance ont touché la GI-TI dans les dernières années. Après son déménagement dans un nouvel édifice en février 2014, le Commissariat a, durant l'exercice 2014-2015, effectué une évaluation des menaces et des risques (EMR) à l'échelle de l'organisation pour évaluer les menaces et les risques pour la sécurité de l'information, des programmes, des systèmes, des services et des espaces physiques du Commissariat.

L'objectif préliminaire de la vérification consistait à offrir au commissaire l'assurance du caractère adéquat et de l'efficacité de la gouvernance, de la gestion des risques et des contrôles qui appuient les processus de GI et de TI du Commissariat. Selon l'évaluation des risques au moment de la planification, la portée de la vérification a été définie de façon à inclure les processus de gouvernance de la GI-TI, y compris la gouvernance de la capacité en GI-TI des RH, les applications de GI-TI, la gestion du changement liée aux systèmes de TI ainsi que les processus de gestion des projets facilités par la GI-TI.

Résumé des constatations

Les principales observations découlant de la vérification sont présentées ci-dessous :

Forces

- Le Commissariat a élaboré une stratégie de GI-TI pour 2014-2017 qui définit l'orientation en matière de GI-TI du Commissariat et s'harmonise avec les priorités et la vision organisationnelle du Commissariat.
- L'équipe de la GI-TI du Commissariat possède l'expérience et les compétences nécessaires pour exécuter un grand nombre d'initiatives de GI-TI.
- Le Commissariat a élaboré des documents de projet, y compris des chartes de projet, des plans de projet et des exigences fonctionnelles, pour les grands projets axés sur la GI-TI examinés dans le cadre de la vérification. Il s'agit notamment du Renouvellement du Ci2, un système de gestion de cas, et d'Officium, un système électronique de gestion des documents et des dossiers.
- Pour augmenter l'adoption d'Officium au Commissariat et améliorer l'expérience des utilisateurs, la GI-TI a récemment mené de nombreuses activités de communication et de gestion des changements auprès des utilisateurs finaux liées à la mise en œuvre du système électronique de gestion des documents et des dossiers.

Constatations

- Même si le Commissariat a élaboré une stratégie de GI-TI (ainsi qu'un plan d'appui en matière de GI-TI), ces documents n'ont pas fait l'objet de discussions officielles avec la haute direction ou n'ont pas été approuvés par elle. De plus, il n'existe pas de processus structuré pour des communications ni de mises à jour régulières entre la GI-TI et la haute direction.
- Les responsables des applications opérationnelles n'ont pas officiellement été identifiés ou définis pour les applications de TI du Commissariat. De plus, le CSC assume actuellement les fonctions d'un comité de GI-TI de la direction plutôt que d'un comité consultatif sur les changements qui définirait la façon dont les changements apportés aux applications de TI seraient approuvés.
- Il n'existe aucun cadre officiel de gestion des projets de GI-TI, ni de programme officiel de signalement des avantages obtenus à la haute direction.

Conclusion

Conformément aux observations susmentionnées et à la portée générale de la vérification, le Commissariat éprouve quelques légers problèmes en ce qui a trait à l'efficacité de ses processus de gouvernance de GI-TI actuels. Les recommandations incluses dans le présent rapport visent à renforcer ces processus. Les réponses de la direction sont présentées à la fin de chaque constatation.

La vérification et le rapport qui en découle ont été réalisés à l'intention de la direction du Commissariat. L'utilisation du rapport à d'autres fins pourrait ne pas être appropriée.

Déclaration de conformité

Selon notre jugement professionnel, des procédures de vérification suffisantes et adaptées ont été appliquées et des données ont été recueillies à l'appui de l'opinion fournie et contenue dans le présent rapport. Cette opinion se fonde sur la comparaison des conditions qui prévalaient au moment de la vérification, en fonction des critères de vérification convenus avec la direction. Elle s'applique uniquement aux processus vérifiés. La vérification a été menée conformément aux Normes relatives à la vérification interne du gouvernement du Canada. Nous avons recueilli des éléments de preuve pour fournir à la haute direction une assurance raisonnable de l'exactitude des conclusions tirées de la vérification.

2. Objectif, portée et méthodologie de la vérification

Contexte

Le Commissariat à la protection de la vie privée du Canada (le Commissariat) est chargé de surveiller le respect de la *Loi sur la protection des renseignements personnels*, qui porte sur les pratiques de traitement des renseignements personnels utilisées par les ministères et organismes fédéraux, ainsi que de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), la loi fédérale sur la protection des renseignements personnels dans le secteur privé.

Le commissaire à la protection de la vie privée du Canada est un haut fonctionnaire du Parlement qui relève directement de la Chambre des communes et du Sénat. Il enquête sur les plaintes qui sont déposées par des personnes à l'endroit du gouvernement du Canada et d'entreprises du secteur privé de manière indépendante de tout autre secteur du gouvernement.

En sa qualité de défenseur du droit des Canadiennes et des Canadiens à la protection de la vie privée, le commissaire :

- enquête sur les plaintes, mène des vérifications et intente des poursuites judiciaires en vertu de deux lois fédérales;
- publie de l'information sur les pratiques relatives au traitement des renseignements personnels dans les secteurs public et privé;
- appuie et effectue des recherches sur des enjeux liés à la protection de la vie privée, et en fait connaître les conclusions;
- sensibilise la population aux enjeux touchant la protection de la vie privée et les lui faire comprendre.

Le Commissariat a élaboré une stratégie de GI-TI pour 2014-2017, ainsi qu'un plan de GI-TI distinct et plus détaillé pour 2015. Les organismes de gouvernance en place aux fins de la GI-TI sont le Comité de direction (CD du Commissariat, regroupant un représentant de chaque direction générale (DG), ainsi que le Comité de suivi des changements, composé de représentants du niveau des gestionnaires.

Le directeur de la GI-TI agit à titre de dirigeant principal de l'information, sous l'autorité du directeur général de la Gestion intégrée du Commissariat. Ce groupe comprend 22 ETP, et il est doté d'un budget annuel d'environ 1,7 million de dollars en salaires. Son budget de fonctionnement s'élève à 1,1 million de dollars. La GI-TI est responsable de la prestation de conseils et de directives en matière de GI-TI ainsi que de la gestion, de la coordination, du suivi et de la production de rapports pour tous les investissements en GI-TI tout au long du cycle de vie de la GI-TI.

Même s'il s'agit d'une organisation relativement petite, compte tenu de la nature de son travail et de son mandat stratégique, le Commissariat a indiqué qu'il croyait important de pouvoir compter sur une solide infrastructure de TI qui fait la promotion d'activités très efficaces tout en assurant un positionnement de force en matière de sécurité de la TI qui respecte les exigences de la politique du Secrétariat du Trésor sur la sécurité.

Le Commissariat a connu une très forte croissance au cours de la dernière décennie, et des événements d'importance ont touché la GI-TI dans les dernières années. Après son déménagement dans un nouvel édifice en février 2014, le Commissariat a, durant l'exercice 2014-2015, effectué une évaluation des menaces et des risques (EMR) à l'échelle de l'organisation pour évaluer les menaces et les risques pour la sécurité de l'information, des programmes, des systèmes, des services et des espaces physiques du Commissariat.

Objectif et portée de la vérification

L'objectif préliminaire de la vérification consistait à fournir au commissaire l'assurance du caractère adéquat et de l'efficacité de la gouvernance, de la gestion des risques et des contrôles qui appuient les processus de GI et de TI du Commissariat.

L'étape de planification de la vérification a consisté en une évaluation à grande échelle des risques de GI-TI pour le Commissariat, y compris l'animation d'un atelier sur les risques auquel participaient des représentants de la GI-TI et de toutes les directions. Selon l'évaluation des risques au moment de la planification, la portée de la vérification a été définie de façon à inclure les processus de gouvernance de la GI-TI, y compris la gouvernance de la capacité en GI-TI des RH, les applications de GI-TI, la gestion du changement liée aux systèmes de TI ainsi que les processus de gestion des projets facilités par la GI-TI. La période de vérification s'échelonnait du 1er avril 2013 au 31 décembre 2014.

Méthodologie de la vérification

L'approche et la méthodologie utilisées pour la vérification sont conformes aux normes de vérification interne énoncées par l'Institut des vérificateurs internes (IVI) ainsi qu'à la Politique sur la vérification interne du gouvernement du Canada.

À titre d'agent du Parlement, le Commissariat travaille indépendamment du gouvernement du Canada et même s'il n'est donc pas tenu de participer aux initiatives lancées au sein de la fonction publique pour améliorer la gestion, il compte assurer la conformité avec ces pratiques. Le Commissariat est fermement résolu à atteindre une norme d'excellence organisationnelle, à appliquer de saines pratiques de gestion des activités et à améliorer son rendement de façon continue. Par conséquent, les cadres de contrôle suivants ont été mis à contribution pour la vérification :

- le cadre des contrôles de gestion de base (CGB) et des critères de vérification définis par le Bureau du contrôleur général (BCG);
- le Cadre de responsabilisation de gestion (CRG) qui énonce les attentes du Conseil du Trésor à l'égard des cadres supérieurs de la fonction publique en matière de saine gestion de la fonction publique.

On a également inclus d'autres critères pour assurer un traitement approprié, compte tenu de la portée de la vérification.

La vérification comprenait une phase de planification prolongée qui tenait compte à l'origine de l'ensemble des risques en matière de GI-TI du Commissariat. Les risques préliminaires ont été déterminés par des entrevues et l'examen de documents, puis regroupés en énoncés de risque, qui ont été présentés et soumis au vote au cours d'un atelier sur le risque auquel ont participé des représentants de diverses directions du Commissariat. Durant l'atelier, on a tenu compte du risque résiduel, c.-à-d. le niveau de risque déterminé par les participants suivant les mesures de contrôle et les pratiques que ces derniers estimaient être en cours au moment de l'atelier. En s'appuyant sur les risques déterminés au cours de la phase de planification de la vérification, on a mis au point un programme de vérification fondé sur le risque pour décrire en détail les modalités de traitement de l'objectif, des critères et des risques de

la vérification. Le programme de vérification comprenait les procédures suivantes :

- Entrevue avec le Directeur des Services de GI-TI pour mieux comprendre certains aspects particuliers des processus de GI-TI (voir l'appendice A);
- Entrevues avec des directeurs pour obtenir leurs points de vue sur des sujets propres à la GI-TI (voir l'appendice A);
- Examen du mandat actuel et du mandat révisé des comités de gouvernance;
- Examen des ordres du jour et des comptes rendus de réunion des comités de gouvernance;
- Examen des processus de gestion des projets de TI, y compris la documentation préparée pour les projets Officium et Ci2;
- Examen des produits relatifs aux communications de la GI-TI (p. ex. bulletins, courriels).

La vérification s'est déroulée selon le calendrier suivant :

- Phase de planification : octobre 2014 – novembre 2014
- Phase d'exécution : novembre 2014 – décembre 2014
- Phase de rapport : janvier 2015 – février 2015
- Présentation au comité de vérification du Commissariat : mars 2015

3. Constatations et recommandations

Forces relevées

Les forces ci-dessous concernent l'approche actuelle de la recherche appliquée :

- Le Commissariat a élaboré une stratégie de la GI-TI pour 2014-2017 qui établit l'orientation de la GI-TI du Commissariat et l'harmonise avec les priorités et la vision générales du Commissariat.
- L'équipe de la GI-TI du Commissariat est expérimentée, hautement qualifiée, et elle gère un volume élevé d'initiatives de la GI-TI.
- Le Commissariat a préparé la documentation, y compris les chartes et les plans de projet et les exigences fonctionnelles, pour les projets d'envergure fondés sur la GI-TI qui ont été examinés dans le cadre de la vérification (p. ex. renouvellement du Ci2, qui est un système de gestion des cas, et Officium, qui est un système de gestion électronique des documents et des dossiers).
- Afin d'accroître l'utilisation d'Officium au sein du Commissariat ainsi que l'expérience de l'utilisateur, la GI-TI a entrepris dernièrement un grand nombre d'activités liées à la communication et à la gestion du changement qui portent sur la mise en œuvre du système de gestion électronique des documents et des dossiers et qui sont destinées aux utilisateurs.

Conclusions de la vérification

Conclusion n^{o} 1 : Planification stratégique de la GI-TI

Puisque la GI-TI joue un rôle critique dans la réalisation des priorités ministérielles, l'équipe de vérification s'attendait à ce qu'il existe[1] une stratégie de GI-TI globale harmonisée avec les priorités et la vision générales du Commissariat, élaborée après consultation avec les secteurs d'activité et approuvée par la haute direction. Elle s'attendait aussi à ce que la haute direction reçoive des comptes rendus périodiques sur les plans et les initiatives en matière de GI-TI. Compte tenu de la taille de l'organisation du Commissariat, les activités de gestion et de gouvernance de la GI-TI n'exigent pas nécessairement de nombreux processus et niveaux d'approbation, mais ces derniers devraient être officiels et constants.

Le Commissariat a élaboré une stratégie de la GI-TI 2014-2017 (ainsi qu'un plan d'appui de la GI-TI 2015) conforme à la vision et aux priorités générales du Commissariat. Bien que la GI-TI ait sollicité la rétroaction de chaque secteur d'activité (par l'intermédiaire de discussions entre le Directeur de la GI-TI et les directeurs généraux de chaque direction) pour élaborer la stratégie et le plan, ces derniers n'ont pas fait l'objet de discussions avec la haute direction, et elle ne les a pas encore approuvés (au 31 décembre 2014). Le directeur de la GI-TI a constaté que seule une direction a commenté l'ébauche de stratégie.

[1] Pour de plus amples renseignements, voir les cinq processus du COBIT liés aux fonctions Évaluer, Diriger et Surveiller (EDS), p. ex. EDS01 Assurer l'établissement et l'entretien du cadre de gouvernance, qui comprend la méthode de gouvernance EDS01.02 Diriger le système de gouvernance, qui stipule ce qui suit : « *Informer les dirigeants et obtenir leur appui, leur adhésion et leur engagement. Orienter les structures, les processus et les méthodes de gouvernance de la TI conformément aux principes de conception de la gouvernance, aux modèles de prise de décision et aux niveaux d'autorisation qui ont été adoptés. Définir l'information nécessaire à la prise de décisions éclairées.* » [Traduction]

Une ébauche de déroulement du travail lié à la stratégie de la GI-TI a été mise au point par la GI-TI afin de décrire le processus d'élaboration de la stratégie; cependant, le document n'a pas été approuvé par la haute direction. L'examen des points à l'ordre du jour des réunions du CD du Commissariat durant la période de vérification a montré que les discussions sur la stratégie de la GI-TI et la planification n'en faisaient pas partie. On a constaté que le CD devait discuter de la stratégie de la GI-TI 2014-2017 en mai 2014, mais qu'en raison d'autres priorités, la discussion a été reportée.

Le plan de la GI-TI 2015 décrit les grandes lignes des projets de GI-TI en cours et futurs, y compris l'estimation des efforts nécessaires à leur réalisation et le calendrier de chaque projet. Suivant l'estimation de l'affectation des ressources, on prévoit l'utilisation à plus de 100 % de quatre postes de GI-TI au sein du Commissariat, ce qui signifie que le nombre ou la taille des initiatives de GI-TI et/ou le niveau de ressources devront probablement être revus. Une liste de projet distincte sert à faire le suivi des projets en cours; cependant, elle ne permet pas de saisir le niveau d'efforts dépensés en réalité ou de concilier de façon permanente l'estimation du niveau d'efforts et le niveau d'efforts réel qui a été consacré aux initiatives en cours et à celles qui sont terminées. La situation des projets ainsi que les contraintes et les risques éventuels en matière de ressources n'ont pas fait l'objet d'un compte rendu officiel au CD.

Incidence

Sans stratégie et plan de GI-TI approuvés, ou de communication/mises à jour officielles périodiques entre l'équipe de la GI-TI et la haute direction, leurs priorités en matière de GI-TI risquent de ne pas correspondre. De plus, la haute direction pourrait ne pas comprendre les risques et les limites liés à la GI-TI, par exemple les différentes priorités établies entre les projets de GI-TI en fonction des contraintes en matière de ressources, ou des problèmes de mise en œuvre posés par des projets qui nécessitent l'intervention de la haute direction. La direction de la GI-TI du Commissariat s'est montrée très réceptive à toutes les demandes des secteurs opérationnels, et la planification comme l'attribution des ressources en matière de GI-TI s'est faite de façon officieuse. Dans le contexte actuel du Commissariat où les ressources sont de plus en plus limitées et où la charge de travail en matière de GI-TI est lourde, il est important que la haute direction comprenne à quel point il est essentiel que l'équipe de la GI-TI puisse répondre aux priorités établies pour le Commissariat. Le manque de communication officielle ou efficace a donné lieu à des questions au sujet de décisions prises il y a plusieurs années, par exemple le choix de SharePoint comme système de gestion de base des documents du Commissariat. Étant donné que certains membres de la haute direction pensent qu'ils n'ont pas suffisamment participé au processus de prise de décision ou qu'ils ne le comprenaient pas assez, ils continuent à poser des questions au sujet de ce choix. Une telle situation a peut-être augmenté la résistance des utilisateurs et nuit à leurs activités de gestion du changement.

Recommandation

1. Nous recommandons que le DG de la Direction générale de la Gestion intégrée s'assure que la haute direction participe au développement de la stratégie et des plans de GI-TI et les approuve officiellement en temps opportun, et qu'elle soit mise au courant de l'état d'avancement des stratégies et des plans de GI-TI approuvés. L'objectif de ces mises à jour est de s'assurer que les projets actuels liés à la GI-TI et futurs sont cohérents avec l'ensemble des priorités et la vision du Commissariat, ainsi que de discuter des décisions prises au sujet de l'attribution des ressources pour veiller à établir des priorités et optimiser les ressources du Commissariat.

Réponse de la direction et plan d'action	Responsabilités et échéancier
Nous acceptons la recommandation et adopterons les mesures suivantes :	DG de la Direction générale de la Gestion intégrée (avril-mai 2015)

Réponse de la direction et plan d'action	Responsabilités et échéancier
1. Nous informerons le CD du flux de travail lié à la stratégie d'IM-IT pour : a. s'assurer que les gens comprennent bien le processus d'élaboration de la stratégie et en particulier le rôle du CD dans ce processus, b. confirmer la meilleure méthode pour tenir le CD informé des mises à jour ou des écarts survenant dans la stratégie et les plans de GI-TI en cours de réalisation. 2. Nous demanderons l'approbation du CD pour la stratégie et les plans de GI-TI 2015-2016. 3. Nous fournirons des mises à jour trimestrielles au CD.	

Conclusion n° 2 : Surveillance des applications et des changements

L'équipe de vérification s'attendait à ce que les principales applications aient été officiellement attribuées à des responsables opérationnels désignés[2]. Même si l'équipe de la GI-TI est responsable de l'entretien et du fonctionnement des applications, c'est le groupe opérationnel qui doit définir les résultats opérationnels attendus (c.-à-d. les exigences) pour la mise en œuvre et l'approbation des décisions au sujet de la façon dont les applications soutiennent les activités. De plus, l'équipe de vérification s'attendait à ce qu'un processus officiel soit mise en œuvre pour cerner, entrer, analyser et approuver les demandes de changement aux applications ainsi qu'établir des priorités entre elles. L'équipe de la GI-TI pourrait faciliter le processus, mais les responsables opérationnels identifiés des applications en resteraient responsables.

Les responsables opérationnels n'ont pas encore été officiellement identifiés, leur rôle n'a pas encore été défini, et ce, pour aucune des applications de TI du Commissariat. Les secteurs opérationnels ont examiné la GI-TI pour prendre en charge le développement et le soutien des applications d'IT ainsi que les activités de gestion connexes, y compris les demandes de changement.

Un cadre de gestion des processus pour les demandes de changements liés aux applications de TI a été documenté en août 2014. La haute direction doit l'approuver. Ce cadre prévoit que l'équipe de la GI-TI établisse des priorités entre les demandes de changements, qui pourront ensuite être envoyées au CSC pour approbation finale. Le CSC n'a pas encore approuvé des demandes de changement. Le processus de gestion du changement documenté se fonde sur un processus similaire utilisé précédemment pour le projet de renouvellement du Ci2. Depuis la fin du projet de renouvellement du Ci2, les demandes de changement sont généralement traitées de façon officieuse.

[2] Pour de plus amples renseignements, voir les processus de COBIT 5 liés aux fonctions Construction, acquisition et mise en œuvre (CAM), par exemple CAM06 Gestion des changements, qui inclut la pratique de gouvernance CAM06.01 Évaluation, établissement de priorités et approbation des demandes de changement, qui stipule qu'il est nécessaire d'évaluer toutes les demandes de changement pour déterminer leur incidence sur les processus opérationnels et les services de TI, ainsi que déterminer si les changements pourraient nuire à l'environnement opérationnel et faire prendre des risques inacceptables. Il faut s'assurer que les changements sont consignés, priorisés, classés, évalués, autorisés, planifiés et programmés. Le personnel de GI-TI s'occupe de ces processus, mais ce sont clairement la haute direction et leurs responsables délégués qui en ont la responsabilité.

En date du 31 décembre 2014, le CSC s'était réuni quatre fois depuis que le processus de gestion du changement officiel a été documenté. Le mandat du CSC indique que son rôle est de superviser la mise en œuvre et la gestion des changements liés aux applications opérationnelles de TI du Commissariat. Le mandat ne stipule pas comment les demandes de changements seront approuvées, et le CSC ne s'est pas encore prononcé sur cette question, ni sur la question de savoir qui devraient être les membres votants (cela pourrait dépendre de l'application pour laquelle un changement est demandé), et enfin, quel est le quorum et comment sont actuellement approuvées les demandes de changement. Le CSC est composé de plus de 28 membres de plusieurs directions du Commissariat, tous identifiés dans le mandat du comité comme des collaborateurs et approbateurs. Jusqu'à présent, les discussions du CSC concernent l'information sur les projets de GI-TI, mais pas sur les demandes de changements en particulier, et aucune décision du CSC n'a été inscrite dans le compte-rendu des réunions.

Incidence

Faute de nominations officielles de responsables opérationnels des applications de TI, l'équipe de la GI-TI, qui ne connaît pas toujours bien les processus opérationnels soutenus par les applications de TI, continue de prendre les décisions en matière de gestion des applications. Les secteurs opérationnels doivent comprendre qu'il existe un lien important entre les processus opérationnels et les applications de TI qui les appuient, et ce, pour qu'ils n'oublient pas de prendre en compte le fait que lorsque des processus opérationnels sont changés, cela a une incidence sur les applications. Il peut s'agir par exemple de la façon dont les données sont entrées ou encodées dans une application existante de TI.

Le CSC fonctionne actuellement comme un comité de gestion de GI-TI qui vérifie l'information avant qu'elle soit présentée au CD. Cette fonction est très utile, mais le CSC ne remplit pas entièrement son mandat de comité consultatif sur le changement, qui devrait définir la façon dont les applications de TI sont approuvées. Il s'agit notamment d'identifier les intervenants qui doivent approuver les changements, par exemple, le responsable opérationnel de l'application de TI et son rôle fonctionnel de soutien comme la sécurité et la protection des renseignements personnels. Sans processus bien défini de conseil sur les changements, le processus pourrait être aussi inefficient (étant donné le nombre actuel de membres du CSC) que peu réaliste quant aux risques encourus (étant donné que les rôles et les responsabilités de chacun ne sont pas clairs).

Recommandations

2. Nous recommandons que la Direction générale de la Gestion intégrée s'assure que des responsables organisationnels soient désignés pour chaque application importante de TI (p. ex. Ci2, Officium, systèmes financiers et systèmes de RH), et que leurs rôles et responsabilités soient clairement définis, leur soient communiqués et qu'ils les acceptent.

Réponse de la direction et plan d'action	Responsabilités et échéancier
Nous sommes d'accord avec la recommandation. L'équipe de la GI-TI élaborera un modèle permettant de désigner des responsables chargés du volet organisationnel d'application dans les directions, mais pas du financement des mises à jour et des mises à niveau des applications. L'équipe de la GI-TI travaillera de concert avec la Direction pour trouver des fonds lorsque cela est nécessaire. Nous devrons plus précisément : 1. Développer une méthode pour définir officiellement, assigner et communiquer les rôles et responsabilités pour les applications importantes du Commissariat; la méthode adoptée visera à appuyer efficacement les	DG, Gestion intégrée (septembre 2015)

opérations de GI-TI tout en prenant en compte les réalités opérationnelles et les contraintes d'une petite organisation. 2. Se concerter et obtenir l'approbation officielle des responsables organisationnels désignés pour les systèmes clés.	

3. Nous recommandons que le directeur de la GI-TI s'assure que les examens et les rôles d'approbation des changements demandés pour les applications du CCB soient mieux définis, et notamment qu'il fournisse des lignes directrices pour désigner les membres votants et leur donner un rôle dans l'approbation des changements pour chaque application clé de TI.

Réponse de la direction et plan d'action	Responsabilités et échéancier
Nous acceptons la recommandation et adopterons les mesures suivantes : 1. Révision de la méthode actuelle de gouvernance du Commissariat, y compris de la composition, des rôles et des responsabilités du CSC et de ses rapports hiérarchiques avec le CD. 2. Révision du mandat du CSC et ajout d'une définition claire des rôles et des responsabilités en matière de prises de décisions. 3. Présentation du mandat révisé au CD et au CSC pour qu'ils comprennent, approuvent et acceptent officiellement les rôles et responsabilités de chacun.	Directeur de la GI-TI (septembre 2015)

Conclusion n° 3 : Gestion des projets liés à la GI-TI

L'équipe de vérification s'attendait à trouver un cadre officiel de gestion des projets comprenant une méthode pour la réalisation de projets liés à la GI-TI, dont des contrôles officiels aux fins d'examen et d'approbation de projets par la haute direction lors d'étapes importantes (p. ex. la planification, l'exécution et le déploiement.[3]. De plus, l'équipe de vérification s'attendait à ce que le cadre prévoie une façon de cerner les bénéfices attendus des projets et de vérifier s'ils avaient été atteints une fois les projets réalisés. Elle s'attendait également à ce qu'un plan de gestion du changement axé sur la personne ait été élaboré et mis en œuvre pour tous les projets de grande envergure concernant la majorité du personnel du Commissariat. Pour une organisation de la taille du Commissariat, les activités de gestion des projets liés à la GI-TI ne nécessitent pas un grand nombre de processus et de niveaux d'approbation, mais il faut s'assurer que les secteurs clés des méthodes liées à la gestion de projet sont pris en compte, y compris l'approbation officielle de la haute direction lors des étapes importantes du projet.

Le Commissariat ne dispose pas d'un cadre officiel de gestion des projets. Malgré tout, le Commissariat a élaboré des documents de projet, dont des chartes de projet, des plans de projet et des exigences de fonctionnement, et ce, pour la plupart des projets axés sur la GI-TI examinés dans le cadre de la présente vérification (p. ex. renouvellement Ci2 et Officium). Même si des documents de projet ont été élaborés, rien ne permet de prouver que la haute direction a donné son approbation lors des étapes clés du projet.

Bien que des critères de succès aient été inclus dans la charte de projet d'Officium, ils étaient très hauts et ne pouvaient pas être mesurés. Il était par exemple indiqué : « Le nouvel environnement est stable" et « Tous les utilisateurs du Commissariat ont reçu une formation adéquate sur le nouvel outil". Officium a été mis en place il y a plus d'un an, mais la haute direction ne sait pas encore si ses critères de succès ont été atteints, car ils n'ont toujours pas été mesurés et ne lui ont pas été communiqués.

Le projet Officium nécessitait une formation approfondie, et un ensemble exhaustif de documents de cours ont été placés sur l'Intranet du Commissariat. Cependant, le projet n'a pas été appuyé par un plan de gestion du changement et de communication axé sur la personne. Un tel plan aurait permis d'analyser le profil des intervenants, en particulier de cerner leurs besoins en information et de déterminer comment des groupes pourraient participer au développement du projet, notamment grâce à un calendrier intégré qui permettrait de déterminer le contenu approprié, le média, le moment de la formation et le matériel de communication convenant à chaque groupe d'intervenant. La direction des RH du Commissariat dispose d'un cadre et de modèles bien développés pour la gestion du changement; cependant, elle a pris part au projet plus tard. Un groupe de travail composé d'utilisateurs de tout le Commissariat a été formé pendant la mise en œuvre du projet, mais il a été dissous après la mise en place d'Officium.

L'équipe de la GI-TI a récemment mené des activités de communication et de gestion du changement auprès des utilisateurs finaux d'Officium. Ils ont notamment mené un sondage auprès des usagers et ont fait appel à la direction des communications du Commissariat pour créer du matériel de communication. On n'a prévu aucun programme officiel permettant d'évaluer l'adoption d'Officium (nombre d'utilisateurs et nombre de dossiers dans chaque direction), ni de communiquer de telles données à la haute direction, ou encore de prévoir des plans d'action pour régler les éventuels problèmes.

Incidence

[3] Pour de plus amples renseignements, voir les processus de COBIT 5 liés aux fonctions Construction, acquisition et mise en œuvre (CAM), par exemple CAM01 Gestion des programmes et des projets, qui inclut la pratique de gouvernance CAM01.01 Application d'une approche normalisée sur la gestion de programmes et de projets, stipulant qu'il est nécessaire d'appliquer une approche normalisée à la gestion de programmes et de projets, ce qui permet d'examiner la gouvernance et la gestion et de mener des activités de gestion permettant d'optimiser les ressources et d'atteindre les objectifs (relatifs aux exigences, risques, coûts, calendrier, qualité) dans tous les secteurs opérationnels de façon uniforme. Voir aussi CAM05 Méthodes de gestion des changements organisationnels, qui inclut la pratique de gouvernance CAM05.01 sur la façon de provoquer le désir de changement, qui stipule qu'il est nécessaire de comprendre la portée et l'incidence de changements projetés et de l'intérêt/du désir de changement des divers intervenants. Déterminer les mesures à prendre pour inciter les divers intervenants à accepter et à souhaiter une mise en œuvre efficace du changement.

Sans cadre de gestion de projet officiel et de surveillance adéquate par la haute direction, notamment de prise en compte des avantages apportés par les projets, ils risquent de ne pas respecter les objectifs, les échéances et les budgets établis. L'absence d'un programme complet de gestion du changement, notamment le manque de participation des secteurs opérationnels et la possibilité pour les utilisateurs de continuer à utiliser l'ancien système, peut avoir freiné l'adoption d'Officium. Le sondage mené récemment auprès des utilisateurs d'Officium indique que 49 % d'entre eux utilise le système « tout le temps ou souvent » et que les deux tiers d'entre eux réclament davantage de formation. Il faut signaler qu'en raison de l'intégration entre Officium et Ci2 les utilisateurs peuvent accéder aux fonctions d'Officium. Par exemple, les dossiers sauvegardés dans le système de suivi de gestion des cas Ci2 sont entrés dans Officium sans que les utilisateurs sachent qu'ils l'utilisent.

Recommandations

4. Nous recommandons que le directeur de la GI-TI mette en place un cadre de gestion de projet élaboré établissant des paliers au cours desquels l'approbation de la haute gestion du Commissariat est nécessaire ainsi que prévoyant une méthode qui permette d'évaluer la réalisation des avantages et d'organiser des activités de gestion du changement dans la planification intégrée de projet. Cette méthode inclut un suivi effectué par les secteurs opérationnels après la mise en œuvre des projets pour déterminer s'ils ont produit les avantages attendus.

Réponse de la direction et plan d'action	Responsabilités et échéancier
Nous acceptons la recommandation et adopterons les mesures suivantes : 1. Nous élaborerons un cadre de gestion de projet élaboré qui s'appliquera aux projets de grande envergure liés à la GI-TI. Le cadre de gestion tiendra compte de la petite taille du Commissariat. Il mettra également l'accent sur la nécessité d'obtenir l'approbation du CD et sur l'importance d'inclure l'évaluation des avantages réalisés et des activités de gestion du changement dans la planification intégrée du projet. Pour élaborer le cadre de gestion, l'équipe de la GI-TI utilisera les outils existants comme la stratégie de gestion de changement du Commissariat et les outils de planification de projet. Ils consulteront aussi le CSC. 2. Présenter pour approbation le cadre de gestion au CD.	Directeur de la GI-TI (Mars 2016)

5. Nous recommandons que le directeur de la GI-TI continue de travailler de concert avec les directions pour s'assurer qu'un plan complet de gestion du changement axé sur la personne soit mis en place, mais aussi, qu'il bénéficie de l'appui et du suivi nécessaire, et ce, pour permettre la mise en œuvre d'Officium.

Réponse de la direction et plan d'action	Responsabilités et échéancier
Nous sommes d'accord avec la recommandation. Étant donné qu'Officium est maintenant pleinement fonctionnel et que la migration de tous les documents actifs est terminée, il n'est plus nécessaire d'élaborer un plan officiel de gestion du changement. Cependant, nous reconnaissons qu'il est toujours nécessaire de prendre des mesures particulières additionnelles pour assurer la réussite totale du nouveau système. L'équipe de la GI-TI soutiendra et poursuivra la formation et la mise en œuvre du plan d'action tout en examinant les diverses possibilités d'amélioration de l'utilisation et de la compréhension de la nouvelle application. 1. Nous évaluerons le succès de la migration vers Officium en étudiant son utilisation par les employés. 2. Nous élaborons de nouvelles méthodes pour inciter les employés qui ne se servent pas souvent d'Officium à l'utiliser davantage.	Directeur de la GI-TI (Juin 2015)

Appendice A – Personnes interrogées

Les personnes suivantes ont été interrogées dans le cadre du processus interne de vérification :

- Commissaire à la protection de la vie privée du Canada
- Directeur général, Gestion intégrée
- Directrice générale des enquêtes, Loi sur la protection des renseignements personnels
- Directeur général, LPRPDE
- Directeur général, Vérification et revue
- Directrice générale, Communications
- Avocate générale principale et directrice générale
- Directeur, Direction de l'analyse des technologies
- Directrice, Politiques et recherche
- Directrice, Services juridiques et Avocate principale
- Directrice, AIPRP et Chef de la protection des renseignements personnels
- Directeur, Équipe de la GI-TI
- Directrice, Services financiers et administratifs
- Directrice, Gestion des ressources humaines
- Gestionnaire, Programmes et services de gestion de l'information
- Gestionnaire, Direction des enquêtes liées à la LPRP
- Gestionnaire, Services d'analyse, Gestion et soutien des programmes
- Gestionnaire, Planification financière, Établissement des budgets, des rapports et des coûts
- Gestionnaire, Opérations comptables, politiques et systèmes
- Analyste des logiciels malveillants, Direction de la Gestion intégrée
- Enquêteure principale à la protection de la vie privée, bureau de Toronto
- Analyste technique, Programmes et services de gestion de l'information
- Greffier des plaintes, Direction des enquêtes liées à la LPRP

Appendice B – Critères de vérification

Les critères de vérification suivants ont été utilisés pour la présente vérification :

Critères de vérification	Renvoi aux CGF
1. Gouvernance et surveillance	
1.1 Des organismes de surveillance efficaces ont été mis en place pour la GI-TI.	G-1, G-2
1.2 Les rôles et responsabilités relatifs à la gouvernance, à la planification et aux projets liés à la GI-TI ont été clairement définis et communiqués.	AC-1
1.3 Des processus ont été mis en œuvre pour cerner et approuver les changements en matière de fonctionnement et de maintenance des applications d'IT ainsi qu'établir des priorités entre ces changements.	G-4, PR-1
2. Direction et planification en matière de GI-TI	
2.1 La haute direction de l'ensemble du Commissariat et la planification stratégique et opérationnelle orientent la planification et les décisions d'investissement en matière de GI-TI.	G-4, PR-1
2. Des plans d'urgence ont été élaborés pour s'assurer que les problèmes liés à la capacité de GI-TI peuvent être résolus de rapidement et efficacement.	PPL-1, PPL-2
3. Gestion de projets liés à la GI-TI	
3.1 Des processus et des méthodes de contrôle de la gestion de projets sont mis en œuvre pour s'assurer qu'ils atteignent leurs objectifs, mais aussi respectent les délais et le budget impartis. Ces processus prévoient une documentation adéquate des avantages apportés par les projets ainsi qu'une méthode efficace pour vérifier qu'ils atteignent leurs objectifs.	CFS-4