# Audit des systèmes en voie de développement dans le cadre des projets du programme d'infrastructure

## Rapport annuel 2017-2018

Le 18 décembre 2018

Bureau de la vérification et de l'évaluation

Services partagés Canada
Shared Services Canada
Canada

# TABLE DES MATIÈRES

# SOMMAIRE EXÉCUTIF

## Qu'avons-nous examiné?

Dans le cadre de ses efforts visant à moderniser la façon dont le gouvernement fédéral gère son infrastructure de technologie de l'information, Services partagés Canada (SPC) a entrepris une transformation exhaustive des activités à l'échelle du gouvernement du Canada s'articulant autour de six principaux programmes d'infrastructure. Étant donné la complexité et l'ampleur de ces programmes d'infrastructure par rapport à des programmes typiques, le Comité ministériel de vérification de SPC a recommandé qu'ils fassent l'objet d'une série d'audits des systèmes en voie de développement (SVD).

Pour aider SPC à gérer cette transformation complexe, le Bureau de la vérification et de l'évaluation a mené, en 2016-2017, puis en 2017-2018, des programmes d'audits trimestriels des SVD relatifs aux programmes d'infrastructure de technologie de l'information (TI) de SPC.

Le présent rapport dresse un résumé de trois des quatre audits des SVD de 2017-2018, lesquelles ont porté sur les sujets suivants :

- Gestion de projets – Activités par rapport aux projets
- Regroupement des centres de données – Fermeture de centres de données
- Cybersécurité et sécurité de la TI – Exigences de sécurité de la TI relatives à l'approvisionnement

Le quatrième audit des SVD de 2017-2018 concerne le Guide d'exploitation pour la gestion de projets et sera publiée sous forme de rapport distinct.

## Pourquoi est-ce important?

La réussite du Plan d'infrastructure de SPC à l'échelle du gouvernement du Canada est liée en grande partie à la réussite des six programmes d'infrastructure de TI qui font l'objet des audits des SVD. Ces audits aident la direction à établir si les programmes d'infrastructure sont sur la bonne voie et servent de système de détection précoce permettant de cerner les problèmes en temps opportun, contribuant ainsi au bon déroulement des programmes.

## Qu'avons-nous constaté?

Pour chacun des sujets examinés, les constatations de l'audit se sont concentrées sur les domaines présentant les risques les plus élevés.

**Gestion de projets – Activités par rapport aux projets :** Pour la mise en œuvre de son Plan d'infrastructure, SPC assure la gestion d'un portefeuille d'activités et de projets. Les activités consistent en des tâches dont la gestion peut s'accomplir sans avoir recours à un processus de supervision rigoureux. Les projets, qui sont plus complexes et nécessitent une gouvernance plus

stricte, produisent des résultats déterminés et précis, généralement à l'appui des objectifs d'une politique gouvernementale.

SPC avait établi des processus et des contrôles permettant de transformer une activité en projet (et vice versa), et les répercussions de tels changements étaient bien comprises. Des disparités ont toutefois été constatées dans la manière de définir, de consigner et de surveiller les activités. En outre, les critères de classification permettant de différencier entre les activités et les projets n'avaient pas été consignés par écrit ou appliqués de manière uniforme. Cela a donné lieu à certains cas où des projets étaient gérés comme des activités, et vice versa.

Toute activité gérée comme s'il s'agissait d'un projet risque d'être inutilement entravée par une supervision et des exigences en matière de rapports trop strictes; alors qu'un projet géré comme s'il s'agissait d'une activité pourrait ne pas se voir accorder le financement, les ressources et la supervision nécessaires. Dans les deux cas, ces situations risquent de se traduire par un manque d'efficacité.

En réponse à ces constatations, la direction de SPC a fourni et communiqué une définition officielle des projets et des activités au moyen du Cadre de gouvernance des projets. Elle a révisé le Guide d'exploitation et le processus de gouvernance de la gestion de projet pour veiller à ce que les décisions soient prises et que le suivi soit fait. Elle fera maintenant rapport régulièrement à un comité de gouvernance interne de haut niveau sur la liste principale des projets.

**Regroupement des centres de données – Fermeture de centres de données :** Cette grande initiative d'infrastructure vise la fermeture de centres de données existants et le transfert de services aux nouveaux centres de données d'entreprise pour fournir un meilleur service aux partenaires et économiser de l'argent. Pour assurer l'exécution efficace de l'initiative, les regroupements de centres de données doivent être classés par ordre de priorité, et les économies de coûts qui en découlent doivent faire l'objet d'un suivi et être rapportées à la haute direction.

Malgré les quelques mesures qui avaient été prises pour classer les centres de données par ordre de priorité et procéder à leur regroupement, il demeurait, de toute évidence, certaines difficultés touchant la consignation incomplète, les outils de gestion des données inefficaces et les rapports présenter à la direction de SPC. La liste des regroupements de centres de données prévues n'était pas suivie de façon uniforme, et la justification des changements n'était pas toujours consignée et communiquée par écrit au sein de SPC ou à l'intention des partenaires. Toute modification de la liste des regroupements prévus pourrait avoir des répercussions sur les priorités et objectifs stratégiques des partenaires et de SPC.

La direction s'est engagée à corriger les lacunes, et les plans d'action de la direction comprennent notamment la mise au point de la liste des regroupements de centres de données prévues en 2017-2018, la tenue de réunions continues entre SPC et les principaux partenaires. Le tout afin garantir que les centres de données visés par un regroupement sont bien identifiés, l'élaboration d'une stratégie de communication pour mobiliser les partenaires au sujet des plans de regroupement de centres de données et un meilleur suivi des coûts et des avantages liés au regroupement de centres de données et la présentation de rapports connexes à la haute direction.

**Cybersécurité et sécurité de la TI – Exigences de sécurité de la TI relatives à l'approvisionnement :** SPC doit vérifier si les processus servant à définir, à évaluer et à approuver les exigences en matière de sécurité de la TI ont été mis en place et sont appliqués efficacement pour les processus d'approvisionnement liés aux projets d'infrastructure. L'audit a permis de constater que SPC n'engageait pas toujours un dialogue avec les fournisseurs pour s'assurer que les discussions sur la sécurité avaient lieu et n'avait pas mis au point les documents clés nécessaires pour établir les exigences de sécurité. Les consultations avec les propriétaires d'entreprise au sujet des exigences de sécurité n'avaient pas toujours lieu, et les rôles et responsabilités relatifs à l'approbation de ces exigences n'avaient pas été établis. Pour cette raison, les exigences de sécurité de certains grands projets de SPC n'avaient pas été bien définies ou n'étaient pas harmonisées avec les capacités de l'industrie.

La direction compte donner suite aux recommandations en élaborant davantage le Guide d'exploitation pour la gestion et la réalisation de projets et le Cadre de gouvernance des projets. Ces outils comprennent : les renvois et les liens vers les documents requis en matière de cybersécurité et de sécurité de la TI et la définition des rôles et des responsabilités pour l'élaboration et l'approbation des exigences de sécurité.

## Prochaines étapes

La direction de SPC est en accord avec les constatations des trois missions d'audit effectuées et a présenté des mesures et des plans d'action pour apporter les améliorations qui s'imposent. Au moment de la rédaction du présent sommaire, plus de la moitié des recommandations avaient été mises en œuvre et clôturées. Pour plus d'information, voir l'annexe B.

Le Bureau de la vérification et de l'évaluation continuera à assurer un suivi de tous les points en suspens et fournira périodiquement des rapports au président et au Comité ministériel de vérification de SPC.

Begonia Lojk

Dirigeante principale de la vérification et de l'évaluation, par intérim

# A. INTRODUCTION

## 1. Contexte et justification de l'audit

### 1.1 Contexte

Services partagés Canada (SPC) a été créé dans le but de moderniser la façon dont le gouvernement fédéral assure la gestion de son infrastructure de technologie de l'information (TI) afin de mieux soutenir la prestation de programmes et de services à la population canadienne. SPC fournit des services obligatoires de courriel, de centres de données et de réseaux à des organisations partenaires, de manière regroupée et normalisée, afin d'appuyer l'exécution des programmes et la prestation des services du gouvernement fédéral. L'approche pangouvernementale permet à SPC de faire des économies d'échelle et d'offrir des services d'infrastructure de TI efficaces, fiables et sécurisés aux ministères fédéraux. SPC fournit aussi certains services technologiques facultatifs aux organismes gouvernementaux selon le principe du recouvrement des coûts.

En 2016, le Ministère a réalisé un examen exhaustif de ses plans pour moderniser et transformer les systèmes d'infrastructure de TI du gouvernement du Canada. Le Plan d'infrastructure de TI du gouvernement du Canada qui en a résulté décrit les grandes lignes de l'orientation stratégique de SPC, ses responsabilités et ses priorités en vue de transformer l'infrastructure de TI du gouvernement du Canada et d'améliorer la qualité de la prestation numérique des programmes et des services offerts aux Canadiens.

Le Plan d'infrastructure de TI de SPC à l'échelle du gouvernement fédéral s'appuie sur les six principaux programmes d'infrastructure de SPC qui composent le programme de modernisation :

- Regroupement des centres de données
- Initiative de transformation des services de courriels
- Appareils technologiques en milieu de travail
- Transformation de la cybersécurité et de la sécurité de la TI
- Programme de transformation des télécommunications
- Transformation de la gestion des services de TI

Ces six grands programmes d'infrastructure sont reconnus comme étant extrêmement complexes, très coûteux et essentiels à la modernisation du gouvernement du Canada. Ces programmes d'infrastructure englobent chacun de nombreux projets qui évoluent continuellement et rapidement et mettent particulièrement l'accent sur les économies annuelles et l'amélioration de l'efficacité à l'échelle du gouvernement du Canada.

Pour aider SPC à gérer cette transformation complexe de l'infrastructure de TI, le Bureau de la vérification et de l'évaluation a commencé, en 2016-2017, à mener des audits trimestriels des systèmes en voie de développement (SVD) relatifs aux programmes d'infrastructure de SPC. À ce jour, huit programmes d'audit des SVD ont été exécutés, et deux autres sont en cours. Les

quatre premièrs audit des SVD sont résumées dans le rapport annuel d'audit 2016-2017 des SVD et portent sur les sujets suivants :

- Planification de la transformation
- Établissement de rapports sur le rendement et gestion financière
- Projet de réseau étendu du gouvernement du Canada
- Migration des charges de travail

Le présent rapport dresse un résumé des trois premiers programmes d'audits des SVD exécutés en 2017-2018 :

- Gestion de projets – Activités par rapport aux projets
- Regroupement des centres de données – Fermeture de centres de données
- Cybersécurité et sécurité de la TI – Exigences de sécurité de la TI relatives à l'approvisionnement

En 2017-2018, il a été décidé que chaque programme d'audit des SVD fera l'objet d'un rapport d'audit distinct. Ainsi, le rapport de SVD final 2017-2018, qui portera sur la gestion des projets, sera publié dans un rapport d'audit distinct.

## 1.2 Justification des audits

La réussite du Plan d'infrastructure de SPC à l'échelle du gouvernement du Canada repose sur la réussite des six programmes d'infrastructure de TI qui font l'objet des audits des SVD. Ainsi, ces audits des SVD aident la direction à établir si les programmes d'infrastructure sont sur la bonne voie et servent de système de détection précoce permettant de cerner les problèmes en temps opportun, contribuant ainsi au bon déroulement des programmes.

Pour 2017-2018, les sujets ont été sélectionnés en fonction du risque.

## 1.3 Autorité de l'audit

L'audit a été incluse au Plan d'audit axé sur les risques de 2017-2020, lequel a été approuvé par le président de Services partagés Canada selon la recommandation du Comité ministériel de vérification.

# 2. Objectif, portée et méthode

## 2.1 Objectif

Les objectifs globaux des audits des SVD consistent à fournir à la direction une évaluation des points suivants :

- les progrès et l'atteinte des objectifs de chaque programme selon les jalons définis dans le cadre du programme et le calendrier de transformation;

- les principaux contrôles internes, les processus de gouvernance et le cadre de gestion des risques liés à la transformation à un point du cycle d'élaboration où des améliorations peuvent être mises en œuvre et des processus peuvent être adaptés.

Chaque programme trimestriel d'audit des SVD est axé sur un volet en particulier ainsi qu'un ensemble distinct d'objectifs et de critères d'audit. Les objectifs des trois sujets couverts dans le présent rapport sont les suivants :

- **Gestion de projets – Activités par rapport aux projets :** Établir si les processus et les contrôles visant à changer les projets de transformation en activités (et vice versa) ont été établis et respectés et si l'incidence des changements a été comprise.
- **Regroupement des centres de données – Fermeture de centres de données :** Déterminer si les regroupements de centres de données ont été effectués en fonction des priorités et de manière efficace, et établir si les économies de coûts liées aux regroupements de centres de données ont fait l'objet d'un suivi et ont été relevées de façon précise.
- **Cybersécurité et sécurité de la TI – Exigences de sécurité de la TI relatives à l'approvisionnement :** Établir si les méthodes servant à définir, à évaluer et à approuver les exigences de sécurité de la TI ont été définies et mises en œuvre efficacement.

## 2.2 Portée

La portée se limitait aux processus et aux contrôles au sein des programmes d'infrastructure de TI de SPC : Initiative de transformation des services de courriels; Appareils technologiques en milieu de travail; Programme de transformation des télécommunications; Regroupement des centres de données; Cybersécurité et sécurité de la TI; Gestion des services de TI.

## 2.3 Méthode

L'approche d'audit des SVD intègre les caractéristiques clés suivantes :

- une approche descendante fondée sur les risques avec une perspective intégrée sur l'ensemble des programmes d'infrastructure qui tient compte des interdépendances des programmes;
- la planification continue, l'exécution, l'établissement de rapports et l'amélioration de la planification pour chaque cycle trimestriel afin d'appliquer une harmonisation continue entre l'attribution des ressources de l'audit des SVD et les risques et priorités pour SPC.

L'audit des SVD permet d'évaluer (sur les plans qualitatif et quantitatif) si les programmes sont sur la bonne voie, en cernant rapidement les principaux problèmes.

Au cours des étapes d'exécution des audits, nous avons :

- interrogé les cadres supérieurs, les gestionnaires et le personnel de SPC;

- examiné tous les documents, p. ex. audits antérieures, guides gouvernementaux et politiques sur la gestion de projet ainsi que documents relatifs au processus de gestion de projet de SPC;
- fait l'analyse des données.

Les quatre premier audit des SVD ont été effectuées de façon cyclique et rassemblées dans un rapport annuel. Les cinquième, sixième et septième audits des SVD de 2017-2018 sont résumés dans le présent rapport annuel. Les audits prochains des SVD seront présentés individuellement dans des rapports distincts à mesure qu'ils seront terminés.

## 2.4 Énoncé de conformité

L'audit est conforme aux Normes internationales pour la pratique professionnelle de l'audit interne, comme l'ont démontré les résultats du programme d'amélioration et d'assurance de la qualité. Une inspection des pratiques professionnelles a été effectuée.

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 étaient basés sur une comparaison des conditions qui existaient au moment de l'audit selon des critères établis convenus avec la direction. Les constatations et les conclusions s'appliquent seulement à l'entité examinée ainsi qu'à l'étendue et la période visées par l'audit.

# B. RÉSUMÉ DES CONSTATATIONS

## 1. Gestion de projets – Activités par rapport aux projets

### 1.1 Contexte

Une gestion de projet saine et efficace est essentielle pour appuyer les programmes d'infrastructure de SPC. En 2017, la Direction générale de la gestion et de l'exécution des projets a été créée pour fournir des processus centralisés de gestion de projets, une gouvernance saine et une supervision efficace de la gestion de projets. Il était important d'examiner précocement l'efficacité avec laquelle les nouveaux processus de gestion de projets ont été mis en place pour fournir une rétroaction à la direction de SPC.

Pour assurer une gestion saine des projets, il est fondamental de faire la distinction entre les activités et les projets. Il est essentiel de s'assurer que les deux sont gérés correctement afin de garantir une gouvernance adéquate et des pratiques de gestion efficaces.

De manière générale, les activités sont des séries de tâches ne nécessitant pas de processus de gouvernance rigide. À l'inverse, les projets doivent produire des résultats déterminés et précis à l'appui d'un objectif en matière de politique publique; ils nécessitent toutefois un calendrier précis, un plan de ressources et un processus de gouvernance. Les activités gérées par erreur comme des projets peuvent faire l'objet d'une gouvernance et d'exigences d'établissement de rapports inutiles. Les projets qui sont gérés par erreur à la façon d'activités peuvent ne pas bénéficier du financement, des ressources et d'un encadrement appropriés. Dans les deux cas, ces situations risquent de se traduire par un manque d'efficacité.

### 1.2 À propos du programme d'audit

Cet audit s'est concentré sur les processus et les contrôles liés aux processus de changement, visant les activités et les projets de transformation. Ceux-ci sont importants, car tous insuffisance dans ces processus et contrôles pourrait nuire à la réception par les projets du financement, des ressources et de la supervision adéquats et, par conséquent, avoir des répercussions sur leur efficacité globale.

L'objectif était de déterminer si les processus et les contrôles visant à changer les activités en projets (et vice versa) sont établis et respectés, et à comprendre les répercussions de ces changements. L'audit englobait les projets d'infrastructure de la TI dans lesquels les activités avaient été changées en projets (et vice versa) entre le 1er janvier et le 31 décembre 2016. La phase d'examen s'est déroulée du 8 janvier au 16 mars 2017.

### 1.3 Constatations

Des incohérences ont été relevés dans les seuils appliqués pour différencier entre les activités et les projets; ils n'avaient pas été consignés ou appliqués de manière uniforme au moment de l'audit. Bien que SPC ait adopté la définition du Conseil du Trésor du Canada pour le terme

« projet », celle-ci n'avait pas été appliquée en tenant compte de la nature transformationnelle et opérationnelle unique du Ministère. Le manque de cohérence a entraîné des divergences au niveau de l'interprétation et de l'application d'une direction générale à l'autre. En réponse à cette constatation, la direction de SPC a fourni et communiqué une définition officielle des projets et des activités au moyen du Cadre de gouvernance des projets.

L'audit a permis de constater que les systèmes de SPC assurent un suivi adéquat des projets et des services, mais ne suivent pas les activités dans la même mesure. Par exemple, il n'existait aucun processus pour classer les activités avec précision ou pour repérer et corriger les erreurs dans le classement des activités. Il n'existait par ailleurs aucun répertoire des activités à l'appui du Plan d'infrastructure de TI du gouvernement du Canada et aucun processus systématique pour suivre et surveiller ces activités. En l'absence de ces processus, il y a un risque que les activités fassent l'objet de rapports erronés et qu'on omette des interdépendances entre des projets et des activités. La direction de SPC est d'accord avec cette constatation et a révisé le Guide d'exploitation pour la gestion de projets et le processus de gouvernance pour s'assurer que des décisions sont prises et qu'un suivi est effectué.

Les projets d'infrastructure de TI inscrits dans le système de gestion des dossiers de projets ne correspondaient à ceux inscrits dans le Plan d'infrastructure de TI du gouvernement du Canada. SPC ne pourra pas établir de rapports précis sur l'avancement relativement au Plan si les projets ne sont pas désignés et suivis de manière uniforme. Désormais, la direction de SPC présentera des rapports périodiques sur la liste de projets principale à un comité de gouvernance interne de niveau supérieur.

# 2. Regroupement des centres de données – Fermeture de centres de données

## 2.1 Contexte

SPC gère plus de 500 anciens centres de données existants qui appuient les fonctions opérationnelles essentielles et non essentielles à la mission pour les 43 ministères et organismes liés au mandat de SPC. La façon la plus économique de régler le problème de la « désuétude » du gouvernement consiste à regrouper ces centres de données en un nombre réduit de services de centres de données modernes et sécurisés. Le regroupement des centres de données est un élément clé du plan d'infrastructure de SPC qui aboutit à la fermeture et à la mise hors service des anciens centres de données existants.

Il est important que SPC dispose d'un plan clair établi selon un ordre de priorités qui lui permettra de respecter ses engagements de regroupement des centres de données. Il est également nécessaire d'avoir des renseignements précis sur les coûts afin de comprendre les avantages financiers qui s'accumuleront grâce aux fermetures en temps opportun et à la mise hors service des centres de données existants.

## 2.2 À propos du programme d'audit

Cet audit s'est concentré sur la gestion et la supervision du processus de fermeture des centres de données. Des processus de gouvernance solides garantiraient que le Ministère soit capable de respecter précisément ses engagements de regroupement de centres de données et de suivre les coûts du programme.

Ce sujet est important parce que les changements apportés aux priorités de fermeture des centres de données peuvent avoir une incidence sur la capacité de SPC d'atteindre les objectifs de regroupement prévus et sur les plans d'activités et les engagements de financement des partenaires. Un suivi précis des coûts et des avantages aidera SPC à établir des rapports sur les avantages cumulatifs liés au regroupement de centres de données.

L'audit visait à établir si les fermetures de centres de données ont été effectuées en fonction d'un ordre de priorité et exécutées de façon efficace, et à établir si les économies de coûts liées aux fermetures de centres de données font l'objet d'un suivi et de rapports précis. Elle englobait les processus et contrôles portant sur les fermetures de centres de données ainsi que les économies de coûts au sein de SPC. La phase d'examen de cet audit a démarré le 20 avril pour se terminer le 9 juin 2017.

## 2.3 Constatations

L'audit a permis de découvrir que, bien que certaines activités aient eu lieu pour établir des priorités dans la fermeture de centres de données, en raison des problèmes liés aux documents incomplets et aux outils de gestion des données inefficaces, il n'a pas été possible de suivre ou de regrouper les coûts de façon cohérente.

À titre d'exemple, au moment de l'audit, la liste prévue des centres de données de SPC visés pour fermeture n'était ni exacte ni à jour. La direction était au courant et avait déjà entrepris des travaux pour examiner la liste. SPC mettra également en œuvre un processus pour en assurer l'exhaustivité de la liste.

Dans l'échantillon examiné, les documents conservés sur les divers centres de données, inscrits dans l'outil de suivi de SPC ne contenaient pas tous les renseignements obligatoires sur les centres de données et leurs coûts connexes. Par ailleurs, le processus servant à recueillir et à valider les renseignements reçus n'était pas suivi de façon cohérente. Une grande partie de l'information avait été remplie à la création de SPC, et la direction doit désormais mettre en place un processus pour la mettre à jour et en assurer l'exactitude.

En 2016-2017, les projets de fermeture de centres de données n'ont pas respecté le calendrier défini. Seul un tiers des fermetures prévues a été achevé, et quatre centres de données ne figurant pas dans le plan d'origine ont été fermés. La justification de ces changements n'était pas toujours consignée ou communiquée au sein de SPC ou aux partenaires. Même s'il existera forcément toujours des divergences par rapport au plan, en raison de catastrophes naturelles et de défaillances de l'infrastructure, il demeure important de classer les fermetures de centres de données par ordre de priorité dans un plan approuvé, puis de communiquer clairement ce plan aux partenaires et parties intéressées. SPC élabore actuellement une stratégie et un plan d'établissement des priorités.

Les coûts et les avantages découlant des fermetures de centres de données n'ont pas fait l'objet d'un suivi et d'un rapprochement exact par rapport aux systèmes financiers. Par conséquent, il est impossible d'analyser les coûts et les économies et d'établir des rapports précis à leur sujet. Par ailleurs, la planification et l'établissement de priorités seront difficiles. La direction a accepté d'améliorer son système de suivi des coûts.

# 3. Cybersécurité et sécurité de la TI – Exigences de sécurité de la TI relatives à l'approvisionnement

## 3.1 Contexte

Les processus d'approvisionnement représentent un vecteur clé pour bon nombre de projets d'infrastructure de SPC. Il est important que les processus d'approvisionnement de SPC comprennent des exigences en matière de sécurité de la TI. Cela permettra ultimement l'application de pratiques de sécurité de la TI efficaces dans les projets d'infrastructure de SPC.

Pour garantir la réussite des processus d'approvisionnement, il est nécessaire de collaborer avec les parties intéressées comme les fournisseurs pour garantir leur respect des normes industrielles et la faisabilité globale de la demande d'approvisionnement. Une consultation limitée auprès des partenaires et parties intéressées pourrait conduire SPC à fournir des profils de sécurité trop normatifs et à ajouter des coûts et des retards inutiles aux projets; de plus les profils pourraient ne pas respecter les capacités de l'industrie.

Au début d'un processus d'approvisionnement, les exigences en matière de sécurité doivent être clairement consignées dans la demande de propositions, puis correctement approuvées. Il est important d'obtenir des avis pertinents pour garantir que les exigences en matière de sécurité répondent aux besoins opérationnels des secteurs de service.

## 3.2 À propos du programme d'audit

Cet audit s'est concentré sur l'évaluation des contrôles dans les processus d'exigences en matière de sécurité de la TI de SPC et sur leur mise en œuvre dans les mécanismes d'approvisionnement. En cas de problème constaté sur ces contrôles ou leur mise en œuvre, les projets de TI de SPC pourraient ne pas respecter les normes de l'industrie ou les exigences en matière de sécurité. Sans approbation adéquate de la part de l'autorité responsable, il y a un risque que des exigences incorrectes en matière de sécurité nuisent au projet dans son ensemble et à la sécurité de l'infrastructure.

L'objectif consistait donc à vérifier que les processus servant à définir, à évaluer et à approuver les exigences en matière de sécurité de la TI dans l'approvisionnement ont été mis en place et sont appliqués efficacement. L'audit portait sur les processus et contrôles pertinents, relatifs à la définition, à l'évaluation et à l'approbation des exigences de sécurité pour l'approvisionnement prévues des projets. Un échantillon de trois projets d'infrastructure majeurs a été sélectionné pour voir si les processus adéquats ont été respectés en ce qui concerne la définition, l'évaluation et l'approbation des exigences de sécurité incluses dans la demande de propositions. La phase d'examen s'est déroulée du 4 juillet au 15 septembre 2017.

## 3.3 Constatations

L'audit a permis d'examiner la mesure dans laquelle les fournisseurs ont été mobilisés en ce qui a trait à la faisabilité des exigences de sécurité définies, pendant la phase d'examen et

d'amélioration des exigences des trois grands approvisionnements. Dans un cas, les fournisseurs n'ont pas du tout été mobilisés, et l'approvisionnement a fini par échouer. Dans les deux autres cas, dans lesquels les fournisseurs ont été mobilisés, SPC n'a pas entièrement répondu à toutes leurs questions. La direction de SPC a accepté de réviser le processus d'approvisionnement afin de garantir qu'une collaboration ait lieu, que les exceptions soient approuvées adéquatement et que toutes les questions des fournisseurs soient abordées correctement.

L'audit a permis de noter que les documents dont a besoin la Direction générale de la cybersécurité et de la sécurité de la TI pour établir les exigences de sécurité n'étaient pas définis de façon uniforme. Par ailleurs, les discussions importantes sur la sécurité n'avaient pas toujours lieu avec les secteurs de service. Par conséquent, les documents nécessaires n'étaient pas fournis de manière uniforme par les équipes de projet à l'appui des exigences de sécurité, ce qui augmentait le risque d'erreur et d'exigences de sécurité inappropriées. La direction de SPC élaborera et communiquera un processus visant à garantir que les renseignements sur la sécurité soient recueillis et qu'une consultation soit entreprise auprès des secteurs de service au titre du cadre de gouvernance des projets de SPC.

Pour terminer, l'audit a permis de découvrir que l'autorité chargée d'approuver les exigences de sécurité finales incluses dans les demandes de propositions n'était pas identifiée. Dans l'échantillon examiné, il n'existait aucune preuve d'approbation des exigences de sécurité par la Direction générale de la cybersécurité et de la sécurité de la TI. La direction définira et communiquera les rôles et les responsabilités pour cette approbation.

# C. CONCLUSION

Dans ce cycle annuel des audits des SVD, le Bureau de la vérification et de l'évaluation a mené quatre audits trimestriels. Trois d'entre elles sont résumées dans le présent rapport et ont porté sur les différences entre les activités et les projets d'infrastructure, les fermetures de centres de données, et les exigences de sécurité de la TI relatives à l'approvisionnement. Ces audits sont importants, car elles se sont intéressées aux processus opérationnels clés qui appuient le plan d'infrastructure de SPC.

Les résultats globaux des trois audits des SVD inclus dans le présent rapport démontrent que, tandis que SPC continue à suivre son plan d'infrastructure et à atteindre les objectifs de ses programmes, il existe des incohérences dans les conditions de mise en place et de respect des processus et structures de gouvernance. Alors que le Ministère continuera d'avancer pour respecter le premier objectif de l'audit (c.-à-d. atteindre les objectifs du projet), des travaux supplémentaires seront nécessaires pour réussir à atteindre le second objectif de l'audit (amélioration et adaptation des contrôles internes principaux, des processus de gouvernance et du cadre de gestion du risque que représente la transformation).

Depuis l'achèvement de ces audits, la direction a produit des plans d'action pour gérer les risques recensés (voir l'annexe B). Le Bureau de la vérification et de l'évaluation de SPC surveille la mise en œuvre de ces plans d'action. Au moment de la publication du présent rapport, plus de la moitié des plans d'action étaient achevés et SPC s'est engagé à mettre en œuvre les autres.

# ANNEXE A : CALENDRIER DU PROGRAMME DES AUDITS DES SVD

| Titre | Période d'exécution |
|---|---|
| SVD 1 : Planification de la transformation | Janvier à mars 2016 |
| SVD 2 : Établissement de rapports sur le rendement et la gestion financière | Avril à juin 2016 |
| SVD 3 : Programme de transformation des télécommunications : réseau étendu du gouvernement du Canada | Juillet à septembre 2016 |
| SVD 4 : Regroupement des centres de données : migration des charges de travail | Octobre à décembre 2016 |
| SVD 5 : Activités par rapport aux projets | Janvier à mars 2017 |
| SVD 6 : Fermetures de centres de données | Avril à juin 2017 |
| SVD 7 : Exigences relatives à la sécurité de la TI | Juillet à septembre 2017 |
| SVD 8 : Guide d'exploitation pour la gestion de projets | Octobre à décembre 2017 |
| SVD 9 : Informatique de haute performance | Mars à avril 2018 |
| SVD 10 : Gestion des coûts liés aux projets | Juin à septembre 2018 |

# ANNEXE B : RECOMMANDATIONS ET RÉPONSES DE LA DIRECTION

Le tableau suivant présente les recommandations figurant dans chaque audit des systèmes en voie de développement, accompagnées de la réponse de la direction.

**L'état des plans d'action de la direction pour chaque recommandation, en septembre 2018, est indiqué ci-après.**

## SVD 5 : Activités par rapport aux projets

**Recommandations**

5.1 Nous recommandons que le sous-ministre adjoint principal, Gestion et exécution des projets, établisse, approuve et communique des seuils définis pour les services à l'appui de la classification précise des projets et des activités. **Terminée**

5.2 Nous recommandons que le sous-ministre adjoint principal, Gestion et exécution des projets, mette à jour et clarifie le processus de changement des activités de transformation en projets de transformation (ou vice versa), au besoin. **Terminée**

5.3 Nous recommandons que le sous-ministre adjoint principal, Gestion et exécution des projets, [Retiré par AIPRP] et s'assure que la liste est mise à jour et utilisée de façon uniforme au sein de SPC. **Terminée**

**Réponse de la direction concernant SVD 5 : Activités par rapport aux projets**

La direction est d'accord avec ces recommandations et a élaboré des plans d'action afin d'atténuer les risques ciblés dans le cadre de l'audit. Dans ces plans d'action, la direction s'est engagée à définir officiellement et à communiquer des niveaux de service clairement définis, qui appuient la classification complète des projets et activités. À cette fin, la direction mettra clairement à jour les processus visant à changer les activités de transformation en projets de transformation (et vice versa). Par ailleurs, elle désignera clairement [Retiré par AIPRP] la tiendra à jour et s'assurera de son efficacité à titre d'outil régulièrement utilisé.

**Mise à jour de décembre 2018 sur SVD 5 : Activités par rapport aux projets**

La Direction générale de la gestion et de l'exécution des projets a élaboré et publié le Guide d'exploitation pour la gestion et la réalisation de projets qui :

- fournit un outil de référence pour les processus propres à SPC, suivant les pratiques exemplaires de l'industrie, conformément au *Guide du référentiel des connaissances en gestion de projet* (Guide PMBoK) du Project Management Institute et à la Politique sur la gestion des projets du Conseil du Trésor;
- fournit une ligne directrice pour établir si une initiative est soit un projet, soit une activité opérationnelle;
- renforce et définit mieux la relation entre le processus de planification de la transformation et le processus de gouvernance du projet.

Une liste de projets a été approuvée dans le cadre de la gouvernance de SPC et est tenue, mise à jour et utilisée sur une base régulière.

## SVD 6 : Fermetures de centres de données

**Recommandations**

6.1.1 Nous recommandons que le sous-ministre adjoint, Services de centres de données :

- élabore et consigne un processus qui établit précisément les priorités relatives aux centres de données comme suit : priorité élevée, moyenne ou faible (justifier les fermetures d'urgence) et qu'il mette à jour les plans approuvés ainsi que la liste des fermetures basées sur les priorités de gestion, le financement et la capacité;
- établisse et communique un processus d'approbation des écarts/exceptions des priorités de centre de données, y compris la documentation des répercussions (sur la portée, les délais, le budget et la monétisation).
- **En cours**

6.1.2 Nous recommandons que le sous-ministre adjoint, Services de centres de données :

- effectue un rapprochement de toutes les listes de centres de données afin de s'assurer que la liste finale est complète et exacte pour la planification et l'établissement des priorités;
- procède à des exercices de validation périodiques afin de s'assurer que la liste officielle des fermetures de centres de données est tenue à jour.
- **En cours**

6.1.3 Nous recommandons que le sous-ministre adjoint, Services de centres de données :

- établisse quels sont les renseignements essentiels qui servent à définir les priorités et à concrétiser les avantages de la fermeture des centres de données1 dans l'outil d'application de fermeture de centres de données (y compris les documents obligatoires pour les processus de fermeture de centres de données au complet, du début à l'aboutissement);
- communique les exigences relatives aux outils de collecte de données et indique clairement les champs de saisie de données obligatoires pour recueillir les renseignements essentiels et assurer l'exhaustivité;
- consigne la preuve des visites des sites, les approbations et la validation des données recueillies afin d'assurer l'exactitude des renseignements.
- **En cours**

6.2.1a Nous recommandons que le sous-ministre adjoint, Services de centres de données :

- consigne un plan de fermeture de centre de données en collaboration avec les partenaires, en incluant les rôles et les responsabilités, les délais, les besoins en ressources et les approbations des partenaires concernés;
- rédige et obtienne les lettres d'entente auprès des partenaires afin de transférer les locaux ou la monétisation de sorte que les fermetures soient terminées au cours de l'exercice financier donné.
- **En cours**

6.2.1b Nous recommandons que le sous-ministre adjoint principal, Direction générale de la gestion et de l'exécution des projets, s'assure que les projets non financés et interrompus soient supprimés des rapports sur l'état d'avancement du projet concerné. **Terminée**

6.3.1a Nous recommandons que le sous-ministre adjoint, Services des centres de données, s'assure que les estimations des coûts de fermeture de centres de données contenues dans l'outil d'application de fermeture de centres de données soient corroborées par les documents à l'appui pertinents. **En cours**

6.3.1b Nous recommandons que le sous-ministre adjoint, Direction générale du dirigeant principal des finances :

- s'assure que les coûts de fermeture de chaque centre de données, et la monétisation reçue, puissent faire l'objet d'un suivi et être rapportés à la haute direction en temps opportun;
- collabore avec la Direction générale des services de centres de données pour rapprocher les coûts et les avantages de la fermeture des centres de données de l'outil de l'application de fermeture des centres de données à SIGMA[2].
- **En cours**

[1] Ces renseignements peuvent comprendre, entre autres, l'expiration de l'accord d'occupation, l'expiration du bail, la monétisation, le mesurage des locaux, les questions urgentes, etc.
[2] SIGMA est un système financier clé utilisé par SPC pour effectuer le suivi et la surveillance des coûts-avantages associés aux activités, aux projets et aux programmes.

**Réponse de la direction concernant SVD 6 : Fermetures de centres de données**

La direction est d'accord avec ces recommandations et a élaboré des plans d'action afin d'atténuer les risques ciblés dans le cadre de l'audit. Dans ces plans d'action, la direction s'est engagée à exploiter les outils et renseignements disponibles pour veiller à ce que la liste des centres de données soit exhaustive, exacte et soumise à une validation régulière afin de s'engager dans une activité de fermeture à jour et fondée sur des priorités, et qui est communiquée en conséquence. Par ailleurs, la direction s'est engagée à approfondir sa planification et sa collaboration avec les partenaires pour mieux coordonner les fermetures et l'activité financière.

**Mise à jour de décembre 2018 sur SVD 6 : Fermetures de centres de données**

La Direction générale des services de centres de données a donné suite aux constatations de l'audit au moyen de divers plans d'action de gestion élaborés en fonction de cinq recommandations pour lesquelles la Gestion des installations a dirigé le travail effectué au nom de la Direction générale. Les outils de suivi et d'établissement des priorités, les stratégies de communication et de mobilisation des parties prenantes, les besoins de financement et le suivi des dépenses, les outils de validation des processus et des données et d'autres activités ont été présentés dans un Manuel complet de stratégies de fermetures de centres de données. Les documents et les processus ont été discutés, rédigés et finalisés dans le cadre d'un atelier en deux parties qui a eu lieu les 28 juin 2018 et 10 octobre 2018. Le groupe de travail était composé de parties prenantes clés, y compris des ministères partenaires et d'autres directions générales de SPC concernées.

La première version du Manuel complet de stratégies de fermetures de centres de données a été achevée et est en cours de diffusion générale. On y trouve un certain nombre de processus visant à assurer l'amélioration de l'intégrité des données et des pratiques de communication appropriées. Les plans d'action de la direction de la Direction générale des services de centres de données ont été achevés et présentés dans le cadre des exercices de suivi du plan d'action de la direction du Comité ministériel de vérification menant à la réunion de février 2018 du Comité.

La Direction générale de la gestion et de l'exécution des projets veille à ce que la liste des projets en cours soit tenue à jour et à ce que les projets non financés et interrompus soient supprimés régulièrement des rapports sur l'état d'avancement du projet concerné.

La Direction générale du dirigeant principal des finances a établi un processus pour que les coûts de fermeture des centres de données puissent être suivis dans SIGMA par fermeture de site. Des codes relatifs aux ordres internes ont été créés afin de pouvoir suivre les coûts par fermeture. De plus, les avantages de la monétisation sont affichés dans l'affectation budgétaire initiale et dans les budgets supplémentaires des dépenses subséquents et peuvent être communiqués à la haute direction en temps opportun.

## SVD 7 : Exigences relatives à la sécurité de la TI dans les approvisionnements

**Recommandations**

7.1.1 Nous recommandons que le sous-ministre adjoint principal, Services ministériels, mette en œuvre des contrôles pour garantir que toutes les demandes de renseignements des fournisseurs sont abordées pendant le processus d'examen et d'amélioration des exigences. **Terminée**

7.1.2 Nous recommandons que le sous-ministre adjoint principal, Services ministériels, mette à jour la Directive sur la gouvernance des achats pour garantir que la décision d'omettre toute phase du processus d'approvisionnement collaboratif soit présentée au niveau le plus élevé de la gouvernance d'un approvisionnement donné, comme cela est défini dans la Directive sur la gouvernance des achats. **En cours**

7.2.1 Nous recommandons que le sous-ministre adjoint, Cybersécurité et sécurité de la TI, élabore et communique un processus nécessitant l'avis consigné des équipes de projet pour appuyer la création des exigences de sécurité (y compris les évaluations des facteurs relatifs à la vie privée) incluses dans la phase d'approvisionnement de demande de propositions. **Terminée**

7.2.2 Nous recommandons que le sous-ministre adjoint principal, Gestion et exécution des projets, inclue les documents requis (définis par Cybersécurité et sécurité de la TI) dans le Guide d'exploitation pour la gestion et la réalisation de projets ou dans le cadre de gouvernance des projets. **Terminée**

7.3.1 Nous recommandons que le sous-ministre adjoint, Cybersécurité et sécurité de la TI, en collaboration avec le sous-ministre adjoint principal, Gestion et exécution des projets, confirme et communique les rôles et les responsabilités dans l'élaboration et l'approbation des exigences finales en matière de sécurité, à inclure dans les demandes de propositions. **Terminée**

7.3.2 Nous recommandons que le sous-ministre adjoint principal, Gestion et exécution des projets, inclue les rôles et les responsabilités dans l'élaboration et l'approbation des exigences de sécurité pour les projets dans le Guide d'exploitation pour la gestion et la réalisation de projets. **Terminée**

**Réponse de la direction concernant SVD 7 : Exigences relatives à la sécurité de la TI dans les approvisionnements**

La direction est d'accord avec ces recommandations et a élaboré des plans d'action afin d'atténuer les risques ciblés dans le cadre de l'audit. Dans ces plans d'action, la direction s'est engagée à améliorer les relations que le Ministère entretient avec les fournisseurs, en améliorant les contrôles relatifs aux processus d'approvisionnement initial et en renforçant la fonction d'examen et d'approbation pour les projets plus complexes. En ce qui concerne les demandes de propositions, la direction s'est engagée à créer un processus solide d'exigence d'une cote de sécurité et à garantir que la documentation essentielle est fournie dans ses guides et cadres. Les rôles et les responsabilités propres à l'élaboration et à l'approbation des exigences de sécurité doivent être confirmés et définis clairement dans les demandes de propositions et les guides opérationnels.

**Mise à jour de décembre 2018 sur SVD 7 : Exigences relatives à la sécurité de la TI dans les approvisionnements**

Cybersécurité et sécurité de la TI a élaboré un modèle de plan d'évaluation de la sécurité pour consigner le processus par lequel tous les systèmes nouveaux ou mis à jour seront évalués pour les risques de sécurité avant leur mise en œuvre dans l'infrastructure de SPC. Le modèle de plan d'évaluation de la sécurité :

- exige des observations consignées par les équipes de projet;
- appuie la création d'exigences en matière de sécurité;
- définit les rôles et les responsabilités en matière d'exigences de sécurité;
- doit être rempli pour chaque projet ayant une incidence sur l'infrastructure de TI exploitée par SPC.

À ce jour, le modèle de plan d'évaluation de la sécurité est utilisé pour consigner le processus d'évaluation de la sécurité et les résultats de tous les projets de TI ayant une incidence sur l'infrastructure de SPC, et pour faire rapport sur celui-ci

La Direction générale de la gestion et de l'exécution des projets a mis à jour le Guide d'exploitation pour la gestion et la réalisation de projets au moyen d'un lien direct qui donne accès aux exigences relatives à la cybersécurité et à la sécurité de la TI, y compris les données nécessaires à l'élaboration des exigences du projet. Le Guide d'exploitation pour la gestion et la réalisation de projets mis à jour décrit également les rôles et les responsabilités en matière d'élaboration et d'approbation des exigences de sécurité pour les projets, en fonction des commentaires de Cybersécurité et sécurité de la TI.

Les Services ministériels ont entrepris un examen exhaustif de la gouvernance en matière d'approvisionnement afin de cerner les possibilités d'uniformiser la surveillance

et de clarifier les responsabilités. Un cadre révisé de gouvernance de l'approvisionnement sera approuvé d'ici le 20 juin 2019.

# ANNEXE C : SIGLES

| Acronyme | Signification du sigle |
|---|---|
| GC | Gouvernement du Canada |
| TI | Technologie de l'information |
| SPC | Services partagés Canada |
| SVD | Système en voie de développement |