Rapports de la vérificatrice générale du Canada au Parlement du Canada

Rapport 7

La cybersécurité des renseignements personnels dans le nuage

Rapport de l'auditeur indépendant | 2022

Bureau du vérificateur général du Canada

Office of the Auditor General of Canada

Rapport d'audit de performance

Le présent rapport fait état des résultats d'un audit de performance réalisé par le Bureau du vérificateur général du Canada en vertu de la *Loi sur le vérificateur général*.

Un audit de performance est une évaluation indépendante, objective et systématique de la façon dont le gouvernement gère ses activités et ses ressources et assume ses responsabilités. Les sujets des audits sont choisis en fonction de leur importance. Dans le cadre d'un audit de performance, le Bureau peut faire des observations sur le mode de mise en œuvre d'une politique, mais pas sur le bien-fondé de celle-ci.

Les audits de performance sont planifiés, réalisés et présentés conformément aux normes professionnelles d'audit et aux politiques du Bureau. Ils sont effectués par des auditeurs compétents qui :

- établissent les objectifs de l'audit et les critères d'évaluation de la performance;
- recueillent les éléments probants nécessaires pour évaluer la performance en fonction des critères;
- communiquent les constatations positives et négatives;
- tirent une conclusion en regard des objectifs de l'audit;
- formulent des recommandations en vue d'apporter des améliorations s'il y a des écarts importants entre les critères et la performance évaluée.

Les audits de performance favorisent une fonction publique soucieuse de l'éthique et efficace, et un gouvernement responsable qui rend des comptes au Parlement et à la population canadienne.

La publication est également diffusée sur notre site Web à l'adresse www.oag-bvg.gc.ca.

This publication is also available in English.

N° de catalogue FA1-27/2022-1-7F-PDF

ISBN 978-0-660-45994-3

ISSN 2561-3456

Photo de la page couverture : alice-photo/Shutterstock.com

Table des matières

Introduction

Information générale

La migration de l'information et des services du gouvernement vers le nuage

7.1 Le terme « nuage » désigne les serveurs informatiques auxquels les gens ont accès par Internet ainsi que les applications logicielles et les bases de données qui fonctionnent sur ces serveurs. Malgré ce que leur nom laisse entendre, les serveurs infonuagiques se trouvent dans des centres de données physiques partout dans le monde. Les organisations qui s'en servent, y compris le gouvernement du Canada, ne sont pas tenues de posséder et d'exploiter leurs propres serveurs physiques ou applications logicielles ou d'en assurer la maintenance. Elles peuvent se servir des serveurs infonuagiques sur demande et ne payent que ce dont elles ont besoin.

7.2 Le Secrétariat du Conseil du Trésor du Canada a publié la Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada en 2016 et l'a mise à jour en 2018. La Stratégie enjoint aux ministères (organisations fédérales) d'envisager l'infonuagique comme option privilégiée pour la prestation des services de technologies de l'information. Selon le Secrétariat, l'infonuagique offre les avantages suivants :

- des économies d'échelle;
- des services sur demande;
- de la souplesse;
- des services régis par des contrats;
- la sécurité.

7.3 Il est indiqué dans la Stratégie que les fournisseurs de services infonuagiques et les ministères fédéraux qui utilisent leurs services se partagent la responsabilité de la sécurité. Les ministères fédéraux demeurent responsables de la confidentialité, de l'intégrité et de la disponibilité des services informatiques ainsi que de l'information connexe hébergée par un fournisseur de services infonuagiques. Le Plan stratégique des opérations numériques de 2018 à 2022 du Secrétariat du

Conseil du Trésor du Canada reconnaît que pour réduire le plus possible les risques pour la sécurité, les ministères qui ont recours aux services infonuagiques doivent mettre sur pied une main-d'œuvre avisée en matière d'infonuagique.

7.4 Entre avril 2018 et mars 2022, Services partagés Canada a octroyé des contrats et Services publics et Approvisionnement Canada a attribué des **arrangements en matière d'approvisionnement**[1] à un total de 14 fournisseurs de services infonuagiques. Au cours de cette période, plusieurs ministères ont commencé à faire passer leurs applications logicielles et leurs bases de données au nuage. Certains ont aussi lancé des applications infonuagiques. D'avril 2018 à mars 2021, les organisations fédérales ont signalé avoir dépensé un total de 210 millions de dollars en services infonuagiques.

La sécurité de l'information stockée dans le nuage

7.5 Les cyberattaques peuvent entraîner l'interruption des services ainsi que la défaillance ou la destruction d'infrastructures essentielles, comme les services bancaires et le réseau de distribution d'énergie électrique. Elles peuvent aussi compromettre des données personnelles, porter atteinte à la réputation, occasionner des coûts financiers, perturber de manière importante les activités d'entreprises canadiennes et entraîner des difficultés financières pour la population. Les événements géopolitiques (tels que l'invasion de l'Ukraine) et les conflits commerciaux internationaux peuvent accroître de façon considérable les risques liés à la cybersécurité. Les médias ont signalé de nombreux exemples d'atteintes à la sécurité de systèmes infonuagiques.

7.6 Puisque les organisations fédérales ont commencé à faire passer des applications logicielles et des bases de données au nuage, les renseignements personnels de Canadiennes et de Canadiens s'y trouvent. Pour protéger les renseignements dans le nuage, le gouvernement a mis en œuvre un modèle de responsabilité partagée qui repose sur la collaboration d'un certain nombre de parties.

Rôles et responsabilités

7.7 **Secrétariat du Conseil du Trésor du Canada** — Le Secrétariat fournit des politiques et des orientations sur les services infonuagiques, notamment dans la Stratégie d'adoption de l'informatique en nuage du gouvernement. Il assure aussi la coordination des interventions à la suite d'incidents de cybersécurité, comme il est décrit dans le Plan de gestion des événements de cybersécurité du gouvernement du Canada.

1 **Arrangement en matière d'approvisionnement** — Méthode utilisée par Services publics et Approvisionnement Canada pour acquérir des biens et des services en qualifiant au préalable les fournisseurs et en établissant les clauses et les conditions essentielles qui s'appliqueront à tout contrat subséquent.

7.8 **Services partagés Canada** — À titre de fournisseur de services communs au gouvernement, le Ministère fournit aux autres ministères fédéraux l'accès aux fournisseurs de services infonuagiques approuvés dans le cadre de marchés qu'il gère. Il assure aussi la gestion et la surveillance de la plupart des serveurs et des centres de données du gouvernement du Canada et un accès sécurisé au nuage.

7.9 **Services publics et Approvisionnement Canada** — À titre de fournisseur de services communs au gouvernement, le Ministère établit des arrangements en matière d'approvisionnement avec des fournisseurs de services infonuagiques préqualifiés dans le but de permettre à d'autres ministères d'obtenir les services logiciels qu'ils offrent. Dans certains cas, les ministères peuvent se procurer ces services directement auprès de ces fournisseurs ou d'autres fournisseurs. Pour les contrats excédant certains seuils financiers, Services publics et Approvisionnement Canada établit le contrat et en assure la gestion au nom d'un ministère. Le Ministère évalue aussi les contrôles de sécurité matérielle des fournisseurs de services infonuagiques et de leur personnel.

7.10 **Centre de la sécurité des télécommunications du Canada** — Le Centre canadien pour la cybersécurité, qui fait partie du Centre de la sécurité des télécommunications du Canada, est la source de conseils, d'avis, de services et de soutien en matière de cybersécurité pour la population canadienne. Il doit notamment effectuer des évaluations de la sécurité des fournisseurs de services infonuagiques retenus par Services partagés Canada et Services publics et Approvisionnement Canada dans le cadre de certains de leurs processus d'approvisionnement en services infonuagiques. Il surveille aussi les réseaux ministériels et la sécurité dans le nuage et offre de la formation, des conseils et des orientations sur la sécurité infonuagique. Le Centre aide aussi les organisations fédérales à mettre en œuvre des infrastructures numériques sécurisées.

7.11 **Chacun des ministères** — Les ministères (organisations fédérales) mettent en œuvre leurs propres **contrôles de sécurité**[2] et assurent la surveillance des renseignements et des activités des utilisatrices et utilisateurs sur leurs propres applications logicielles. Ils demeurent en définitive responsables et comptables des risques relatifs à la sécurité découlant de leur utilisation des services infonuagiques. Les ministères sont tenus de signaler les atteintes à la protection de la vie privée au Secrétariat du Conseil du Trésor du Canada et au Commissariat à la vie privée du Canada.

2 **Contrôles de sécurité** — Tout type de contre-mesure de sauvegarde ou de protection qui vise à éviter, à détecter, à neutraliser ou à limiter les risques liés à la sécurité des biens matériels, de l'information, des systèmes informatiques ou d'autres actifs. Ces contre-mesures sont nommées « contrôles » dans le présent rapport.

Objet de l’audit

7.12 Cet audit visait à déterminer si le Secrétariat du Conseil du Trésor du Canada, Services partagés Canada, Services publics et Approvisionnement Canada, le Centre de la sécurité des télécommunications du Canada et les ministères fédéraux sélectionnés avaient mis en place une gouvernance, des lignes directrices et des outils adéquats et efficaces pour prévenir les événements de cybersécurité qui pourraient compromettre les renseignements personnels de la population canadienne stockés dans le nuage, détecter ces événements et agir en conséquence. Pour des raisons de sécurité nationale, le nom des ministères fédéraux sélectionnés aux fins de l’audit n’est pas mentionné dans le présent rapport.

7.13 Nous avons examiné des applications logicielles et des bases de données stockées dans le nuage auxquelles ont recours un certain nombre de ministères. Nous avons aussi cherché à déterminer si le gouvernement fédéral avait respecté ses engagements en matière d’environnement et de développement durable dans le cadre de ses processus d’approvisionnement de services infonuagiques. Nous n’avons pas examiné la sécurité de l’information stockée sur place dans les centres de données du gouvernement.

7.14 Cet audit est important parce que, de plus en plus, les ministères fédéraux font passer leurs applications logicielles et leurs bases de données au nuage. Certaines de ces applications et bases de données contiennent des renseignements personnels de Canadiennes et de Canadiens. Les ministères doivent conjuguer leurs efforts pour protéger ces renseignements contre de nombreux risques, y compris des cyberattaques.

7.15 La section intitulée **À propos de l’audit**, à la fin du présent rapport, donne des précisions sur l’objectif, l’étendue, la méthode et les critères de l’audit.

Constatations et recommandations

Message général

7.16 L’information stockée numériquement, soit sur place dans des centres de données ou dans le nuage, est exposée à des risques de compromission. Dans l’ensemble, nous avons constaté que les exigences mises en place par le gouvernement pour réduire les risques pour la sécurité liés au stockage d’information dans le nuage n’étaient pas toujours suivies par les ministères que nous avons audités. De plus, ces exigences, de même que les responsabilités et les rôles connexes, n’étaient pas toujours clairement définies, ce qui a donné lieu à une mise

en œuvre non uniforme et à des risques accrus. Ce point est important parce que le Secrétariat du Conseil du Trésor du Canada a demandé aux ministères d'envisager le déplacement de leurs applications et bases de données vers le nuage; de plus en plus de renseignements personnels de Canadiennes et de Canadiens y sont donc transférés. Parallèlement, les cyberattaques deviennent plus fréquentes et plus perfectionnées. Le risque de répercussions considérables sur le gouvernement et ses activités augmente.

7.17 Le gouvernement doit prendre des mesures immédiates pour renforcer sa manière de prévenir et de détecter les cyberattaques et d'intervenir en conséquence. Il devrait prendre ces mesures dès maintenant, pendant que les ministères en sont encore aux premières étapes du transfert des renseignements personnels vers le nuage. Ces mesures comprennent notamment le renforcement des principaux contrôles de sécurité pour prévenir et détecter les atteintes à la sécurité et intervenir en conséquence. Elles comprennent aussi la définition des responsabilités et des rôles communs clairs en matière de cybersécurité — qui sont très complexes dans un environnement infonuagique — de sorte que tous les ministères sachent exactement ce qu'ils doivent faire.

7.18 Nous avons aussi constaté que, quatre ans après avoir demandé aux ministères d'envisager la transition vers l'infonuagique, le Secrétariat du Conseil du Trésor du Canada n'avait toujours pas fourni de méthode de financement à long terme pour son adoption. Il n'avait pas non plus donné aux ministères les outils pour calculer le coût de la transition, de l'exploitation de l'infonuagique et de la sécurisation de l'information stockée dans le nuage. Les ministères ont besoin d'une méthode de financement et d'outils d'établissement des coûts pour s'assurer de disposer de la main-d'œuvre, de l'expertise, des compétences, de la formation, du financement et des autres ressources dont ils ont besoin pour sécuriser l'information stockée dans le nuage de manière à prévenir les menaces et les risques les plus importants et intervenir en conséquence. Une approche de financement et des outils d'établissement des coûts sont essentiels pour l'adoption de l'infonuagique et renforceraient les capacités de cyberdéfense du gouvernement du Canada, tant à l'échelle ministérielle que dans l'ensemble du gouvernement.

La protection des renseignements personnels dans le nuage

Il y avait des faiblesses dans les contrôles des ministères pour prévenir les cyberattaques, les détecter et intervenir en conséquence

Ce que nous avons constaté

7.19 Nous avons constaté qu'il y avait des lacunes dans l'utilisation par Services partagés Canada et Services publics et Approvisionnement Canada des contrôles de prévention des atteintes à la cybersécurité. Ces constatations portent sur des inspections de sécurité et sur certains aspects des mesures de sécurité d'informatique en nuage, un type de contrôle de sécurité. Nous ne pouvons pas publier ces constatations parce que le faire révélerait des vulnérabilités et poserait un risque à la sécurité nationale. Nous les avons plutôt signalées directement aux ministères concernés.

7.20 Nous avons aussi constaté des lacunes dans les contrôles visant à détecter les atteintes à la cybersécurité et à intervenir en conséquence. Par exemple, nous avons constaté que le Secrétariat du Conseil du Trésor du Canada avait effectué peu d'exercices de simulation en vue de tester et d'améliorer le Plan de gestion des événements de cybersécurité du gouvernement du Canada, qui décrit le processus à suivre pour réagir aux atteintes à la cybersécurité touchant plusieurs ministères. En outre, nous avons constaté que chaque ministère n'avait pas son propre plan ministériel de gestion des événements de cybersécurité en place et n'avait pas entièrement défini ses rôles et responsabilités en matière de gestion des incidents.

7.21 Enfin, nous avons constaté que les clauses de sécurité des contrats n'étaient pas claires ni uniformisées. Au cours de l'audit, Services partagés Canada et Services publics et Approvisionnement Canada ont amorcé des travaux pour remédier à ces enjeux.

7.22 L'analyse à l'appui de cette constatation porte sur :

- les lacunes dans les inspections de sécurité;
- les mesures de sécurité d'informatique en nuage non validées et non surveillées de manière uniforme pour tous les contrats;
- les clauses de sécurité des contrats imprécises et non uniformisées;
- les lacunes en ce qui concerne les plans de gestion des événements de cybersécurité et leur utilisation.

Importance de cette constatation

7.23 Cette constatation est importante parce que les atteintes à la cybersécurité sont à la hausse, et des contrôles robustes pour les prévenir, les détecter et intervenir en conséquence peuvent en réduire le risque et limiter la compromission des renseignements personnels des Canadiennes et des Canadiens, si de telles atteintes se produisaient.

Contexte

7.24 Chaque ministère est responsable de gérer ses propres risques de cybersécurité et de mettre en œuvre des contrôles de sécurité. Toutefois, les ministères s'appuient également sur plusieurs ministères centraux pour la mise en œuvre de certains contrôles de sécurité visant à prévenir les atteintes, à les détecter et à intervenir en conséquence. Par conséquent, il existe un niveau élevé de responsabilité partagée dans l'ensemble du gouvernement fédéral en ce qui concerne la gestion de la cybersécurité des renseignements personnels dans le nuage. Nous avons examiné ces responsabilités pour quatre catégories de contrôles de sécurité (voir la pièce 7.1). Une mesure de sécurité d'informatique en nuage (voir les pièces 7.1 et 7.2) est un type de contrôle de sécurité.

Analyse à l'appui de la constatation

Les lacunes dans les inspections de sécurité

7.25 Nous avons constaté qu'il y avait des lacunes dans la façon dont les inspections de sécurité visant les fournisseurs de services infonuagiques étaient réalisées. Nous ne pouvons pas publier nos constatations parce que le faire révélerait de l'information sur des vulnérabilités et poserait un risque à la sécurité nationale. Par conséquent, nous les avons signalées directement à Services publics et Approvisionnement Canada. Nos constatations sont accompagnées d'une recommandation à l'intention de Services publics et Approvisionnement Canada concernant la communication des résultats des inspections liées à la sécurité matérielle aux parties prenantes et les réinspections liées à la sécurité matérielle.

Pièce 7.1 — Divers ministères fédéraux se partagent les responsabilités liées aux principaux contrôles de sécurité infonuagique

Contrôle	Objectif	Rôles et responsabilités
Évaluations de la sécurité des fournisseurs de services infonuagiques	Déterminer si le personnel des fournisseurs, l'équipement matériel et les services fournis respectent les exigences de sécurité du gouvernement du Canada	• Services publics et Approvisionnement Canada a la responsabilité d'inspecter les installations physiques dans lesquelles les fournisseurs de services infonuagiques conservent les serveurs qui stockent les renseignements protégés. • Les ministères doivent vérifier et surveiller la conformité du fournisseur de services infonuagiques, d'après les résultats de l'inspection de Services publics et Approvisionnement Canada, avant de permettre à ces installations de traiter, de stocker ou de transmettre des données qui pourraient inclure des renseignements personnels de Canadiennes et de Canadiens. Ces évaluations et réévaluations doivent être réalisées en temps opportun et doivent être exhaustives parce que l'évolution de la technologie peut amener de nouveaux enjeux et de nouveaux risques que les ministères doivent comprendre, prendre en compte et atténuer.
Mesures de sécurité d'informatique en nuage	Protéger les données stockées dans le nuage ou transmises au moyen de réseaux dans le nuage	• Les ministères doivent mettre en œuvre ces mesures de sécurité conformément à la Directive sur les services et le numérique du Conseil du Trésor. • Services partagés Canada **valide**[3] la mise en œuvre des mesures de sécurité, de surveiller la conformité des ministères avec ces mesures sur une base mensuelle et de signaler les cas de non-conformité au Secrétariat du Conseil du Trésor du Canada.

3 **Valider** — Dans le contexte de la validation des mesures de sécurité, ce terme s'entend de l'examen des éléments probants confirmant que les ministères ont mis en œuvre les mesures de sécurité conformément à la Directive sur les services et le numérique du Conseil du Trésor.

Contrôle	Objectif	Rôles et responsabilités
		Si les mesures de sécurité ne sont pas mises en œuvre et exécutées de manière uniforme dans l'ensemble des ministères, il y a un risque accru que des pirates exploitent les vulnérabilités. Un suivi périodique permet aussi de maintenir un niveau de sécurité adéquat. Des faiblesses en matière de sécurité pourraient passer inaperçues et ne pas être contrôlées si le suivi n'est que partiellement réalisé.
Clauses de sécurité dans les contrats et les arrangements en matière d'approvisionnement des services infonuagiques	Définir les exigences de sécurité et les responsabilités avant qu'un ministère commence à recourir à des services infonuagiques	• Services partagés Canada octroie des contrats et Services publics et Approvisionnement Canada attribue des arrangements en matière d'approvisionnement à des fournisseurs de services infonuagiques. Ces contrats et arrangements définissent les exigences de sécurité pour la gestion des comptes, des incidents et des vulnérabilités et pour la surveillance des systèmes. L'absence de clauses de sécurité uniformisées dans les contrats et les arrangements en matière d'approvisionnement de services infonuagiques peut entraîner un manque de cohérence dans les pratiques contractuelles et donner lieu à des contrôles de sécurité insuffisants.
Plans et exercices de gestion des événements de cybersécurité	Décrire comment détecter des atteintes à la sécurité au sein d'un ministère et dans l'ensemble du gouvernement et intervenir en conséquence	• Le Secrétariat du Conseil du Trésor du Canada a en place le Plan de gestion des événements de cybersécurité du gouvernement du Canada pour détecter une attaque visant les systèmes d'information et de technologie d'une organisation, réagir à ces attaques et limiter leurs conséquences. • Les ministères doivent aussi avoir des plans assortis de procédures semblables.

Contrôle	Objectif	Rôles et responsabilités
		Ces plans sont essentiels pour protéger l'information et les biens technologiques contre les cybermenaces parce qu'ils présentent des politiques, des procédures, des rôles et responsabilités et des lignes directrices qui réduisent au minimum le temps de réaction et amoindrissent le risque de confusion.

Les mesures de sécurité d'informatique en nuage non validées et non surveillées de manière uniforme pour tous les contrats

7.26 Les mesures de sécurité d'informatique en nuage sont un ensemble de contrôles de base que les ministères doivent mettre en œuvre pour prévenir et détecter les cyberattaques dans leurs environnements infonuagiques. Les 12 mesures de sécurité d'informatique en nuage présentées à la pièce 7.2 visent à renforcer la sécurité dans les environnements basés sur le nuage.

7.27 Au titre de la Directive sur les services et le numérique du Conseil du Trésor, les ministères qui concluent des marchés avec des fournisseurs de services infonuagiques doivent mettre en œuvre des mesures de sécurité d'informatique en nuage avant d'utiliser ces services et veiller à ce que ces mesures restent en place. La Directive ne vise pas les contrats passés avec des fournisseurs de services infonuagiques autres que ceux établis par Services partagés Canada, notamment ceux conclus auprès de fournisseurs préqualifiés dans le cadre d'un arrangement en matière d'approvisionnement de Services publics et Approvisionnement Canada. Le Secrétariat du Conseil du Trésor du Canada a la responsabilité de surveiller la conformité des ministères aux mesures de sécurité d'informatique en nuage. Le Secrétariat peut révoquer l'accès d'un ministère au nuage si des mesures de protection ne sont pas mises en place.

7.28 Nous avons constaté que, dans le cadre des contrats qu'il avait établis entre des ministères et des fournisseurs de services infonuagiques, Services partagés Canada avait vérifié si les ministères avaient mis en œuvre les mesures de sécurité dans les trente premiers jours. Toutefois, il avait seulement réalisé des suivis en continu limités par la suite. Nous avons aussi constaté que pour les services infonuagiques établis par Services publics et Approvisionnement Canada, personne n'avait vérifié si les ministères avaient mis des mesures de sécurité en place au départ, et personne n'effectuait de suivi de la conformité en continu. À notre avis, ce manque d'uniformité

dans l'application des contrôles dans l'ensemble du gouvernement fait augmenter les risques de compromission des renseignements personnels de la population canadienne qui sont stockés dans le nuage.

Pièce 7.2 — Le gouvernement du Canada a établi 12 mesures de sécurité de l'informatique en nuage qui servent d'ensemble minimal de contrôles de sécurité

Mesures de sécurité d'informatique en nuage	Objectif
1. Protéger le compte racine ou des administrateurs généraux	Protéger le compte racine ou principal utilisé pour établir le service infonuagique.
2. Gestion des privilèges d'administration	Établir des stratégies et des procédures de contrôle d'accès pour la gestion des privilèges administratifs.
3. Accès à la console du nuage	Limiter l'accès aux appareils gérés par le gouvernement du Canada et aux utilisatrices et utilisateurs autorisés.
4. Comptes de surveillance organisationnels	Créer un compte fondé sur les rôles pour permettre la surveillance et la visibilité organisationnelle.
5. Emplacement des données	Établir des politiques pour limiter les applications et l'information sensibles du gouvernement du Canada aux emplacements géographiques approuvés.
6. Protection des données au repos	Protéger les données au repos par défaut (p. ex. stockage) pour les applications dans le nuage.
7. Protection des données en transit	Protéger les réseaux de transit de données à l'aide de mesures appropriées de chiffrement et de protection du réseau.
8. Segmenter et séparer	Segmenter et séparer les renseignements en fonction de leur sensibilité.
9. Services de sécurité du réseau	Établir des périmètres de réseau externes et internes et surveiller l'achalandage du réseau.
10. Services de cyberdéfense	Établir un protocole d'entente pour les services de défense et de surveillance des menaces.
11. Journalisation et surveillance	Activer la journalisation de l'information et des événements du réseau et du système pour l'environnement infonuagique et les charges de travail basées sur le nuage.
12. Configuration des contrats d'infonuagique	Restreindre les logiciels dans le marché des fournisseurs de services infonuagiques tiers aux produits approuvés par le gouvernement du Canada.

Source : D'après les Mesures de sécurité d'informatique en nuage du GC, gouvernement du Canada

7.29 Nous avons examiné la validation effectuée par Services partagés Canada de la façon dont les ministères avaient mis en œuvre les mesures de sécurité. Nous avons constaté que le Ministère n'avait pas évalué efficacement certains des contrôles et qu'il avait parfois attribué une note de passage à des ministères qui n'avaient pas correctement mis en œuvre les mesures de sécurité. Voici deux exemples que nous avons relevés :

- Dans le cadre de la mesure de sécurité nº 6 (sur la protection des données au repos), les ministères doivent demander des conseils aux responsables de la protection de la vie privée avant de stocker des renseignements personnels dans les environnements infonuagiques. Toutefois, nous avons constaté que Services partagés Canada n'avait pas vérifié si les ministères l'avaient fait.
- Dans le cadre de la mesure de sécurité nº 8 (sur la segmentation et la séparation de l'information), les ministères doivent fournir des diagrammes techniques de leurs conceptions de la sécurité réseau à des personnes chargées d'évaluer l'exhaustivité et l'exactitude de ces diagrammes. Or nous avons relevé un cas où la personne chargée de l'évaluation avait uniquement vérifié si un diagramme avait été fourni, et non s'il était complet ou exact.

7.30 Nous avons constaté que même si Services partagés Canada avait validé la mise en œuvre au sein de tous les ministères des 12 mesures de sécurité dans les 30 jours suivant l'établissement de leurs contrats avec des fournisseurs de services infonuagiques, il n'a assuré le suivi de la conformité continue que pour 2 mesures de sécurité sur 12. En outre, il n'a vérifié que les aspects administratifs de ces deux mesures (notamment ceux liés à la facturation et aux rapports) et pas si elles étaient toujours en place et si elles fonctionnaient comme prévu. Services partagés Canada laissait donc la surveillance en continu des mesures du point de vue de la sécurité à la discrétion de chaque ministère.

7.31 **Recommandation** — En consultation avec Services partagés Canada et Services publics et Approvisionnement Canada, le Secrétariat du Conseil du Trésor du Canada devrait faire ce qui suit :

- étendre les exigences relatives aux mesures de sécurité aux contrats de services infonuagiques qui découlent d'arrangements en matière d'approvisionnement établis par Services publics et Approvisionnement Canada;
- préciser qui est responsable de la validation initiale et de la surveillance en continu des mesures de sécurité d'informatique en nuage ainsi que les processus à suivre.

Réponse du Secrétariat du Conseil du Trésor du Canada — *Recommandation acceptée*.

Les réponses détaillées se trouvent dans le tableau **Recommandations et réponses** à la fin du présent rapport.

Les clauses de sécurité des contrats imprécises et non uniformisées

7.32 Nous avons constaté que les contrats de services infonuagiques mis en place par Services partagés Canada et les arrangements en matière d'approvisionnement établis par Services publics et Approvisionnement Canada comportaient peu de détails sur les obligations des fournisseurs de services en cas d'incidents de sécurité, notamment les délais d'intervention visés et les personnes chargées d'intervenir.

7.33 D'avril 2018 à mars 2022, les ministères ont attribué des contrats de services infonuagiques ou des arrangements en matière d'approvisionnement à 14 fournisseurs de services infonuagiques. Nous avons passé en revue tous ces contrats et arrangements et avons constaté que, même si les arrangements prévoyaient des obligations en matière de sécurité et de protection des renseignements personnels, aucun des ministères n'avait défini de manière suffisamment détaillée les obligations des ministères ou des fournisseurs de services infonuagiques en ce qui concerne la gestion des incidents de sécurité et des atteintes à la vie privée, notamment la rapidité avec laquelle les parties doivent intervenir et la personne chargée de communiquer les incidents et les atteintes (et à qui il faut les communiquer).

7.34 Nous avons aussi constaté qu'aucun des ministères n'avait inclus de clauses ou de conditions normalisées en matière de sécurité dans les contrats et les arrangements en matière d'approvisionnement qu'ils avaient établis. Toutefois, les deux ministères ont depuis reconnu la nécessité d'établir de telles clauses et conditions pour éviter les méthodes incompatibles de passation de contrats et le dédoublement des efforts. En février 2022, les ministères, avec le concours du Secrétariat du Conseil du Trésor du Canada et du Centre de la sécurité des télécommunications du Canada, ont formé un groupe de travail sur l'approvisionnement de services infonuagiques dans le but d'accomplir les tâches suivantes :

- mettre au point une approche d'approvisionnement de services infonuagiques du gouvernement du Canada assortie de modèles comprenant des modalités normalisées;
- normaliser les rôles et les responsabilités dans le cadre du processus d'approvisionnement de services infonuagiques;
- préciser les exigences relatives à la sécurité des contrats de services infonuagiques au sein du gouvernement fédéral.

Les lacunes en ce qui concerne les plans de gestion des événements de cybersécurité et leur utilisation

7.35 Lorsqu'un événement de cybersécurité se produit, les principales organisations chargées de la sécurité et les ministères doivent être en mesure d'intervenir rapidement et de manière coordonnée. Pour ce faire, ils doivent avoir en place des plans de gestion des événements de cybersécurité qui ont été mis à l'essai et dont l'efficacité a été prouvée dans le cadre d'exercices de simulation. La capacité du gouvernement à détecter les cyberattaques à l'échelle du gouvernement et à intervenir en conséquence dépend de la capacité de chaque ministère à le faire à l'échelle ministérielle.

7.36 Le Plan de gestion des événements de cybersécurité du gouvernement du Canada est entré en vigueur en avril 2020, remplaçant une version antérieure publiée en janvier 2018. Ce plan explique les rôles et responsabilités des ministères et des organismes centraux chargés de la coordination des interventions dans le cadre des événements ayant des répercussions sur l'ensemble du gouvernement. Il présente les procédures d'évaluation, de classification et d'acheminement des événements. Selon le Plan, les ministères doivent veiller à l'amélioration continue de leur capacité à réagir aux événements de cybersécurité. Ils doivent notamment tester les plans et les procédures, mettre en œuvre les leçons apprises, tenir à jour des listes de personnes à qui ont été assignées des responsabilités établies dans le plan et former le personnel, y compris le personnel chargé de la cybersécurité.

7.37 Dans le cadre de notre examen de l'intervention du gouvernement lors d'un événement antérieur, nous avons constaté que le Secrétariat du Conseil du Trésor du Canada et le Centre de la sécurité des télécommunications du Canada avaient mené des exercices sur les leçons apprises et élaboré un rapport, des recommandations et un plan d'action pour améliorer les interventions futures.

7.38 Toutefois, nous avons constaté que le Secrétariat du Conseil du Trésor du Canada n'a pas respecté les exigences établies dans le Plan de gestion des événements de cybersécurité du gouvernement du Canada concernant la mise à l'essai des plans et des procédures et la tenue à jour du plan :

- Le Secrétariat n'a pas mis à jour ni renouvelé le Plan malgré ses propres exigences consistant à mettre à l'essai, à modifier et à réviser le plan tous les ans. Il a rédigé une nouvelle version en octobre 2021, mais ne l'avait ni testée ni adoptée au moment de notre audit.
- Le Secrétariat du Conseil du Trésor du Canada a organisé des simulations théoriques pour tester et améliorer l'efficacité du plan. Toutefois, il en a organisé seulement trois depuis 2018 (soit environ une simulation tous les 17 mois), ce qui est bien en deçà du

minimum recommandé (soit une simulation tous les 12 mois). Des exercices de simulation réguliers sont requis en raison du roulement du personnel ainsi que de l'évolution des technologies et des milieux de travail.

7.39 Lors de notre examen des plans ministériels de gestion des événements de cybersécurité des trois ministères que nous avons sélectionnés pour l'audit, nous avons constaté ce qui suit :

- Chacun des trois ministères avait effectué des exercices de simulation et des tests de la sécurité de leurs applications annuellement.
- Chacun des ministères avait préparé des plans, mais deux ministères sur trois nous ont indiqué qu'ils n'avaient ni les fonds ni la capacité nécessaire pour assurer leur pleine mise en œuvre.
- Sur les trois ministères sélectionnés, deux n'avaient pas terminé la définition des rôles et des responsabilités internes pour la gestion des incidents.
- Même si le Secrétariat a commencé à recueillir de l'information auprès des ministères en septembre 2021, au moment de notre audit, il ne savait pas si tous les ministères avaient mis en œuvre des plans de gestion des événements de cybersécurité.

7.40 **Recommandation** — Le Secrétariat du Conseil du Trésor du Canada devrait faire ce qui suit :

- au moins une fois par année, vérifier que le Plan de gestion des événements de cybersécurité du gouvernement du Canada s'applique à l'environnement infonuagique en évolution et aux responsabilités partagées, le revoir et le tester, et le mettre à jour au besoin;
- assurer un suivi chaque année pour s'assurer que les ministères finalisent, exécutent et mettent régulièrement à l'essai leurs plans de gestion des événements de sécurité.

Réponse du Secrétariat du Conseil du Trésor du Canada — *Recommandation acceptée.*

Les réponses détaillées se trouvent dans le tableau **Recommandations et réponses** à la fin du présent rapport.

Les responsabilités et les rôles en matière de cybersécurité infonuagique étaient imprécis et incomplets

Ce que nous avons constaté

7.41 Nous avons constaté que la matrice des responsabilités et des rôles liés à l'infonuagique du gouvernement du Canada du Secrétariat du Conseil du Trésor du Canada, le principal outil que ce dernier utilise pour communiquer les responsabilités et les rôles partagés en matière d'infonuagique, omettait de l'information importante dont les ministères avaient besoin pour mener à bien leurs obligations en matière de cybersécurité. Par conséquent, les organisations ne savaient pas exactement qui devait faire quoi dans certains domaines, par exemple, qui devrait évaluer les contrôles de sécurité des technologies de l'information pour ce qui est des exigences relatives à l'emplacement des données.

7.42 L'analyse à l'appui de la constatation porte sur :

- la confusion des ministères par rapport à leurs rôles en matière de cybersécurité.

Importance de cette constatation

7.43 Cette constatation est importante parce que, même si chaque ministère est responsable et comptable en définitive des risques de sécurité découlant de son utilisation des services infonuagiques, la sécurité des renseignements personnels dans le nuage repose sur un modèle de responsabilité partagée entre, notamment, les ministères et les fournisseurs de services infonuagiques. Pour éviter les atteintes à la sécurité et intervenir rapidement et avec efficacité dans le cas d'une telle atteinte, les obligations, les responsabilités et les rôles doivent être clairement définis. S'il y a des lacunes ou de l'incertitude, les ministères pourraient ne pas comprendre leurs responsabilités en matière de cybersécurité et ne pas s'en acquitter adéquatement.

Contexte

7.44 Le Secrétariat du Conseil du Trésor du Canada communique ses décisions concernant les rôles et responsabilités en matière d'utilisation du nuage et de stockage dans cet environnement par les ministères au moyen de la matrice des rôles et des responsabilités liés à l'infonuagique du gouvernement du Canada, qu'il met à la disposition des ministères. Cette matrice vise à décrire la façon dont les ministères sont censés se répartir les responsabilités dans tous les domaines de l'adoption de l'infonuagique, y compris la sécurité.

Analyse à l'appui de la constatation

La confusion des ministères par rapport à leurs rôles en matière de cybersécurité

7.45 Nous avons constaté que la matrice des responsabilités et des rôles liés à l'infonuagique du gouvernement du Canada du Secrétariat du Conseil du Trésor du Canada ne comprenait pas ou ne modifiait pas les responsabilités et les rôles qui ont évolué ou qui ont été ajoutés depuis mars 2018, date de la dernière mise à jour de la matrice. Voici quatre exemples :

- Le Secrétariat n'avait pas inclus la mise en œuvre et la validation des mesures de sécurité d'informatique en nuage dans sa matrice.
- Le Centre de la sécurité des télécommunications du Canada a la responsabilité d'évaluer les contrôles de sécurité des technologies de l'information des fournisseurs de services infonuagiques. Toutefois, nous avons constaté qu'après la mise en œuvre de la matrice, les ministères avaient aussi l'option d'effectuer eux-mêmes certaines de ces évaluations. Il est difficile de savoir si le Centre devrait surveiller ou superviser les évaluations des Ministères.
- Les responsabilités du Centre de la sécurité des télécommunications du Canada en lien avec la surveillance des activités de nuage pour détecter les événements de cybersécurité et intervenir en conséquence, puis informer et appuyer les ministères touchés, ne sont pas décrites dans la matrice.
- La matrice ne comprend pas les responsabilités du Secrétariat concernant la coordination des exercices de gestion des événements de sécurité dans l'ensemble du gouvernement.

7.46 Les rôles et responsabilités en matière de sécurité infonuagique sont énoncés dans de multiples documents. Par conséquent, nous avons constaté que les ministères étaient confus quant à certains de leurs rôles et responsabilités. Par exemple, la Directive sur les services et le numérique indique que les ministères doivent veiller à ce que les données stockées dans le nuage, y compris les données de nature délicate et les renseignements personnels, soient conservées au Canada. Toutefois, après avoir passé en revue les contrats et arrangements en matière d'approvisionnement établis par Services partagés Canada et Services publics et Approvisionnement Canada, nous avons constaté que les parties concernées ne comprenaient pas toutes cette exigence :

- Les trois ministères sélectionnés nous ont dit qu'ils croyaient que Services publics et Approvisionnement Canada ou le Centre de la sécurité des télécommunications du Canada était responsable de vérifier la conformité à cette exigence.

- Des fonctionnaires de Services publics et Approvisionnement Canada nous ont indiqué que le Centre de la sécurité des télécommunications du Canada était responsable de cette exigence.
- Des fonctionnaires du Centre de la sécurité des télécommunications du Canada nous ont signalé que cette tâche relevait des dirigeantes principales et dirigeants principaux de l'information ou des responsables des données au sein de chaque ministère.

Faute de bien comprendre qui veille à ce que les données stockées dans le nuage restent au Canada, les organisations risquent de ne pas savoir si les renseignements personnels sont en fait stockés dans un autre pays et, le cas échéant, s'ils sont donc assujettis à des lois différentes (et possiblement inférieures) en matière de protection de la vie privée et à des protocoles différents en matière de sécurité.

7.47 **Recommandation** — En consultation avec le Centre de la sécurité des télécommunications du Canada, Services partagés Canada, Services publics et Approvisionnement Canada et les ministères, le Secrétariat du Conseil du Trésor du Canada devrait documenter les rôles et responsabilités nécessaires pour concevoir, mettre en œuvre, valider, surveiller, coordonner et appliquer les contrôles de sécurité nécessaires pour protéger les renseignements sensibles et personnels stockés dans le nuage et communiquer ces rôles et responsabilités de façon proactive à tout ministère qui a recours aux services infonuagiques ou qui envisage d'y avoir recours. Le Secrétariat devrait revoir et actualiser ces rôles et responsabilités au moins tous les 12 mois.

Réponse du Secrétariat du Conseil du Trésor du Canada — *Recommandation acceptée*.

Les réponses détaillées se trouvent dans le tableau **Recommandations et réponses** à la fin du présent rapport.

La fourniture d'un modèle d'établissement des coûts et de financement

Le Secrétariat du Conseil du Trésor du Canada n'avait pas fourni de modèle d'établissement des coûts des services infonuagiques aux ministères ou ne leur avait proposé aucune méthode en matière de financement

Ce que nous avons constaté

7.48 Nous avons constaté que, quatre ans après avoir demandé aux ministères d'amorcer la transition vers l'infonuagique, le Secrétariat du Conseil du Trésor du Canada ne leur avait toujours pas donné les outils requis pour comprendre ce qu'il en coûterait de passer à l'infonuagique et d'exploiter et de sécuriser les applications dans cet environnement,

par rapport au coût de leur maintien dans un centre de données de Services partagés Canada. Nous avons également constaté que lorsque les ministères choisissaient d'héberger leurs applications dans le nuage plutôt que dans un centre de données du gouvernement, ils devenaient responsables du financement relatif à l'exploitation continue et à la sécurité de ces services. Le financement fédéral de ces activités n'était pas transféré de Services partagés Canada aux ministères après l'adoption par ceux-ci des services infonuagiques.

7.49 L'analyse à l'appui de la constatation porte sur :

- L'absence de modèle d'établissement des coûts ou de méthode de financement à long terme

Importance de cette constatation

7.50 Cette constatation est importante parce que les Canadiennes et Canadiens s'attendent à ce que le gouvernement réduise au minimum les coûts et, même si les services infonuagiques peuvent donner des occasions de le faire, s'ils n'ont pas les outils adéquats, les ministères ne peuvent pas réaliser d'analyse des coûts et des avantages pour prendre des décisions éclairées. Il se peut aussi qu'ils ne disposent pas d'un financement adéquat pour appuyer leurs activités infonuagiques permanentes, y compris celles liées à la sécurité.

Analyse à l'appui de la constatation

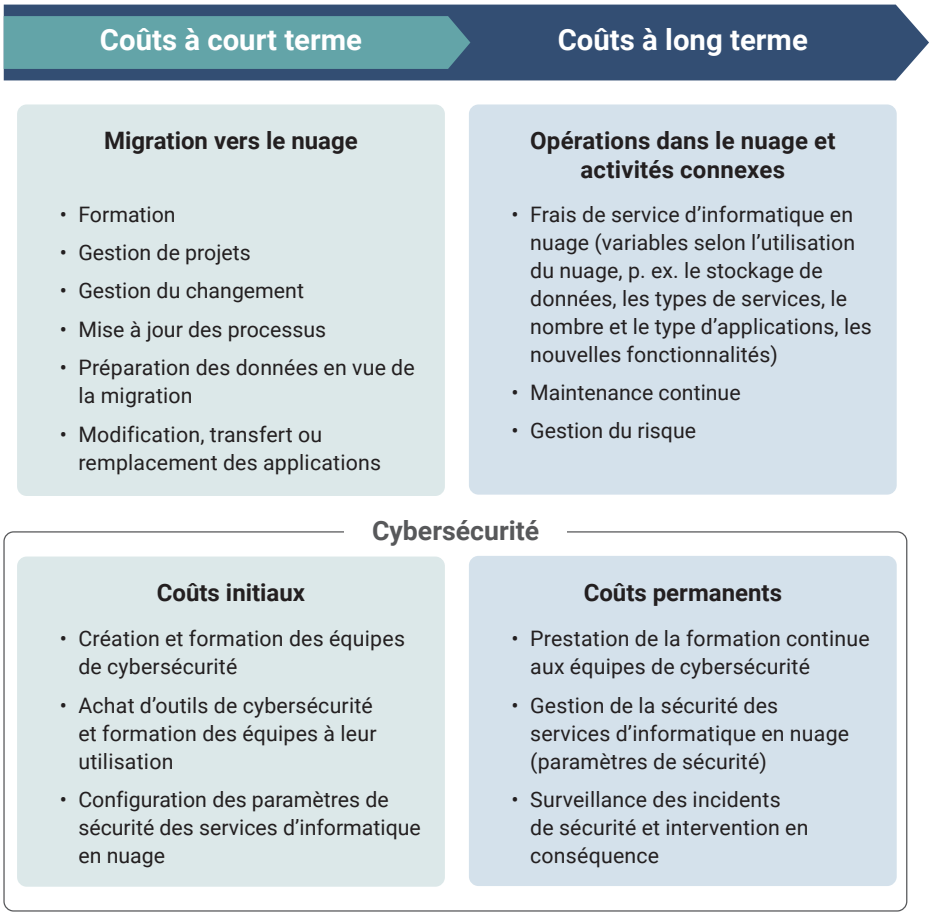
L'absence de modèle d'établissement des coûts ou de méthode de financement à long terme

7.51 Nous avons constaté que lorsque le Secrétariat du Conseil du Trésor a publié sa Stratégie d'adoption de l'infonuagique en 2018, il n'avait pas élaboré ni diffusé de méthode de financement à long terme ou de modèle d'établissement des coûts pour accompagner la Stratégie. Par ailleurs, le Secrétariat n'a pas pu nous fournir de tels documents aux fins d'examen dans le cadre de notre audit. Par conséquent, nous n'avons pas pu déterminer comment un tel modèle ou une telle méthode permettrait de remédier aux difficultés rencontrées par les ministères au moment de comprendre les coûts du passage de l'information vers le nuage et de la sécurisation de celle-ci ainsi que le financement requis pour assurer la protection à long terme de cette information.

7.52 Lorsque les ministères doivent décider si leurs applications ou services seront hébergés dans un centre de données de Services partagés Canada ou dans le nuage, le coût est un facteur important. Il en est ainsi parce que l'adoption de l'infonuagique transfère aux ministères certains coûts du stockage de données qui étaient auparavant pris en charge par Services partagés Canada. Les ministères endossent aussi la responsabilité de financer l'exploitation de l'infonuagique et les nouvelles

responsabilités en matière de cybersécurité qui les accompagnent. Il s'agit notamment de la création d'équipes dotées de compétences en infonuagique et en cybersécurité, l'achat d'outils de cybersécurité et le maintien des activités et de la sécurité en continu (voir la pièce 7.3).

Pièce 7.3 — L'adoption de l'infonuagique entraîne des coûts de cybersécurité à court et à long terme pour les ministères



Remarque : Ces listes donnent des exemples de considérations liées aux coûts et ne sont pas exhaustives.

7.53 Même si du financement à court terme a été mis à la disposition des ministères pour les aider à déplacer leurs applications vers le nuage, des groupes de travail et des comités de cadres supérieurs du gouvernement ont indiqué qu'ils ne savaient toujours pas comment les ministères financeront l'exploitation continue de l'infonuagique. Parallèlement, le Secrétariat nous a signalé que les dépenses ministérielles en services infonuagiques à l'échelle du gouvernement ont augmenté considérablement d'une année à l'autre, passant de 35 millions de dollars en 2018 à près de 120 millions de dollars en 2021.

7.54 Pour aider les ministères à mieux comprendre les coûts de l'adoption des services infonuagiques et éclairer leur prise de décisions, le Secrétariat a prévu d'élaborer un modèle d'établissement

des coûts que les ministères pourraient utiliser pour comparer les coûts du stockage et de l'hébergement des applications dans le nuage par rapport au stockage et à l'hébergement dans les centres de données du gouvernement du Canada. Ce modèle comprendrait les coûts d'acquisition, les coûts liés aux activités opérationnelles en continu (comme la surveillance et le maintien de la sécurité) et les coûts permanents des services infonuagiques. Le Secrétariat nous a également indiqué que le modèle serait axé sur la modernisation et sur l'hébergement des applications existantes.

7.55 Les ministères pourraient obtenir du financement en vue de moderniser la technologie, d'adopter de nouvelles pratiques et de renforcer la capacité et les compétences nécessaires à la modernisation. Pour toutes les nouvelles applications transférées au nuage, les ministères auraient à payer eux-mêmes les coûts liés à leur hébergement, à leur exploitation et à leur maintenance soit en réaffectant des fonds à l'interne ou en demandant des fonds nouveaux ou supplémentaires par l'intermédiaire de présentations au Conseil du Trésor.

7.56 En l'absence de financement à long terme pour l'exploitation en continu, les trois ministères que nous avons sélectionnés aux fins de l'audit se servaient de diverses mesures de financement à court terme pour appuyer l'exploitation de l'infonuagique et la cybersécurité. Ils procédaient notamment à la réaffectation de fonds destinés à d'autres fins. Selon les ministères, les coûts liés à la cybersécurité infonuagique ont nettement augmenté entre l'exercice 2020-2021 et l'exercice 2021-2022, et devraient demeurer élevés en 2022-2023. Par exemple, un ministère nous a signalé que ses coûts ont plus que triplé entre les exercices 2020-2021 et 2021-2022 (passant de 200 000 $ à 700 000 $), et qu'ils devraient se maintenir à ce niveau au cours de l'exercice 2022-2023. Les ministères ont indiqué que la nécessité d'utiliser un financement à court terme pour les services infonuagiques et de cybersécurité compromet la viabilité à long terme de ces activités.

7.57 Même si les grands ministères peuvent avoir la capacité d'absorber certains des coûts de l'adoption de l'infonuagique et des mesures de sécurité, cette approche n'est vraisemblablement pas durable à long terme, et les petits ministères pourraient être incapables d'assumer même une partie de ces coûts. En outre, le financement de la cybersécurité à même les ressources prévues pour les autres activités de technologie de l'information risquerait de compromettre celles-ci.

7.58 **Recommandation** — En consultation avec Services partagés Canada et d'autres ministères, le Secrétariat du Conseil du Trésor du Canada devrait :

- élaborer et fournir un modèle d'établissement des coûts afin d'aider les ministères à prendre des décisions éclairées au sujet de la

transition vers l'infonuagique et à déterminer si des ressources et du financement additionnels sont nécessaires;

- aider les ministères à évaluer le financement de fonctionnement à long terme dont ils ont besoin et appuyer leur accès au financement pour qu'ils puissent s'acquitter de leurs responsabilités en constante évolution à l'égard des activités liées à l'infonuagique, notamment la protection des renseignements de nature délicate dans le nuage.

Réponse du Secrétariat du Conseil du Trésor du Canada — *Recommandation acceptée*.

Les réponses détaillées se trouvent dans le tableau **Recommandations et réponses** à la fin du présent rapport.

La promotion de la responsabilité environnementale et du développement durable

Services publics et Approvisionnement Canada et Services partagés Canada n'avaient pas inclus de critères environnementaux dans le cadre de leurs processus d'approvisionnement en services infonuagiques

Ce que nous avons constaté

7.59 Nous avons constaté que Services publics et Approvisionnement Canada et Services partagés Canada n'avaient pas inclus de critères environnementaux dans le cadre de leurs processus d'approvisionnement en services infonuagiques, même si les deux organisations avaient élaboré des lignes directrices et de la formation obligatoire à l'intention du personnel sur la prise en compte des considérations environnementales dans l'approvisionnement en services, y compris en services infonuagiques.

7.60 L'analyse à l'appui de la constatation porte sur :

- l'absence de critères environnementaux dans le processus d'approvisionnement en services infonuagiques.

Importance de cette constatation

7.61 Cette constatation est importante parce que le gouvernement du Canada s'est fixé l'objectif d'atteindre la carboneutralité d'ici 2050, et il devrait donc veiller à harmoniser ses politiques et ses mesures avec cet objectif. Le fait de ne pas tenir compte des critères environnementaux dans l'approvisionnement en services infonuagiques est une occasion ratée pour les ministères de contribuer à la réalisation

de l'objectif et d'appuyer le Programme de développement durable à l'horizon 2030 des Nations Unies.

7.62 En outre, le Secrétariat du Conseil du Trésor et Services partagés Canada ont noté que les technologies numériques devraient être responsables de 8 % des émissions mondiales de gaz à effet de serre d'ici 2025 et de près de 14 % d'ici 2040. Le fait de ne pas inclure de critères environnementaux dans le processus d'approvisionnement en services infonuagiques entraîne un risque que l'adoption de l'infonuagique n'appuie pas la Stratégie pour un gouvernement vert et même contribue à faire augmenter les émissions.

Contexte

Établir des modes de consommation et de production durables

Source : Nations Unies

7.63 En 2015, le Canada s'est engagé à respecter le Programme de développement durable à l'horizon 2030 des Nations Unies, qui fixe 17 objectifs de développement durable. L'objectif 12 vise à établir des modes de consommation et de production durables. L'une de ses cibles consiste à « promouvoir des pratiques durables dans le cadre de la passation des marchés publics, conformément aux politiques et priorités nationales ».

7.64 En 2017, le Canada a lancé la Stratégie pour un gouvernement vert dans le but que toutes les organisations du gouvernement fédéral intègrent des considérations environnementales à leurs processus d'approvisionnement. La Stratégie recommande aux ministères d'encourager les fournisseurs à divulguer leurs émissions de gaz à effet de serre et des renseignements sur leur rendement environnemental.

7.65 En 2020, la Stratégie pour un gouvernement vert a été présentée en tant que directive du gouvernement du Canada. Elle indique que d'ici 2050, le Canada a l'intention d'atteindre la carboneutralité dans ses activités, y compris pour l'approvisionnement de ses biens et services. La Stratégie indique aussi que le gouvernement inclurait des critères visant à réduire les émissions de gaz à effet de serre dans ses processus d'approvisionnement de biens et de services qui ont une grande incidence sur l'environnement. Comme il a été noté dans le rapport de mai 2022 du commissaire à l'environnement et au développement durable sur la Stratégie pour un gouvernement vert, les progrès réalisés jusqu'ici montrent que le gouvernement n'est pas en voie d'atteindre son objectif de réduction des émissions.

7.66 De plus, la Politique d'achats écologiques de 2018 exige que Services publics et Approvisionnement Canada et Services partagés Canada incluent des options à privilégier en matière de services écologiques dans la mesure du possible. La Politique exige en outre que les ministères achètent de préférence des biens et des services écologiques offrant un bon rapport qualité-prix.

7.67 Au moment de l'audit, le gouvernement du Canada mettait à jour sa Stratégie d'adoption de l'infonuagique. La version la plus récente, datée de février 2022, comprenait une liste de 10 éléments visant à aider les ministères à réaliser une valeur opérationnelle. L'un de ces éléments porte sur la contribution à l'ensemble des objectifs du gouvernement en matière de développement durable par la mise en place d'une infrastructure hautement efficace à l'échelle de l'organisation qui permet de réduire les émissions de gaz à effet de serre et favorise l'écologisation du gouvernement.

Analyse à l'appui de la constatation

L'absence de critères environnementaux dans le processus d'approvisionnement en services infonuagiques

7.68 Nous avons constaté que le Secrétariat du Conseil du Trésor du Canada et Services publics et Approvisionnement Canada avaient élaboré des lignes directrices et de la formation pour aider les agentes et agents de négociation des contrats à intégrer les considérations environnementales dans le processus d'approvisionnement en services. Nous avons aussi constaté que Services publics et Approvisionnement Canada et Services partagés Canada avaient formé leurs agentes et agents d'approvisionnement aux pratiques d'approvisionnement écologiques.

7.69 Toutefois, nous avons constaté que ces ministères n'avaient pas exigé que les fournisseurs de services infonuagiques fassent état de leur rendement environnemental ou qu'ils expliquent comment leurs services contribueraient à réduire les émissions de gaz à effet de serre du Canada. Même si les ministères avaient demandé aux fournisseurs de services infonuagiques de fournir des renseignements sur leurs engagements en matière d'environnement et l'état de leurs activités, ils n'avaient pas exigé de les obtenir ou n'en avaient pas confirmé l'exactitude lorsqu'ils les avaient obtenus.

7.70 Nous avons examiné 14 contrats et arrangements en matière d'approvisionnement en services infonuagiques et avons constaté qu'aucun ne comportait de clauses liées à l'environnement. Par ailleurs, le Guide des clauses et conditions uniformisées d'achat de Services publics et Approvisionnement Canada ne contenait aucune clause environnementale relative aux services infonuagiques.

7.71 Services publics et Approvisionnement Canada nous a affirmé que les ministères peuvent inclure leurs propres exigences environnementales. Cependant, les ministères sélectionnés nous ont expliqué qu'ils ne rédigeaient pas leurs propres clauses contractuelles. Ils se fiaient plutôt au Guide des clauses et conditions uniformisées d'achat pour que les clauses soient appliquées de manière uniforme dans l'ensemble des ministères.

7.72 **Recommandation** — Services publics et Approvisionnement Canada et Services partagés Canada devraient inclure des critères environnementaux dans le cadre de l'approvisionnement en services infonuagiques afin de favoriser la durabilité des pratiques d'approvisionnement et de contribuer à l'atteinte de l'objectif de carboneutralité du Canada.

Réponse des ministères — *Recommandation acceptée.*

Les réponses détaillées se trouvent dans le tableau **Recommandations et réponses** à la fin du présent rapport.

Conclusion

7.73 Nous avons conclu que le Secrétariat du Conseil du Trésor du Canada, Services partagés Canada, Services publics et Approvisionnement Canada, le Centre de la sécurité des télécommunications Canada et les ministères sélectionnés disposaient de contrôles pour prévenir les événements de cybersécurité menaçant la sécurité des renseignements personnels des Canadiennes et des Canadiens dans le nuage, détecter ces événements et intervenir en conséquence. Toutefois, ils n'avaient pas mis en œuvre efficacement ces contrôles et n'avaient pas non plus établi et communiqué clairement les responsabilités et les rôles associés à leur mise en œuvre.

7.74 Nous avons aussi conclu que le Secrétariat du Conseil du Trésor du Canada n'avait pas fourni de méthode de financement ou de modèle d'établissement des coûts à long terme pour aider les ministères à mieux comprendre les coûts de la transition vers les services infonuagiques et de l'exploitation de cet environnement.

7.75 Enfin, nous avons conclu que le gouvernement fédéral n'avait pas inclus de critères environnementaux dans le cadre de ses processus d'approvisionnement en services infonuagiques, même si cela était requis pour réduire les émissions de gaz à effet de serre.

À propos de l'audit

Le présent rapport de certification indépendant sur la cybersécurité des renseignements personnels des Canadiennes et des Canadiens dans le nuage a été préparé par le Bureau du vérificateur général du Canada. Notre responsabilité était de donner de l'information, une assurance et des avis objectifs au Parlement en vue de l'aider à examiner soigneusement la gestion que fait le gouvernement des ressources et des programmes et d'exprimer une conclusion quant à la conformité du Secrétariat du Conseil du Trésor du Canada, de Services partagés Canada, de Services publics et Approvisionnement Canada, du Centre de la sécurité des télécommunications Canada (et de son Centre canadien pour la cybersécurité), et des ministères sélectionnés, dans tous ses aspects importants, aux critères applicables.

Tous les travaux effectués dans le cadre du présent audit ont été réalisés à un niveau d'assurance raisonnable conformément à la Norme canadienne de missions de certification (NCMC) 3001 — Missions d'appréciation directe de Comptables professionnels agréés du Canada (CPA Canada), qui est présentée dans le Manuel de CPA Canada — Certification.

Le Bureau du vérificateur général du Canada applique la Norme canadienne de contrôle qualité 1 et, en conséquence, maintient un système de contrôle qualité exhaustif qui comprend des politiques et des procédures documentées en ce qui concerne la conformité aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables.

Lors de la réalisation de nos travaux d'audit, nous nous sommes conformés aux règles sur l'indépendance et aux autres règles de déontologie des codes de conduite pertinents applicables à l'exercice de l'expertise comptable au Canada, qui reposent sur les principes fondamentaux d'intégrité, d'objectivité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

Conformément à notre processus d'audit, nous avons obtenu ce qui suit de la direction de l'entité :

- la confirmation de sa responsabilité à l'égard de l'objet considéré;
- la confirmation que les critères étaient valables pour la mission;
- la confirmation qu'elle nous a fourni toutes les informations dont elle a connaissance et qui lui ont été demandées ou qui pourraient avoir une incidence importante sur les constatations ou la conclusion contenues dans le présent rapport;
- la confirmation que les faits présentés dans le rapport sont exacts.

Objectif de l'audit

L'objectif de l'audit consistait à déterminer si le gouvernement fédéral — notamment le Secrétariat du Conseil du Trésor du Canada, Services partagés Canada, Services publics et Approvisionnement Canada, le Centre de la sécurité des télécommunications Canada (et son Centre canadien pour la cybersécurité), et les ministères sélectionnés — avait mis en place une gouvernance, des lignes directrices et des outils pour prévenir les événements de cybersécurité touchant les renseignements personnels des Canadiennes et des Canadiens dans le nuage, détecter ces événements et intervenir en conséquence.

Nous avons aussi cherché à déterminer si le gouvernement fédéral avait respecté ses engagements en matière d'environnement et de développement durable dans le cadre de ses processus d'approvisionnement en services infonuagiques. Comme le Bureau du vérificateur général du Canada s'est engagé à atteindre les objectifs de développement durable des Nations Unies, nous avons déterminé que l'objectif 12 s'appliquait à l'approvisionnement en services infonuagiques en raison de sa cible visant à promouvoir des pratiques durables dans le cadre du processus d'approvisionnement public, conformément aux politiques et aux priorités nationales.

Étendue et méthode

L'audit a porté sur la manière dont les ministères se partageaient les responsabilités en matière de sécurité des renseignements personnels. En effet, chaque ministère est responsable de la gestion du risque lié à la cybersécurité au sein de son organisation ainsi que de la mise en œuvre de contrôles de sécurité pour atténuer le risque lié à la cybersécurité dans ses programmes. Toutefois, les ministères dépendent des principales organisations responsables de la sécurité pour la mise en œuvre de certains contrôles de sécurité. Nous avons consulté les trois ministères sélectionnés, qui avaient recours à des services infonuagiques aux fins de stockage ou de traitement des renseignements personnels. Nous les avons interrogés sur les rôles et les responsabilités des principales organisations responsables de la sécurité et avons examiné comment tous les ministères avaient coordonné leur approche en matière de cybersécurité.

Nous avons relevé divers contrôles clés liés à l'atténuation des risques d'atteinte à la sécurité des renseignements personnels dans les applications et les services hébergés dans le nuage : les clauses de sécurité dans les contrats, la validation des mesures de sécurité, les évaluations des contrôles de sécurité matérielle et de sécurité du personnel des fournisseurs de services infonuagiques, les évaluations de la sécurité des services des fournisseurs de services infonuagiques, le Plan de gestion des événements de cybersécurité du gouvernement du Canada et les plans ministériels de gestion des événements de sécurité. Nous avons validé et confirmé l'exactitude, l'exhaustivité et la pertinence de ces contrôles auprès de chaque entité. S'il y avait lieu, nous les avons intégrés aux critères d'audit et nous avons procédé à des tests supplémentaires des contrôles au besoin.

Dans le cadre de nos travaux d'audit, nous avons examiné les plans, stratégies, politiques et lignes directrices connexes, nous nous sommes entretenus avec des porte-parole des ministères et nous avons réalisé des tests des contrôles afin de comprendre l'ensemble des pratiques et des systèmes que le gouvernement fédéral a mis en place pour assurer la sécurité des renseignements personnels dans le nuage. Nous avons réalisé les travaux suivants :

- examen des huit ententes-cadres conclues avec les fournisseurs de services infonuagiques et test d'un échantillon de six arrangements en matière d'approvisionnement pour la fourniture de services infonuagiques afin de déterminer si des exigences relatives à la sécurité (des clauses contractuelles) ont été fixées avec les fournisseurs de services infonuagiques;
- analyse de la validation des mesures de sécurité d'informatique en nuage des ministères sélectionnés;
- examen d'un échantillon de 14 rapports d'inspection liés à la sécurité matérielle sur les fournisseurs de services infonuagiques pour déterminer si les procédures d'inspection physiques avaient été suivies et si les résultats avaient été communiqués;

- examen d'un incident majeur de sécurité afin de déterminer si les procédures de gestion des événements de sécurité avaient été respectées.

Nous n'avons pas examiné les activités d'approvisionnement en services infonuagiques menées par les ministères sélectionnés dans les limites de leurs pouvoirs de passation de marchés. Nous n'avons pas non plus réalisé nos propres tests ou évaluations portant sur la sécurité des technologies de l'information des ministères sélectionnés.

Critères

Pour déterminer si le gouvernement fédéral — notamment le Secrétariat du Conseil du Trésor du Canada, Services partagés Canada, Services publics et Approvisionnement Canada, le Centre de la sécurité des télécommunications Canada (et son Centre canadien pour la cybersécurité), et les ministères sélectionnés — avait mis en place une gouvernance, des lignes directrices et des outils pour prévenir les événements de cybersécurité touchant les renseignements personnels des Canadiennes et des Canadiens dans le nuage, détecter ces événements et réagir en conséquence, nous avons utilisé les critères ci-dessous.

Nous avons également utilisé un critère ci-dessous pour déterminer si le gouvernement fédéral avait respecté ses engagements en matière d'environnement et de développement durable dans le cadre de ses processus d'approvisionnement en services infonuagiques.

Critères	Sources
Le Secrétariat du Conseil du Trésor du Canada définit les rôles et les responsabilités pour la cybersécurité des renseignements personnels dans le nuage.	• Conseil du Trésor, Politique sur la sécurité du gouvernement • Secrétariat du Conseil du Trésor du Canada, Directive sur la gestion de la sécurité • Conseil du Trésor, Politique sur les services et le numérique • Conseil du Trésor, Directive sur les services et le numérique • Secrétariat du Conseil du Trésor du Canada, Plan stratégique du gouvernement du Canada pour la gestion de l'information et la technologie de l'information de 2017 à 2021 • Secrétariat du Conseil du Trésor du Canada, Plan stratégique des opérations numériques : de 2021 à 2024 • Secrétariat du Conseil du Trésor du Canada, Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada, 2018 • Secrétariat du Conseil du Trésor du Canada, Cadre de mise en œuvre du nuage du gouvernement du Canada

Critères	Sources
Le Secrétariat du Conseil du Trésor du Canada a un modèle de financement qui fait en sorte que les ministères disposent des ressources nécessaires pour assurer la cybersécurité de leurs activités dans le nuage, détecter les menaces et intervenir en conséquence.	• Conseil du Trésor, Politique sur les services et le numérique • Conseil du Trésor, Directive sur les services et le numérique • Conseil du Trésor, Politique sur la planification et la gestion des investissements, 2019 • Conseil du Trésor, Politique sur la planification et la gestion des investissements, 2021 • Secrétariat du Conseil du Trésor du Canada, Plan stratégique du gouvernement du Canada pour la gestion de l'information et la technologie de l'information de 2017 à 2021 • Secrétariat du Conseil du Trésor du Canada, Plan stratégique des opérations numériques de 2018 à 2022 • Secrétariat du Conseil du Trésor du Canada, Plan stratégique des opérations numériques : de 2021 à 2024 • Secrétariat du Conseil du Trésor du Canada, Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada, 2018 • Budget 2018, Budget 2019 et Budget 2021
Services partagés Canada procède à la validation des mesures de sécurité d'informatique en nuage avant l'approbation des services infonuagiques.	• Gouvernement du Canada, Mesures de sécurité d'informatique en nuage du gouvernement du Canada • Secrétariat du Conseil du Trésor du Canada, Cadre de mise en œuvre du nuage du gouvernement du Canada • Secrétariat du Conseil du Trésor du Canada, Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage • Secrétariat du Conseil du Trésor du Canada, Gouvernement du Canada – Approche et procédures de gestion des risques à la sécurité de l'informatique en nuage • Profil des mesures de sécurité pour les services du gouvernement du Canada fondés sur l'informatique en nuage • Secrétariat du Conseil du Trésor du Canada, Procédure normale d'exploitation : Validation des mesures de sécurité d'informatique en nuage, 2019

Critères	Sources
Services publics et Approvisionnement Canada et Services partagés Canada, en collaboration avec les ministères sélectionnés, documentent les clauses contractuelles portant sur la gestion de la sécurité, les rôles et les responsabilités en matière de sécurité, la surveillance et les notifications de sécurité ainsi que les exigences relatives à l'emplacement des données.	• Conseil du Trésor, Politique sur la sécurité du gouvernement • Conseil du Trésor, Directive sur la gestion de la sécurité • Conseil du Trésor, Politique sur les services et le numérique • Conseil du Trésor, Directive sur les services et le numérique • Secrétariat du Conseil du Trésor du Canada, Ligne directrice sur les services et le numérique • Conseil du Trésor, Politique sur les marchés • Secrétariat du Conseil du Trésor du Canada, Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage • Secrétariat du Conseil du Trésor du Canada, Orientation relative à la résidence des données électroniques • Secrétariat du Conseil du Trésor du Canada, Gouvernement du Canada – Livre blanc : Souveraineté des données et nuage public • Services publics et Approvisionnement Canada, Guide des approvisionnements • Services publics et Approvisionnement Canada, Manuel de la sécurité des contrats • Services publics et Approvisionnement Canada, Guide des clauses et conditions uniformisées d'achat • Services partagés Canada, Guide des approvisionnements • Centre canadien pour la cybersécurité, Lignes directrices sur la chaîne d'approvisionnement des technologies • Centre canadien pour la cybersécurité, Guide sur l'évaluation et l'autorisation de la sécurité infonuagique • Centre canadien pour la cybersécurité, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie • Center for Internet Security, The 18 CIS Critical Security Controls (disponible en anglais seulement)

Critères	Sources
	• Association des professionnels de la vérification et du contrôle des systèmes d'information, Cadre COBIT 2019 (Objectifs de contrôle de l'information et des technologies associées)
Services publics et Approvisionnement Canada procède à la vérification de la conformité des fournisseurs de services infonuagiques (emplacements physiques et enquête sur le personnel) aux exigences relatives à la sécurité et à l'emplacement des données et effectue ces vérifications de manière périodique	• Conseil du Trésor, Politique sur la sécurité du gouvernement • Conseil du Trésor Directive sur la gestion de la sécurité • Secrétariat du Conseil du Trésor du Canada, Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage • Secrétariat du Conseil du Trésor du Canada, Orientation relative à la résidence des données électroniques • Secrétariat du Conseil du Trésor du Canada, Gouvernement du Canada – Livre blanc : Souveraineté des données et nuage public • Services publics et Approvisionnement Canada, Politique sur le Programme de sécurité des contrats, 2019 • Services publics et Approvisionnement Canada, Guide des approvisionnements • Services publics et Approvisionnement Canada, Manuel sur la sécurité des contrats • Centre canadien pour la cybersécurité, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie • Center for Internet Security, The 18 CIS Critical Security Controls (disponible en anglais seulement) • Association des professionnels de la vérification et du contrôle des systèmes d'information, Cadre COBIT 2019 (Objectifs de contrôle de l'information et des technologies associées) • Organisation internationale de normalisation, ISO/IEC 27001, Management de la sécurité de l'information

Critères	Sources
Le Centre de la sécurité des télécommunications Canada et le Centre canadien pour la cybersécurité procèdent à des évaluations de la sécurité des fournisseurs de services infonuagiques et communiquent les résultats aux ministères fédéraux.	• *Loi sur le Centre de la sécurité des télécommunications* • Conseil du Trésor, Politique sur la sécurité du gouvernement • Conseil du Trésor, Directive sur la gestion de la sécurité • Conseil du Trésor, Politique sur les services et le numérique • Conseil du Trésor, Directive sur les services et le numérique • Centre canadien pour la cybersécurité, Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques • Centre canadien pour la cybersécurité, Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique • Centre canadien pour la cybersécurité : La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie • Secrétariat du Conseil du Trésor du Canada, Cadre de mise en œuvre du nuage du gouvernement du Canada • Center for Internet Security, The 18 CIS Critical Security Controls (disponible en anglais seulement) • Association des professionnels de la vérification et du contrôle des systèmes d'information, Cadre COBIT 2019 (Objectifs de contrôle de l'information et des technologies associées) • Organisation internationale de normalisation, ISO/IEC 27001, Management de la sécurité de l'information

Critères	Sources
Le Secrétariat du Conseil du Trésor du Canada et le Centre de la sécurité des télécommunications Canada (et son Centre canadien pour la cybersécurité) ont un processus en place pour assurer la liaison avec les parties prenantes et les administratrices générales et administrateurs généraux au sujet d'événements de sécurité qui pourraient avoir des répercussions sur l'ensemble du gouvernement. Les ministères sélectionnés documentent les pratiques de gestion des événements de sécurité et procèdent à des exercices pour détecter les événements de cybersécurité, y réagir et produire des rapports afférents. Ils coordonnent ces activités au sein de leur ministère, avec les fournisseurs de services infonuagiques ainsi qu'avec le Secrétariat du Conseil du Trésor du Canada, le Centre de la sécurité des télécommunications Canada et le Centre canadien pour la cybersécurité pour les événements touchant l'ensemble du gouvernement. Le Secrétariat du Conseil du Trésor du Canada coordonne les exercices pangouvernementaux de gestion des événements de sécurité visant à détecter les événements de cybersécurité, à y réagir et à produire des rapports afférents.	• Conseil du Trésor, Politique sur la sécurité du gouvernement • Conseil du Trésor, Directive sur la gestion de la sécurité • Conseil du Trésor, Politique sur les services et le numérique • Conseil du Trésor, Directive sur les services et le numérique • Secrétariat du Conseil du Trésor du Canada, Cadre de mise en œuvre du nuage du gouvernement du Canada • Secrétariat du Conseil du Trésor du Canada, Normes relatives au numérique du gouvernement du Canada : Directives • Secrétariat du Conseil du Trésor du Canada, Plan de gestion des événements de cybersécurité du gouvernement du Canada, 2019 • Gouvernement du Canada, Stratégie de consignation des événements, 2019 • Secrétariat du Conseil du Trésor du Canada, Guide sur la consignation d'événements • Centre canadien pour la cybersécurité, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie • Center for Internet Security, The 18 CIS Critical Security Controls (disponible en anglais seulement) • Centre canadien pour la cybersécurité, Les 10 meilleures mesures de sécurité des TI • Cloud Security Aliance, Cloud Controls Matrix (disponible en anglais seulement) • Association des professionnels de la vérification et du contrôle des systèmes d'information, Cadre COBIT 2019 (Objectifs de contrôle de l'information et des technologies associées)

Critères	Sources
Le gouvernement fédéral respecte ses engagements en matière d'environnement et de développement durable dans le cadre de ses processus d'approvisionnement en services infonuagiques.	• Conseil du Trésor, Politique d'achats écologiques • Conseil du Trésor, Politique sur les marchés • Environnement et Changement climatique Canada, Réaliser un avenir durable : Stratégie fédérale de développement durable pour le Canada, 2016-2019 • Secrétariat du Conseil du Trésor du Canada, Stratégie pour un gouvernement vert : Une directive du gouvernement du Canada, 2020 • Conseil du Trésor, Directive sur la gestion de l'approvisionnement • Services publics et Approvisionnement Canada, Guide des approvisionnements • Services publics et Approvisionnement Canada, Guide des clauses et conditions uniformisées d'achat • Services partagés Canada, Guide des approvisionnements

Période visée par l'audit

L'audit a porté sur la période allant du 1er avril 2017 au 31 mars 2022. Il s'agit de la période à laquelle s'applique la conclusion de l'audit.

Date du rapport

Nous avons fini de rassembler les éléments probants suffisants et appropriés à partir desquels nous avons fondé notre conclusion le 21 octobre 2022, à Ottawa, au Canada.

Équipe d'audit

L'audit a été réalisé par une équipe multidisciplinaire du Bureau du vérificateur général du Canada dirigée par Jean Goulet, directeur principal. Le directeur principal est responsable de la qualité de l'audit dans son ensemble. Il doit s'assurer notamment que les travaux d'audit sont exécutés conformément aux normes professionnelles, aux exigences des textes légaux et réglementaires applicables ainsi qu'aux politiques et au système de gestion de la qualité du Bureau.

Recommandations et réponses

Dans le tableau qui suit, le numéro qui précède chaque recommandation correspond au numéro du paragraphe de la recommandation dans le rapport.

Recommandation	Réponse
7.31 En consultation avec Services partagés Canada et Services publics et Approvisionnement Canada, le Secrétariat du Conseil du Trésor du Canada devrait faire ce qui suit : • étendre les exigences relatives aux mesures de sécurité aux contrats de services infonuagiques qui découlent d'arrangements en matière d'approvisionnement établis par Services publics et Approvisionnement Canada; • préciser qui est responsable de la validation initiale et de la surveillance en continu des mesures de sécurité d'informatique en nuage ainsi que les processus à suivre.	**Réponse du Secrétariat du Conseil du Trésor du Canada** — Recommandation acceptée. Le Secrétariat du Conseil du Trésor du Canada collaborera avec Services partagés Canada, le Centre de la sécurité des télécommunications et Services publics et Approvisionnement Canada pour : • publier la matrice des responsabilités liées à l'infonuagique afin d'indiquer officiellement les personnes responsables de valider et de surveiller de façon continue les contrôles de protection, de les superviser et d'en assurer la conformité d'ici la fin de septembre 2022; • clarifier et prolonger les processus devant être suivis pour les contrats attribués aux fournisseurs de services infonuagiques par Services publics et Approvisionnement Canada dans le cadre des mises à jour à la procédure normalisée d'exploitation pour valider les contrôles de protection du nuage d'ici décembre 2022; • mettre à jour les contrôles de protection du nuage du gouvernement du Canada et la directive sur les services et le numérique pour refléter les contrôles de protection qui s'appliquent aux services infonuagiques, y compris les services infonuagiques fournis par Services publics et Approvisionnement Canada d'ici janvier 2023. En outre, le Secrétariat du Conseil du Trésor du Canada: • établira une carte de pointage pour rendre compte du niveau de conformité des ministères aux contrôles de protection du nuage du gouvernement du Canada d'ici février 2023; • collaborera avec Services partagés Canada dans ses efforts pour mettre en œuvre les outils servant à automatiser la surveillance des contrôles de protection pour les fournisseurs des services infonuagiques les plus utilisés au gouvernement du Canada d'ici avril 2023;

Recommandation	Réponse
	• continuera de fournir des conseils et une orientation aux ministères sur la façon de faire en sorte qu'ils effectuent les activités d'évaluation de la sécurité et d'autorisation pour les applications infonuagiques au moyen d'outils comme le guide de sécurité pour les solutions du système informatique qui décrit un ensemble de tâches de sécurité à prendre en considération au moment de concevoir et de mettre en œuvre des solutions pour les systèmes de renseignements du gouvernement du Canada dans les environnements infonuagiques.
7.40 Le Secrétariat du Conseil du Trésor du Canada devrait faire ce qui suit : • au moins une fois par année, vérifier que le Plan de gestion des événements de cybersécurité du gouvernement du Canada s'applique à l'environnement infonuagique en évolution et aux responsabilités partagées, le revoir et le tester, et le mettre à jour au besoin; • assurer un suivi chaque année pour s'assurer que les ministères finalisent, exécutent et mettent régulièrement à l'essai leurs plans de gestion des événements de sécurité.	**Réponse du Secrétariat du Conseil du Trésor du Canada** — Recommandation acceptée. Le Secrétariat du Conseil du Trésor du Canada fera en sorte : • que le Plan de gestion des événements de cybersécurité (PGECS) du gouvernement du Canada soit examiné et mis à l'essai au moins une fois par année et mis à jour au besoin. Cela comprend une mise à jour du PGECS du gouvernement du Canada dont la publication est prévue à la fin de l'automne 2022 et l'inclusion de scénarios infonuagiques dans des exercices de simulation du PGECS du gouvernement du Canada; • qu'un processus soit en place pour vérifier que les ministères ont établi et mis en œuvre un PGECS ministériel qui concorde avec le PGECS du gouvernement du Canada et qui est soumis une fois par année au Secrétariat du Conseil du Trésor du Canada aux fins d'examen d'ici l'automne 2023; • que des outils soient prévus et disponibles, ce qui permettra aux ministères de mettre régulièrement à l'essai le PGECS de leur ministère, comme un produit de simulation préparé à l'avance qui met l'accent sur un scénario infonuagique que les ministères peuvent utiliser pour exécuter leur propre exercice de simulation, ainsi que d'explorer des options pour établir un mode d'approvisionnement qui permettra de faciliter les exercices de simulation infonuagiques d'ici mars 2023.

Recommandation	Réponse
7.47 En consultation avec le Centre de la sécurité des télécommunications du Canada, Services partagés Canada, Services publics et Approvisionnement Canada et les ministères, le Secrétariat du Conseil du Trésor du Canada devrait documenter les rôles et responsabilités nécessaires pour concevoir, mettre en œuvre, valider, surveiller, coordonner et appliquer les contrôles de sécurité nécessaires pour protéger les renseignements sensibles et personnels stockés dans le nuage et communiquer ces rôles et responsabilités de façon proactive à tout ministère qui a recours aux services infonuagiques ou qui envisage d'y avoir recours. Le Secrétariat devrait revoir et actualiser ces rôles et responsabilités au moins tous les 12 mois.	**Réponse du Secrétariat du Conseil du Trésor du Canada** — Recommandation acceptée. Le Secrétariat du Conseil du Trésor du Canada collaborera avec le Centre de la sécurité des télécommunications, Services partagés Canada, Services publics et Approvisionnement Canada et les ministères pour : • publier la matrice des responsabilités liées à l'infonuagique afin d'indiquer officiellement les personnes responsables de valider et de surveiller de façon continue les contrôles de protection, de les superviser et d'en assurer la conformité d'ici la fin de septembre 2022; • effectuer un examen pour faire en sorte que les rôles et les responsabilités requis à l'appui de la conception, de la mise en œuvre, de la validation, de la surveillance, de la coordination et de l'exécution de tous les contrôles de sécurité nécessaire pour protéger les renseignements personnels et de nature délicate dans le nuage sont pertinents, mis à jour et documenté dans la matrice des responsabilités liées à l'infonuagique d'ici mars 2023; • accroître les communications régulières et proactives sur les rôles et les responsabilités dans n'importe quel ministère qui utilise ou envisage d'utiliser des services infonuagiques en apportant des mises à jour à la matrice des responsabilités liées à l'infonuagique par l'intermédiaire de forums comme le Comité d'examen de l'architecture intégrée du gouvernement du Canada, le comité directeur sur l'infonuagique du directeur général, le groupe de travail sur le réseau d'experts en matière d'infonuagique et d'informatique du gouvernement du Canada ainsi que des sites d'échange de renseignements comme l'infocentre sur l'infonuagique du gouvernement du Canada à compter de septembre 2023; • établir un processus pour un examen annuel et une publication de la matrice des responsabilités liées à l'infonuagique et fournir des mises à jour à la communauté d'ici mars 2023.

Recommandation	Réponse
7.58 En consultation avec Services partagés Canada et d'autres ministères, le Secrétariat du Conseil du Trésor du Canada devrait : • élaborer et fournir un modèle d'établissement des coûts afin d'aider les ministères à prendre des décisions éclairées au sujet de la transition vers l'infonuagique et à déterminer si des ressources et du financement additionnels sont nécessaires; • aider les ministères à évaluer le financement de fonctionnement à long terme dont ils ont besoin et appuyer leur accès au financement pour qu'ils puissent s'acquitter de leurs responsabilités en constante évolution à l'égard des activités liées à l'infonuagique, notamment la protection des renseignements de nature délicate dans le nuage.	**Réponse du Secrétariat du Conseil du Trésor du Canada** — Recommandation acceptée. Le Secrétariat du Conseil du Trésor du Canada consulte actuellement la communauté du gouvernement du Canada pour discuter des modèles opérationnels de l'infonuagique, des critères d'établissement de priorités et des modèles de financement connexes. Une série de recommandations orientera la dirigeante principale de l'information du gouvernement du Canada sur les directives pour mener des activités dans le nuage à l'automne 2022. Le Secrétariat du Conseil du Trésor du Canada, en consultation avec les ministères et Services partagés Canada : • élaborera et fournira un modèle d'établissement des coûts et des conseils pour aider les ministères à prendre des décisions informées sur le passage à l'infonuagique d'ici juin 2023; • aidera les ministères, y compris Services partagés Canada, à prévoir les coûts à moyen et long terme requis pour fonctionner dans un environnement infonuagique d'ici juin 2023.
7.72 Services publics et Approvisionnement Canada et Services partagés Canada devraient inclure des critères environnementaux dans le cadre de l'approvisionnement en services infonuagiques afin de favoriser la durabilité des pratiques d'approvisionnement et de contribuer à l'atteinte de l'objectif de carboneutralité du Canada.	**Réponse du Ministère** — Recommandation acceptée. Services publics et Approvisionnement Canada et Services partagés Canada conviennent que des critères environnementaux devraient être inclus dans l'approvisionnement en services infonuagiques. Pour le moment, l'accord-cadre infonuagique de Services partagés Canada n'inclut pas en soi des exigences en matière de durabilité, mais il offre la possibilité d'inclure de telles exigences dans les futures sollicitations. Services partagés Canada a élaboré des critères environnementaux cotés, qu'il prévoit d'inclure dans les prochains appels d'offres concurrentiels en vertu de l'accord-cadre infonuagique du gouvernement du Canada à compter de l'automne 2022. Cet accord-cadre comprend des exigences d'écologisation liées aux objectifs de réduction des gaz à effet de serre. De plus, Services partagés Canada a confirmé qu'à l'heure actuelle, sept des huit fournisseurs de l'accord-cadre infonuagique du gouvernement du Canada ont des cibles égales ou supérieures aux engagements nets zéro du Canada.

Recommandation	Réponse
	L'arrangement en matière d'approvisionnement (AMA) pour les logiciels-services de Services publics et Approvisionnement Canada n'évalue pas les critères environnementaux, mais il recueille cette information auprès des fournisseurs afin d'aider les clients à évaluer les solutions de logiciels-services offertes par l'AMA. Services publics et Approvisionnement Canada prévoit actualiser l'information environnementale recueillie dans l'AMA pour les logiciels-services de Services publics et Approvisionnement Canada et mettre à jour l'AMA afin d'aborder les priorités du gouvernement du Canada liées aux émissions nettes de gaz à effet de serre (GES). L'AMA permettra aux clients d'inclure des critères environnementaux dans les appels d'offres lancés dans le cadre de l'AMA, et Services publics et Approvisionnement Canada compte élaborer des clauses contractuelles résultantes concernant les émissions de GES liées aux objectifs de réduction des GES. Services partagés Canada et Services publics et Approvisionnement Canada ont également collaboré pour harmoniser davantage l'approche de l'approvisionnement infonuagique. Dans le cadre de cet exercice, un modèle standard pour les contrats infonuagiques est en cours d'élaboration et devrait être publié à l'automne 2022. Ce modèle comprendra des conditions de durabilité standard pour les fournisseurs de services infonuagiques.