CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

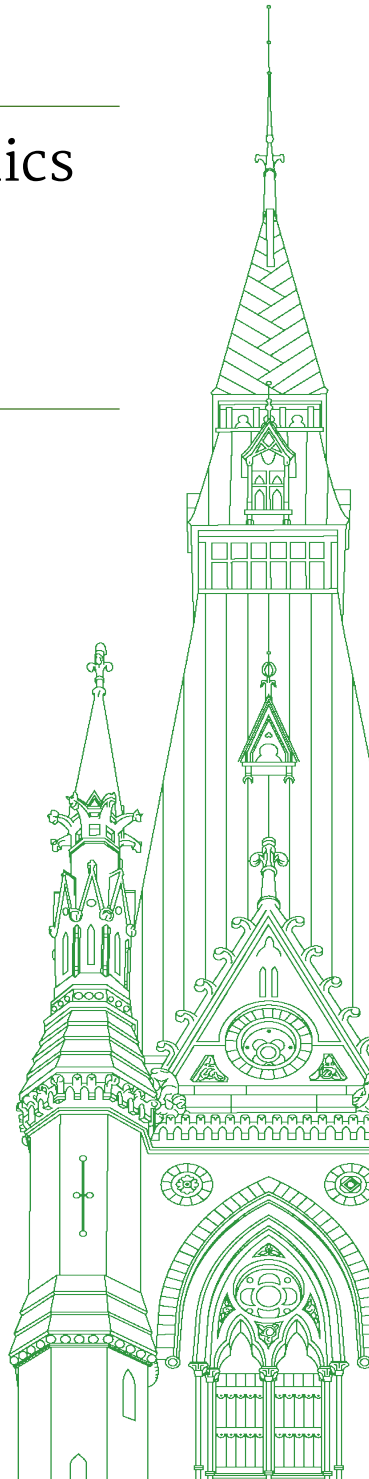
44e LÉGISLATURE, 1re SESSION

Comité permanent des comptes publics

TÉMOIGNAGES

NUMÉRO 056

Le jeudi 30 mars 2023



Président : M. John Williamson

Comité permanent des comptes publics

Le jeudi 30 mars 2023

● (1530)

[*Français*]

Le président (M. John Williamson (Nouveau-Brunswick-Sud-Ouest, PCC)): Je déclare la séance ouverte.

Bonjour, tout le monde. Bienvenue à la 56e réunion du Comité permanent des comptes publics de la Chambre des communes.

Conformément à l'article 108(3)g) du Règlement, le Comité se réunit aujourd'hui pour examiner le rapport 7 de la vérificatrice générale du Canada, intitulé « La cybersécurité des renseignements personnels dans le nuage », dans le cadre de son étude portant sur les rapports 5 à 8 de 2022 de la vérificatrice générale du Canada.

[*Traduction*]

J'aimerais souhaiter la bienvenue à nos témoins.

Tout d'abord, nous accueillons M. Andrew Hayes, sous-vérificateur général, du Bureau du vérificateur général. Nous sommes heureux que vous soyez des nôtres.

Nous avons aussi MM. Jean Goulet et Gabriel Lombardi, directeurs principaux. Merci d'être ici aujourd'hui.

Nous accueillons également M. Rajiv Gupta, dirigeant associé du Centre canadien pour la cybersécurité, qui relève du Centre de la sécurité des télécommunications. Bonjour.

Nous recevons aussi M. Paul Thompson, sous-ministre de Travaux publics et Services gouvernementaux Canada, par vidéoconférence, ainsi que Mme Catherine Poulin, sous-ministre adjointe de la Direction générale de la surveillance.

Nous avons aussi deux représentants de Services partagés Canada, soit M. Sony Perron, président, et M. Costas Theophilos, directeur général de la Direction de la gestion des produits et des services infonuagiques.

Enfin, nous accueillons Mme Catherine Luelo, sous-ministre et dirigeante principale de l'information du Canada pour le Secrétariat du Conseil du Trésor.

Il y aura donc plusieurs déclarations.

Monsieur Hayes, c'est vous qui allez ouvrir le bal. Vous avez la parole pour cinq minutes.

M. Andrew Hayes (sous-vérificateur général, Bureau du vérificateur général): Monsieur le Président, je vous remercie de nous donner l'occasion de discuter de notre rapport sur la cybersécurité des renseignements personnels dans le nuage, qui a été déposé à la Chambre des communes le 15 novembre 2022.

Je tiens à reconnaître que cette séance se déroule sur le territoire traditionnel non cédé du peuple algonquin anishinabe. Je suis accompagné aujourd'hui de Jean Goulet et de Gabriel Lombardi, qui ont dirigé cet audit.

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 Canadiens. L'information stockée numériquement, soit sur place dans des centres de données ou dans le nuage, est exposée à des risques de compromission.

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 sélectionnés disposaient de contrôles pour prévenir et détecter les menaces à la sécurité des renseignements personnels de la population canadienne stockés dans le nuage et intervenir en conséquence.

Dans l'ensemble, nous avons constaté que les ministères que nous avons audités ne respectaient et ne mettaient pas toujours en œuvre les contrôles établis par le gouvernement pour protéger les renseignements stockés dans le nuage ou transmis au moyen du nuage. Ces contrôles comprennent entre autres le chiffrement et les exigences relatives à la sécurité du réseau. Nous avons aussi constaté que les exigences de sécurité, de même que les responsabilités et les rôles connexes, n'étaient pas toujours clairement définis, ce qui a donné lieu à une mise en œuvre non uniforme. Par conséquent, l'information stockée dans le nuage est vulnérable aux cyberattaques, qui sont de plus en plus fréquentes et perfectionnées.

[*Français*]

Nous avons aussi constaté que, quatre ans après avoir demandé aux ministères fédéraux d'envisager la transition vers l'infonuagique, le Secrétariat du Conseil du Trésor du Canada n'avait toujours pas fourni de plan 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 et de l'exploitation de l'infonuagique.

En l'absence d'un plan de financement et d'outils d'établissement des coûts, il est difficile pour les ministères de s'assurer qu'ils disposent de la main-d'œuvre, des ressources et de l'expertise dont ils ont besoin pour sécuriser l'information stockée dans le nuage et intervenir en cas de menaces. Ce plan et ces outils renforceraient les capacités de cyberdéfense du gouvernement du Canada, tant à l'échelle des ministères que dans l'ensemble du gouvernement.

Enfin, nous avons constaté que Services publics et Approvisionnement Canada ainsi que Services partagés Canada 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. Cette constatation est importante, car le Canada s'est fixé l'objectif d'atteindre la carboneutralité d'ici 2050 et s'est engagé à inclure des critères visant à réduire les émissions de gaz à effet de serre dans les processus d'approvisionnement de biens et de services du gouvernement. À ce jour, cela n'a pas été fait dans le cadre de l'approvisionnement en services infonuagiques.

Le gouvernement doit prendre des mesures immédiates, pendant que les ministères en sont aux premières étapes de la transition vers l'infonuagique. Il doit s'assurer que du financement est disponible et que les principaux contrôles de sécurité sont renforcés de façon à prévenir et à détecter les cyberattaques et à intervenir en conséquence. Il est nécessaire, entre autres, de définir des responsabilités et des rôles communs clairs en matière de cybersécurité, de sorte que les ministères concernés, les organismes centraux et les fournisseurs de services infonuagiques sachent exactement ce qu'ils doivent faire.

Je termine ainsi ma déclaration d'ouverture. Nous serons heureux de répondre aux questions des membres du Comité.

Merci.

● (1535)

Le président: Merci beaucoup, monsieur Hayes.

[*Traduction*]

Je cède maintenant la parole au représentant du Centre de la sécurité des télécommunications.

Vous disposez de cinq minutes.

M. Rajiv Gupta (dirigeant associé, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): Monsieur le président, membres du Comité, merci de m'avoir invité à comparaître dans le cadre de l'étude du rapport de la vérificatrice générale du Canada sur la cybersécurité des renseignements personnels dans le nuage, qui a été déposé au Parlement.

Je m'appelle Rajiv Gupta et mes pronoms sont « il » et « lui ». Je suis le dirigeant associé du Centre canadien pour la cybersécurité, ou Centre pour la cybersécurité, au Centre de la sécurité des télécommunications.

[*Français*]

Le Centre canadien pour la cybersécurité est l'autorité technique en matière de cybersécurité au Canada. Il protège le pays en misant sur des capacités de cybersécurité avancées et constitue la seule source unifiée de soutien et d'avis spécialisés pour les questions opérationnelles en matière de cybersécurité.

[*Traduction*]

Je suis heureux d'avoir à mes côtés mes collègues du Secrétariat du Conseil du Trésor, de Services partagés Canada, et de Services publics et Approvisionnement Canada, car nous avons collaboré étroitement sur des questions de cybersécurité.

Dans le cadre de son rôle opérationnel, le Centre pour la cybersécurité publie des alertes de cybersécurité et des évaluations de menace à l'échelle du gouvernement du Canada afin que les systèmes d'information demeurent sécurisés et protégés et qu'ils puissent contrer les menaces les visant. Dans le cadre de son rôle éducatif, le Centre pour la cybersécurité s'efforce d'accroître les connaissances en matière de cybersécurité au gouvernement grâce à des initiatives comme le Carrefour de l'apprentissage.

[*Français*]

Le Carrefour de l'apprentissage est situé dans le Centre canadien pour la cybersécurité et offre de la formation visant à améliorer la cybersécurité du gouvernement du Canada et des organisations liées aux infrastructures essentielles.

[*Traduction*]

Durant l'exercice 2021-2022, le Carrefour de l'apprentissage a renouvelé sa collaboration avec l'École de la fonction publique du Canada, ou EFPC, afin d'offrir un programme de cybersécurité uniforme à l'ensemble des...

M. Maninder Sidhu (Brampton-Est, Lib.): J'invoque le Règlement, monsieur le président. Je n'entends pas l'interprétation.

Le président: Je suis désolé, vous n'entendez pas l'interprétation?

Je vais vérifier auprès du greffier. Un instant, je vous prie.

Monsieur Gupta, je vais vous donner un peu plus de temps. Vous pourriez peut-être recommencer au début de votre paragraphe et ralentir un peu le débit. Les interprètes ont parfois du mal à suivre le rythme. C'est ce qui pourrait expliquer le problème.

Entendez-vous l'interprétation maintenant? Oui, d'accord.

Je vous redonne la parole, monsieur. Merci.

[*Français*]

M. Rajiv Gupta: Merci beaucoup.

Comme je le disais, le Carrefour de l'apprentissage est situé dans le Centre canadien pour la cybersécurité et offre de la formation visant à améliorer la cybersécurité du gouvernement du Canada et des organisations liées aux infrastructures essentielles.

[*Traduction*]

Durant l'exercice 2021-2022, le Carrefour de l'apprentissage a renouvelé sa collaboration avec l'École de la fonction publique du Canada, ou EFPC, afin d'offrir un programme de cybersécurité uniforme à l'ensemble des fonctionnaires fédéraux. Le personnel du Carrefour de l'apprentissage et celui de l'EFPC ont créé ensemble un cours en ligne afin d'offrir aux fonctionnaires ne travaillant pas dans un domaine technique des connaissances de base sur l'informatique en nuage. Il s'agit d'une priorité pour la fonction publique alors que l'infrastructure TI des ministères continue de migrer vers le nuage.

Les organismes du gouvernement du Canada tirent de plus en plus parti de l'informatique en nuage, qui a le potentiel d'offrir des services de TI souples, flexibles et rentables. Comme l'indique son rapport annuel de 2021-2022, le CST ne cesse d'ouvrir la voie en ce qui a trait à la migration gouvernementale vers le nuage.

[*Français*]

En effet, le CST a adopté très tôt des technologies infonuagiques et s'est également assuré d'être le premier à appliquer ses propres avis et conseils internes.

● (1540)

[*Traduction*]

Il a d'ailleurs été le premier organisme à mettre en oeuvre d'une manière sécurisée des applications commerciales infonuagiques en installant des capteurs au niveau du nuage. L'organisme a aussi fait preuve de leadership en communiquant à d'autres ministères les leçons qu'il a apprises ainsi que des avis et des conseils pertinents.

Comme je l'ai mentionné, le Centre pour la cybersécurité est l'entité opérationnelle qui est responsable de protéger le gouvernement du Canada contre les cybermenaces, comme les rançongiciels et le cyberespionnage.

[*Français*]

Nous travaillons avec des partenaires fédéraux pour défendre les réseaux gouvernementaux et l'information de nature délicate des institutions fédérales.

[*Traduction*]

Bien que le risque zéro n'existe pas en ce qui a trait aux cybermenaces, nous veillons à la mise en place des mesures de protection les plus élevées. Le Centre pour la cybersécurité a recours à des capteurs autonomes qui détectent les cyberactivités malveillantes visant les réseaux, les systèmes et l'infrastructure infonuagique du gouvernement. Nous utilisons trois types de capteurs: les capteurs au niveau du réseau, les capteurs au niveau du nuage et les capteurs au niveau de l'hôte.

Ces capteurs permettent au Centre pour la cybersécurité de détecter les cybermenaces en temps réel. Grâce aux connaissances classifiées que nous détenons sur les comportements des auteurs de menace, nous pouvons assurer notre défense et bloquer ces menaces.

Nous collaborons avec nos partenaires fédéraux pour que des mesures de protection adéquates soient mises en oeuvre afin d'assurer la sécurité et la confidentialité de l'information qu'ils placent dans le nuage. L'environnement infonuagique ne cesse d'évoluer et nous continuons d'améliorer parallèlement nos outils pour veiller à la défense et à la sécurisation des systèmes gouvernementaux.

[*Français*]

Je tiens à remercier le Bureau du vérificateur général du Canada pour le rapport qu'il a déposé, ainsi que les membres du Comité pour la possibilité de discuter ensemble de ce sujet important.

[*Traduction*]

Bien qu'aucune des recommandations formulées dans le rapport ne vise le CST en particulier, nous sommes heureux d'en tenir compte. Le CST et le Centre pour la cybersécurité prennent très au sérieux la sécurité de l'information, y compris des données gouvernementales hébergées dans le nuage. Par conséquent, nous continuerons de collaborer avec nos partenaires fédéraux afin de suivre ces recommandations.

Membres du Comité, je peux vous assurer que le CST continuera de travailler avec ses partenaires afin de renforcer la cybersécurité au Canada tout en veillant à la mise en place des mesures nécessaires pour garantir la protection de la vie privée de la population canadienne.

Merci de m'avoir donné l'occasion de contribuer à cette importante étude, et c'est avec plaisir que je répondrai maintenant à vos questions.

Le président: Merci beaucoup.

Je cède maintenant la parole à M. Thompson, si je ne me trompe pas, du ministère des Travaux publics et des Services gouvernementaux.

La parole est à vous pour cinq minutes.

M. Paul Thompson (sous-ministre, ministère des Travaux publics et des Services gouvernementaux): Merci beaucoup, monsieur le président.

Je suis heureux de prendre la parole devant vous et les membres du Comité au sujet des mesures que Services publics et Approvisionnement Canada compte prendre à la suite de la vérification de la cybersécurité des renseignements personnels dans le nuage.

[*Français*]

Je suis accompagné aujourd'hui de Mme Catherine Poulin, sous-ministre adjointe de la Direction générale de la surveillance.

Notre ministère s'est engagé, comme acheteur des biens et des services du gouvernement du Canada, à faire en sorte que ses processus d'approvisionnement répondent aux besoins des ministères et des organismes qui composent sa clientèle.

[*Traduction*]

Nous sommes conscients de l'importance de la cybersécurité dans toutes les facettes des activités du gouvernement du Canada, et le gouvernement continue d'investir dans le renforcement de ses capacités à cet égard. Dans le budget de 2023, il prévoit 25 millions de dollars pour que Services publics et Approvisionnement Canada établisse, en collaboration avec la Défense nationale et d'autres intervenants, un programme de certification en cybersécurité pour les achats militaires, afin de mieux protéger la chaîne d'approvisionnement de la défense du Canada.

Par ailleurs, nous savons qu'en utilisant l'infonuagique pour les applications logicielles et les bases de données, nous avons la possibilité non seulement d'améliorer la façon dont les organisations fédérales servent la population, mais aussi de réduire le coût et la maintenance des applications et des serveurs physiques.

Il est clair que les ministères qui ont recours à l'infonuagique, dans le cadre de la stratégie numérique du gouvernement, devront travailler en étroite collaboration pour gérer les risques de sécurité posés par le nuage.

● (1545)

[*Français*]

Sachant que les cybermenaces et les cyberattaques sont de plus en plus graves et fréquentes, notre ministère a accueilli favorablement les résultats de la vérification sur la protection des renseignements personnels dans le nuage.

SPAC, quant à lui, joue deux rôles de soutien importants.

[*Traduction*]

Étant l'acheteur principal du gouvernement du Canada, SPAC fait l'acquisition de services infonuagiques pour le compte des ministères et des organismes. Pour en simplifier le processus, il a établi un arrangement en matière d'approvisionnement avec des fournisseurs qui ont été préqualifiés. De plus, SPAC évalue les contrôles de sécurité physique des fournisseurs de services infonuagiques et de leur personnel.

Lorsque des ministères se chargent eux-mêmes d'acheter des services infonuagiques à l'aide de notre arrangement en matière d'approvisionnement ou d'autres mécanismes d'approvisionnement, nous nous employons à les conseiller et à les guider pour faire en sorte que le nuage soit protégé contre les atteintes à la cybersécurité.

Monsieur le président, bien que la sécurité de l'information soit une priorité importante du gouvernement du Canada, SPAC est déterminé à contribuer à la réalisation d'une autre priorité, à savoir la promotion de la responsabilité environnementale et du développement durable.

Dans son rapport, la vérificatrice générale souligne, à juste titre, que nos processus contractuels n'exigent pas des fournisseurs de services infonuagiques qu'ils fassent état de leur rendement environnemental ou qu'ils expliquent comment leurs services peuvent contribuer à réduire les émissions de gaz à effet de serre du Canada. Elle ajoute que même lorsque des fournisseurs donnent de tels renseignements, il n'y a aucun mécanisme en place pour en confirmer l'exactitude.

La vérificatrice recommande que Services publics et Approvisionnement Canada et Services partagés Canada incluent des critères environnementaux dans leurs achats de services infonuagiques. Ils favoriseront ainsi la durabilité des pratiques d'approvisionnement et aideront le Canada à atteindre son objectif de carboneutralité.

Nos deux organisations souscrivent à cette recommandation. Services publics et Approvisionnement Canada s'est engagé à y donner suite en collaboration avec ses collègues de Services partagés Canada. Concrètement, nous allons exiger des fournisseurs qu'ils donnent des renseignements sur leurs engagements en matière de carboneutralité; inclure, dans les contrats pour des services infonuagiques, des clauses qui comprennent des cibles de réduction des émissions de gaz à effet de serre; et revoir les clauses uniformisées des contrats que nous utilisons pour l'acquisition de services infonuagiques et nos demandes de propositions.

[*Français*]

Nous nous employons également à ajouter des critères environnementaux aux mécanismes d'achat de services infonuagiques existants.

En conclusion, je veux remercier la vérificatrice générale pour son rapport. Je crois que ses recommandations orienteront les améliorations à apporter aux pratiques concernant les services infonuagiques.

Grâce à une collaboration soutenue avec ses partenaires, SPAC sera mieux placé pour respecter ses obligations en matière de changements climatiques et il pourra mieux protéger les renseignements de la population canadienne.

Je vous remercie de votre écoute. Je serai heureux de répondre à vos questions.

Le président: Merci beaucoup, monsieur Thompson.

[*Traduction*]

Je cède maintenant la parole à M. Perron, de Services partagés Canada. Vous disposez de cinq minutes.

M. Sony Perron (président, Services partagés Canada): Je vous remercie, monsieur le président ainsi que les membres du Comité, de votre invitation.

Je suis heureux d'être ici aujourd'hui, en compagnie de Costas Theophilos, directeur général, Gestion des produits et des services infonuagiques, pour répondre aux questions du Comité à propos de l'audit de la vérificatrice générale et des progrès réalisés par Services partagés Canada dans la mise en œuvre des recommandations qui s'y trouvent.

Conformément à son mandat qui consiste à fournir une infrastructure de technologie de l'information moderne et sécurisée, Services partagés Canada modernise l'infrastructure de TI du gouvernement du Canada de façon continue. Pour ce faire, Services partagés Canada a adopté une approche d'entreprise qui permet de poursuivre le regroupement, la normalisation et la modernisation des réseaux et des systèmes à l'échelle du gouvernement.

Il est essentiel de suivre l'évolution constante de la technologie et la croissance des cybermenaces. Ainsi, au cours des dernières années, nous avons largement adopté des solutions numériques, en optimisant notamment l'environnement infonuagique. Nous devons absolument suivre le rythme de ces innovations.

L'adoption de l'infonuagique est une responsabilité partagée au sein du gouvernement du Canada. Services partagés Canada offre un accès contrôlé et sécurisé à l'environnement infonuagique à l'échelle de l'organisation. Plus précisément, Services partagés Canada, facilite l'adoption de l'infonuagique par les ministères et organismes. Il leur donne accès à des éléments de base essentiels, comme l'approvisionnement, la connectivité réseau infonuagique sécurisée, ainsi qu'à des conseils et à de l'expertise.

Dans cette optique, Services partagés Canada collabore avec les ministères pour effectuer la migration des données et des applications se trouvant actuellement dans des centres de données vieillissants vers des infrastructures modernes, comme le nuage et les centres de données d'entreprise. Cette démarche permet d'accélérer la modernisation des applications de manière agile, sécuritaire et rentable.

Protéger les renseignements de la population canadienne est une priorité absolue pour Services partagés Canada. C'est pourquoi il est important que l'ensemble des ministères et des organismes adoptent une approche commune. Nous en sommes encore aux premières étapes de l'adoption de l'infonuagique; il faut donc s'attendre à des améliorations et à une évolution des processus et des protocoles.

Bien qu'on ne puisse jamais parler de « risque zéro » en ce qui concerne les cybermenaces, nous veillons à mettre en place les niveaux de protection les plus élevés. Il est important de noter que toutes les informations sont stockées au Canada, et que les informations les plus sensibles sont stockées dans des centres de données appartenant au gouvernement du Canada.

[*Français*]

Nous accueillons favorablement le rapport et les recommandations de la vérificatrice générale. Cet audit nous aide à renforcer le cadre opérationnel des services infonuagiques. Ce renforcement est particulièrement important alors que nous nous fions de plus en plus à l'environnement infonuagique.

SPC a un rôle dans quatre des cinq recommandations de l'audit.

Pour ce qui est de la première recommandation, SPC collabore étroitement avec le Secrétariat du Conseil du Trésor pour renforcer la validation et l'application des mesures de sécurité et pour s'assurer de la coordination avec les ministères. Les mesures de sécurité pour l'infonuagique établissent des exigences de sécurité minimales de configurations et d'opérations que les ministères doivent respecter dans les environnements infonuagiques. Cela comprend la façon dont les données sont gérées et le lieu où elles sont stockées. SPC a amorcé l'automatisation des mesures de sécurité afin d'évaluer la conformité en temps réel. Ce système sera mis à l'essai avec des ministères pilotes à partir de l'automne 2023.

En ce qui concerne la deuxième recommandation, le gouvernement du Canada a fixé une exigence de sécurité minimale pour les informations dans le nuage. SPC collabore avec les ministères pour valider les situations où des écarts persistent.

À l'égard de la troisième recommandation, qui porte sur les modèles de financement de l'infonuagique, SPC travaille avec le Secrétariat du Conseil du Trésor pour déterminer les prochaines étapes de l'établissement d'un modèle de recouvrement des coûts de l'infonuagique. Nous envisageons que le modèle de coûts soit disponible sous peu.

Pour ce qui est de la quatrième recommandation, SPC ainsi que Services publics et Approvisionnement Canada publieront bientôt un modèle standard de contrat de services infonuagiques. Celui-ci comprendra des modalités relatives à la durabilité pour les fournisseurs de services infonuagiques.

De fait, SPC a commencé à inclure des critères environnementaux dans les appels d'offres publiés au titre de l'accord-cadre infonuagique. Par exemple, certaines procédures comprennent désormais des critères cotés, ce qui encourage les fournisseurs à fixer des objectifs de réduction des émissions de gaz à effet de serre.

À l'avenir, SPC inclura les critères environnementaux cotés dans tous les nouveaux appels d'offres concurrentiels aux termes de l'accord-cadre infonuagique.

Monsieur le président, membres du Comité, SPC travaille sans relâche pour gérer les risques de sécurité liés à l'infonuagique et pour améliorer la cybersécurité afin de protéger les données et la vie privée des Canadiens et des Canadiennes.

Merci. Nous répondrons avec plaisir à vos questions.

● (1550)

[*Traduction*]

Le président: Merci beaucoup.

Enfin, c'est au tour de Mme Luelo, du Secrétariat du Conseil du Trésor.

Vous avez la parole pour cinq minutes.

Mme Catherine Luelo (sous-ministre, dirigeante principale de l'information du Canada, Secrétariat du Conseil du Trésor): Je vous remercie, monsieur le président, de même que les membres du Comité. C'est la première fois que je comparais devant le Comité. Je connais déjà certains d'entre vous et je suis heureuse de rencontrer les autres aujourd'hui.

Je travaille pour le gouvernement depuis 21 mois, après avoir passé 30 ans dans le secteur privé. J'en suis donc à mes premières armes en ce qui concerne tous ces différents exercices.

En ma qualité de dirigeante principale de l'information du Canada, j'assure un leadership d'ensemble pour la gestion de la technologie de l'information ainsi que pour la gestion de l'information, des services et de la transformation numérique au sein du gouvernement du Canada. Je suis entourée de mes collègues ici aujourd'hui, mais nous pourrions être accompagnés de 100 autres personnes de tous les ministères. La modernisation de l'infrastructure numérique du gouvernement est un travail d'équipe, tout comme la cybersécurité, bien sûr.

Mon organisation gère certaines lois, comme celles qui concernent l'accès à l'information et le gouvernement ouvert, et nous supervisons tous les grands programmes de technologie. Nous sommes également responsables du Plan de gestion des événements de cybersécurité du gouvernement du Canada — c'est tout un titre —, que nous désignons aussi par l'acronyme PGEC GC.

En ce qui concerne la protection des renseignements personnels des Canadiens, nous établissons les politiques, définissons les exigences en matière de cybersécurité et mettons à exécution les décisions relatives à la gestion des risques liés à la cybersécurité pour le compte du gouvernement. Notre travail est encadré par la Politique sur la sécurité du gouvernement, la Politique sur les services et le numérique et divers mécanismes sous-jacents, comme les normes numériques.

Je souhaite faire passer quelques messages de première importance en réponse au rapport de la vérificatrice générale. Nous accueillons favorablement ce rapport et, comme la vérificatrice l'a fait remarquer, nous en sommes au stade des balbutiements. Nous en sommes au début du commencement. C'est le moment idéal pour nous de recevoir ces constatations qui nous permettront de nous améliorer. D'après l'expérience que j'ai acquise dans d'autres milieux, une fonction d'audit rigoureuse aide vraiment les organisations à vocation technologique à s'améliorer. Je suis impatiente d'établir une collaboration continue avec la vérificatrice générale dans ce dossier et d'autres.

Comme je l'ai mentionné, nous entamons tout juste le processus de modernisation de notre environnement technologique. Seulement 35 % des systèmes du gouvernement du Canada sont en bon état et le nuage est essentiel à leur modernisation. La migration vers le nuage est un des moyens dont on dispose, et il convient de signaler que des organisations publiques et privées du monde entier font face à la même situation. J'ai travaillé pour plusieurs grandes entreprises canadiennes, et j'y ai observé certains des éléments que nous avons remarqués ici.

Le gouvernement du Canada prend la protection des renseignements des Canadiens très au sérieux et, comme Sony l'a dit, les services ne seront pas tous hébergés dans le nuage. Notre plan ne consiste pas à utiliser uniquement le nuage. Il y aura le nuage, certes, mais il y aura aussi des centres de données d'entreprise, en partie pour des raisons financières et en partie pour des raisons utilitaires. Les mesures de sécurité du nuage, qui sont un ensemble normalisé de contrôles, évolueront au fil du temps. Le contexte des menaces change, tout comme l'environnement technique, et nous y demeurerons attentifs. Nous continuerons de resserrer la surveillance et les mécanismes de contrôle de la conformité pour l'utilisation de l'infonuagique dans l'ensemble de l'administration publique afin de veiller à ce que les directives et les exigences de conformité soient très claires.

Je tiens à parler de quelques domaines où nous avons fait des progrès depuis la publication du rapport de la vérificatrice générale. Nous avons mis à jour le document sur les rôles et les responsabilités liés à infonuagique, y compris une matrice connexe, et nous l'avons publié à l'interne pour que les membres de notre équipe puissent y avoir accès. En novembre 2022, nous avons mis à jour le Plan de gestion des événements de cybersécurité du gouvernement du Canada. Il s'agit du plan que nous avons mis en place pour réagir aux incidents de cybersécurité qui visent l'organisation gouvernementale. Ce plan, dont la première version a été publiée en 2015, est continuellement mis à l'épreuve, examiné et ajusté, comme le veut la pratique courante pour tout type de plan de cybersécurité. En fait, il y a environ quatre semaines, nous avons effectué une simulation à l'échelle du gouvernement. Cet examen comprenait une composante infonuagique, ce qui nous a permis de commencer à mettre à l'épreuve nos mesures d'intervention en cas de cyberincidents dans le nuage.

De plus, nous avons publié en janvier une nouvelle version de la stratégie d'informatique en nuage qui était en préparation depuis plusieurs mois. Nous avons remplacé l'expression l'« informatique en nuage d'abord » par l'« informatique en nuage intelligente » afin de refléter concrètement que nous n'allons pas adopter systématiquement l'infonuagique, mais que nous allons plutôt prendre des décisions équilibrées en fonction de plusieurs facteurs, dont le facteur financier... L'approche de l'informatique en nuage d'abord était la bonne pour donner son élan au gouvernement. Il fallait commencer à orienter les gens vers la nouvelle technologie, et cette approche a permis de mettre le navire sur la bonne voie, pour ainsi dire. Nous avons environ 800 applications hébergées dans le nuage, ce qui demeure un très faible pourcentage de l'ensemble des systèmes qui existent à l'échelle du gouvernement.

● (1555)

Il convient de souligner que mon bureau a publié en janvier des lignes directrices sur la classification des renseignements personnels dans le nuage et, en coordination avec de nombreuses personnes ici présentes, nous avons décidé de désigner certains actifs de grande valeur — comme les renseignements personnels — et certains systèmes qui bénéficieront d'une protection accrue grâce à la mise en place d'un ensemble de contrôles additionnels. Le Programme de modernisation du versement des prestations, qui héberge une grande quantité de données sur les Canadiens, est un bon exemple de cas où nous allons utiliser cette approche.

Enfin, en ce qui concerne l'élaboration continue d'un modèle d'établissement des coûts du nuage, dont Sony a déjà parlé, nous devrions être prêts à publier un document à ce sujet pendant l'été ou à l'automne. Le travail dans ce dossier est déjà très avancé. Le document aidera les ministères à prendre des décisions éclairées sur la migration vers l'infonuagique, en ce qui a trait non seulement au coût de la migration, mais aussi au coût d'exploitation de l'infonuagique. Il est très utile de comprendre ces deux aspects de la question. Nous nous acquitterons ainsi de nos responsabilités liées à la recommandation 4.

Pour conclure, notre but ultime consiste à offrir aux Canadiens, aux entreprises canadiennes et à tous les utilisateurs le service performant et de grande qualité auquel ils s'attendent à l'ère numérique. L'infonuagique fera partie de cette démarche. Nous évaluerons régulièrement notre progression vers l'atteinte de cet objectif, et l'infonuagique est une composante importante de ce plan.

Monsieur le président, je vous remercie encore une fois de m'avoir invitée à comparaître devant vous aujourd'hui. Je serai ravie de répondre à vos questions.

Le président: Merci beaucoup.

Je tiens à dire quelques mots avant de poursuivre.

Selon moi, le rapport dont nous sommes saisis aujourd'hui est l'un des documents les plus importants que le gouvernement peut produire dans le cadre de son travail. En effet, on ne parle pas seulement d'argent ou de politiques, sujets sur lesquels les membres du Comité et les fonctionnaires se penchent constamment, mais bien de l'identité des Canadiens, dont la valeur peut être inestimable. J'espère que le Bureau du vérificateur général continuera de prioriser cet examen pour garantir que les normes en vigueur assureront toujours la sécurité de l'identité et des renseignements des Canadiens.

Je vais poser deux petites questions pour aider les autres membres du Comité.

Monsieur Hayes, je sais qu'au moins une recommandation n'a pas été faite publiquement. Est-ce la seule ou y en a-t-il d'autres que vous avez jugé bon de ne pas divulguer publiquement dans le rapport que nous étudions aujourd'hui?

M. Andrew Hayes: Je vous remercie.

C'est la seule recommandation qui n'a pas été rendue publique.

Le président: Merci.

La question suivante est de nature générale, mais je vais vous la poser, monsieur Perron, car je crois que vous connaissez la réponse. La loi canadienne actuelle exige-t-elle que les renseignements du gouvernement fédéral soient hébergés au pays?

M. Sony Perron: Oui.

Le président: Est-ce que cette exigence est inscrite dans la loi?

M. Sony Perron: Elle figure dans la politique, mais je ne crois pas qu'elle soit inscrite dans la loi. Cette politique relève d'ailleurs de la compétence de Catherine.

Le président: Merci. Je suis certain qu'il y aura des questions à cet égard. Je voulais seulement préparer le terrain parce qu'il y a eu des discussions à ce sujet.

Madame Kusie, vous avez la parole pour six minutes.

[*Français*]

Mme Stephanie Kusie (Calgary Midnapore, PCC): Merci beaucoup, monsieur le président.

Je remercie les témoins d'être parmi nous aujourd'hui.

[*Traduction*]

Monsieur Perron, vous avez dit que le modèle de prévision des coûts proposé sera disponible au printemps 2023. Seriez-vous en mesure de le faire parvenir au Comité lorsqu'il sera prêt?

● (1600)

M. Sony Perron: Je vous remercie de la question, monsieur le président.

C'est un document qui est le fruit de la collaboration entre plusieurs ministères, sous la direction du Secrétariat du Conseil du Trésor. Il n'y a rien à cacher. Nous allons le communiquer aux ministères parce qu'il s'agit d'un outil, et je suppose que je pourrai le transmettre au Comité lorsqu'il sera prêt à être distribué.

Catherine a peut-être quelque chose à ajouter à ce sujet.

Mme Catherine Luelo: Nous serons ravis de vous envoyer ce document.

Mme Stephanie Kusie: Merci infiniment.

Pouvez-vous me dire si les résultats des essais menés auprès des ministères qui participeront au projet pilote à l'automne 2023 pourront être examinés par les parlementaires, et plus particulièrement par les membres du présent comité?

M. Sony Perron: Monsieur le président, je crois que la députée parle de l'automatisation de la vérification des mesures de sécurité. Nous devrons trouver un moyen de vous transmettre cette information. En fait, il existe actuellement 12 mesures de sécurité. Sur les conseils judicieux de la vérificatrice générale, mon équipe a entrepris de vérifier que ces mesures assurent une sécurité constante, pas uniquement au début du processus, mais tout au long de celui-ci. Il s'agira davantage d'une surveillance que d'un exercice ponctuel.

À l'heure actuelle, nous surveillons la conformité de chaque ministère. C'est simplement que le processus n'est pas automatisé. Ce sont les gens de l'équipe de Costa qui vérifient manuellement, sur une base régulière, autour de 200 instances de service infonuagique pour s'assurer que les ministères utilisent ce dernier conformément aux normes établies. Souvent, il suffit d'activer une fonction, mais si le sélecteur est déplacé vers la gauche, par exemple, cela ne fonctionne plus. Nous devons donc veiller à ce que les paramètres soient maintenus, parce que c'est cela qui protège le système.

Pour répondre à la question, nous pouvons certainement revenir devant le Comité ou transmettre au greffier les résultats de notre examen.

Mme Stephanie Kusie: Merci.

Madame Luelo, pensez-vous que les normes d'adaptation à l'infonuagique adoptées par le gouvernement du Canada sont à la hauteur de celles qui sont adoptées à l'étranger?

Mme Catherine Luelo: Je pense que les situations auxquelles nous faisons face sont très semblables à ce qui se passe dans d'autres organisations qui en sont au même stade que nous. Moins de 10 % de nos systèmes sont hébergés dans le nuage. Selon moi, nous adoptons des pratiques exemplaires courantes et, malheureusement, nous tirons souvent les mêmes leçons que d'autres organisations, c'est-à-dire... L'une des principales constatations du rapport de la vérificatrice générale tient au fait que nous avons mis en place des normes et des mesures de sécurité excellentes, mais que celles-ci ne sont pas appliquées de manière uniforme, d'où la grande importance de l'automatisation.

Mme Stephanie Kusie: A-t-on réalisé une analyse comparative internationale?

Mme Catherine Luelo: Pas à ce que je sache, mais je vais demander à mon collègue, qui s'occupe du dossier depuis un peu plus longtemps que moi, si une comparaison internationale a été effectuée. À ma connaissance, il n'y en a pas.

M. Sony Perron: Ce que je sais — peut-être que nos collègues du Centre canadien pour la sécurité pourront nous faire part de leur point de vue sur le sujet —, c'est que le Canada compare souvent ses pratiques avec les normes de cybersécurité adoptées par les États-Unis. Nous effectuons des comparaisons, certes, mais je ne suis pas certain que nous ayons un rapport qui présente une analyse élargie.

M. Rajiv Gupta: Je voudrais ajouter aussi que, lorsque nous évaluons les fournisseurs de services infonuagiques, nous tenons compte des normes comme celles de l'ISO, à l'international, et du FedRAMP, aux États-Unis, ainsi que des rapports SOC 2 de type 2, qui sont exigés dans le cadre du processus d'évaluation. Nous veillons à bien harmoniser nos pratiques avec les normes internationales et américaines dans ce domaine.

Mme Stephanie Kusie: Merci.

Monsieur Hayes, dans l'audit, vous mentionnez qu'une faiblesse en matière de sécurité tient au fait que les clauses de sécurité des contrats sont « imprécises » et non uniformisées. Le Comité permanent des opérations gouvernementales et des prévisions budgétaires a découvert que des entrepreneurs ont été en mesure de commencer à travailler sur le projet avant d'avoir obtenu leur habilitation de sécurité.

S'agit-il du genre de problèmes que vous avez constatés au sein de Services partagés Canada et de Services publics et Approvisionnement Canada?

M. Andrew Hayes: En ce qui concerne les rôles et les responsabilités, nous craignions que le manque de clarté ne soulève des questions quant aux premières personnes devant intervenir et à celles qui doivent gérer les problèmes lorsqu'un événement survient. Nous avons aussi établi que Services partagés Canada et Services publics et Approvisionnement Canada peuvent tous deux améliorer la surveillance et la supervision.

Mme Stephanie Kusie: Pour pousser le sujet un peu plus loin, monsieur Hayes, quelles mesures de sécurité votre bureau a-t-il recommandées pour les contrats relatifs aux TI?

M. Andrew Hayes: Je n'expliquerai pas en détail l'information que nous n'avons pas pu inclure dans le rapport, mais nous avons établi que les mesures de sécurité associées aux exigences de sécurité existantes doivent être totalement mises en œuvre et qu'il faut également effectuer une surveillance continue.

Mme Stephanie Kusie: Dans votre rapport, vous avez aussi recommandé que les « exigences de sécurité » du gouvernement fédéral soient précisées dans les contrats de services infonuagiques. Selon vous, qui devrait assumer cette responsabilité?

M. Andrew Hayes: D'après moi, c'est au Secrétariat du Conseil du Trésor de donner des directives et une orientation stratégique.

Mme Stephanie Kusie: Merci, monsieur Hayes.

Madame Luelo, vous avez dit que moins de 10 % des renseignements du gouvernement sont hébergés dans le nuage à l'heure actuelle. Pensez-vous qu'il faudrait arrêter le transfert des renseignements dans le nuage jusqu'à ce que les recommandations de la vérificatrice générale aient été mises en œuvre?

● (1605)

Mme Catherine Luelo: Je voudrais apporter une précision, il s'agit de 10 % des systèmes et non des données. C'est un peu différent.

Mme Stephanie Kusie: Je suis désolée. Il s'agit de 10 % des systèmes. Toutes mes excuses.

Mme Catherine Luelo: Non, non, ce n'est pas grave, mais la nuance est importante.

Je crois que nous pouvons poursuivre le travail au même rythme. En fait, nous avons déjà pris des mesures énergiques fondées sur les constatations de la vérificatrice générale, comme je l'ai mentionné dans mes observations, et nous allons continuer de renforcer la sécurité au fur et à mesure.

Lorsqu'un nouveau système est mis en production — dans le nuage, par exemple —, il y a toujours une liste d'activités de production qui sert à vérifier que toutes les exigences sont respectées. Nous allons veiller à suivre cette liste de très près pour les migrations vers le nuage afin de nous assurer que nous gérons ce risque.

[*Français*]

Mme Stephanie Kusie: Merci beaucoup.

Merci, monsieur le président.

[*Traduction*]

Le président: Votre temps de parole est épuisé, madame Kusie. Je vous remercie de votre attention.

Madame Bradford, vous avez la parole pour six minutes.

Mme Valerie Bradford (Kitchener-Sud—Hespeler, Lib.): Je vous remercie, monsieur le président.

Je tiens à remercier tous nos témoins. Je crois que c'est aujourd'hui l'une des rares occasions où il y a pratiquement plus de témoins présents que de membres du Comité. Il est bon de voir que la salle est pleine.

Je vais commencer par poser une question à M. Hayes.

Monsieur Hayes, quel est le pourcentage des ministères que vous avez évalués qui présentaient des lacunes dans leurs plans de gestion des événements de sécurité en ce qui a trait à la cybersécurité et aux renseignements personnels hébergés dans l'infonuagique?

M. Andrew Hayes: Nous avons évalué trois ministères. Notre enquête ne concernait pas l'ensemble du gouvernement. Comme il ne s'agit pas d'un échantillon représentatif, les résultats que nous avons obtenus et que nous avons consignés dans notre rapport ne peuvent pas être extrapolés à l'ensemble du gouvernement.

Mme Valerie Bradford: Votre audit a-t-il révélé que des renseignements avaient été compromis?

M. Andrew Hayes: Nous ne nous sommes pas penchés sur ce degré de spécificité. Nous nous sommes principalement intéressés à la vérification de leurs plans et de leur mise en œuvre.

Mme Valerie Bradford: Monsieur Gupta, à mesure que nous passons à des formes de stockage numériques, que fait-on pour assurer la sécurité des données personnelles de la population canadienne?

M. Rajiv Gupta: Nous évaluons en permanence les menaces qui pèsent sur les fournisseurs de services d'infonuagique. Nous fournissons des conseils et des orientations aux fournisseurs de service en infonuagiques, y compris au sein du gouvernement, sur la manière de sécuriser leurs systèmes. Nous observons en continu l'évolution des types de cybermenaces en fonction des nouvelles technologies, et nous veillons à ce que nos renseignements, nos conseils et nos orientations demeurent adéquats.

Nous déployons également des services de cyberdéfense afin de nous assurer que les technologies que nous déployons pour aider le gouvernement prennent réellement compte des nouveaux facteurs de menace que nous observons à partir de sources classifiées et non classifiées. Nous nous assurons également que nos serveurs utilisent les plus récentes technologies disponibles.

Mme Valerie Bradford: Monsieur Thompson, comment le gouvernement fédéral s'assure-t-il que les fournisseurs de services d'infonuagique répondent à ses exigences en matière de sécurité?

M. Paul Thompson: Merci pour cette question, monsieur le président.

Je tiens simplement à souligner que nous avons mis en place un régime d'inspection physique dans le cadre duquel nos employés inspectent les sites des fournisseurs de services infonuagiques et procèdent à des évaluations de sécurité du personnel. Ce sont les deux principales activités que mènent SPAC pour veiller à ce que les fournisseurs de services infonuagiques répondent à nos attentes.

Mme Valerie Bradford: Ma prochaine question s'adresse à M. Gupta, mais Mme Luelo peut également y répondre si elle le souhaite.

Pourquoi le gouvernement passe-t-il d'une stratégie de type « l'infonuagique d'abord » à une stratégie axée sur l'intelligence infonuagique de manière plus générale, et qu'est-ce que cela signifie sur le plan opérationnel?

Mme Catherine Luelo: Permettez-moi de répondre à cette question, puis M. Gupta pourra ajouter quelque chose s'il le souhaite.

La raison principale derrière ce changement de stratégie est que l'utilisation de l'infonuagique nous permet de mettre les choses en place très rapidement. Là où nous pourrions prendre potentiellement des mois pour mettre en place un environnement dans lequel nous pouvons commencer à construire un nouveau système pour les Canadiens ou migrer un nouveau système pour les Canadiens, nous pouvons le faire en quelques heures ou jours dans le système infonuagique, ce qui représente une énorme occasion d'accélérer la prestation de services à la population canadienne.

Il fallait que le gouvernement change de cap, car en fait ASC avait un problème lié au fait que ses centres de données étaient en train de devenir obsolètes. Nous avons donc décidé de commencer à transférer une partie des données de nos centres vers l'infonuagique. Dans le cadre de cette démarche, plusieurs éléments que nous avons appris ont été soulignés dans le rapport de la vérificatrice générale, notamment le fait que notre modélisation des coûts de gestion doit être améliorée. C'est la raison pour laquelle nous avons adopté un modèle davantage centré sur l'infonuagique dans son ensemble. De cette manière, nous comptons réellement appliquer le prisme financier à la migration des données pour déterminer si ce modèle est plus efficace. Pour ce faire, nous prenons compte d'un ensemble de facteurs, tels que la vitesse et les coûts, et nous comparons nos centres de données physiques traditionnels à la technologie infonuagique.

Nous avons donc opéré ce changement de stratégie, et nous continuerons à peaufiner nos méthodes au fur et à mesure. Comme je l'ai indiqué plus tôt, je ne pense pas que nous nous dirigeons dans un monde dans lequel l'ensemble de nos données puisse se trouver dans l'infonuagique. Toutes les grandes organisations à travers le monde sont confrontées aujourd'hui à ce genre de défis.

● (1610)

Mme Valerie Bradford: Merci pour cette réponse. Pour poursuivre dans cet ordre d'idées, comment se comparent les coûts de gestion des services infonuagiques à l'interne par rapport au recours à des fournisseurs tiers?

Mme Catherine Luelo: C'est là le travail que nous entreprenons actuellement. Je vous dirais qu'il n'y a pas de réponse unique. La vitesse a un avantage, mais aussi un coût, et il y a des coûts importants liés à l'achat d'ordinateur auprès d'Amazon Web Services ou de Microsoft Azure par rapport à l'infrastructure que Sony doit mettre en place pour exploiter physiquement une installation comportant des serveurs et d'autres éléments que nous devons héberger dans nos systèmes.

Nous avons transféré certains de nos systèmes dans l'infonuagique afin de pouvoir bénéficier d'exemples concrets concernant les coûts et les avantages d'un environnement entièrement infonuagique par rapport aux centres de données d'entreprise traditionnels. Je dirais que l'hypothèse selon laquelle l'infonuagique est moins coûteuse s'est avérée erronée. Par ailleurs, il est faux d'affirmer que l'on peut obtenir le même degré de souplesse dans un environnement infonuagique dans un centre de données physique. Nous l'avons constaté tout au long de la pandémie et nous avons été en mesure d'utiliser l'infonuagique dématérialisée pour effectuer des avancées très rapides dans certains domaines.

Nous devons trouver un équilibre entre tous ces aspects pour parvenir à une réduction de coûts satisfaisante, car je rappelle qu'il faut du personnel rémunéré pour effectuer le travail autant dans l'environnement infonuagique qu'au sein des centres de données physiques.

Mme Valerie Bradford: Depuis l'adoption du modèle de travail hybride dans la fonction publique, les employés auront besoin d'accéder à leurs données personnelles à distance, quel que soit l'endroit où ils se trouvent. Y a-t-il une grande différence, en ce qui concerne l'accès des employés, entre les centres de données physiques et les centres de données infonuagiques?

Monsieur Perron, souhaitez-vous répondre à cette question?

M. Sony Perron: Merci, monsieur le président. Il s'agit d'une très bonne question.

Nous nous servons de l'infonuagique comme solution commerciale. Mme Luelo a mentionné le terme « hyperscale », qui offre une solution infonuagique. Lorsque cette solution a été certifiée et que nous avons approuvé son utilisation, elle a été intégrée à notre réseau. Le volume d'information, qu'il s'agisse d'un service, d'un programme ou d'une application dans l'infonuagique ou dans un centre de données, passe toujours par notre réseau. Les outils de surveillance fournis par un centre de cybersécurité et les outils de surveillance améliorée dont nous disposons sur les réseaux du gouvernement du Canada s'appliquent toujours à ce que nous appelons la « charge de travail ». Cette charge de travail s'exécute dans l'infonuagique de la même manière que dans le centre de données physique d'une entreprise.

C'est ce qui explique pourquoi les exigences de sécurité, ou l'évaluation effectuée avant d'approuver l'utilisation d'un hyperscale pour fournir ces services [*inaudible*]. La validation des garde-fous et des mesures de contrôle de la sécurité est très importante, car il s'agit d'une option supplémentaire pour l'hébergement des applications. Mme Luelo a très bien expliqué que la souplesse qu'amène la technologie infonuagique, mais nous devons nous assurer que cela se fasse en toute sécurité. Nous ne pouvons pas nous permettre de perdre le niveau de sécurité que nous avons construit autour des centres de données traditionnels [*inaudible*]. Nous devons trouver un moyen d'intégrer l'infonuagique à nos bases de données existantes. Le travail est donc loin d'être fini. Les garde-fous dont nous disposons aujourd'hui vont continuer d'évoluer et de se perfectionner au fil du temps.

Toutefois, le rapport de la vérificatrice générale nous a rappelé un élément important. En effet, saviez-vous que 200 instances de l'infonuagique sont organisées et configurées conformément à ces garde-fous que j'ai mentionnés? Franchement, cela nous a mis la puce à l'oreille. Nous avons chargé notre équipe de vérifier ce point. J'ai été ravi de recevoir un rapport, au printemps dernier, indiquant que nous étions dans une position avantageuse en termes de conformité. Les quelques ministères qui avaient connu des difficultés ont été informés et, avec le soutien du CGCIO, nous avons résolu les problèmes. Néanmoins, la surveillance doit être menée de manière continue. Nous devons toujours nous assurer que le niveau de sécurité est maintenu efficacement.

Voilà pourquoi l'automatisation est un aspect important. Une intervention humaine pour régler cinq cas est une chose; toutefois, lorsque nous en sommes à 200, 400, voire 500 cas, il devient presque impossible d'avoir les yeux sur tout, tout le temps. L'automatisation nous permet de recevoir une alerte si une mesure de sécurité est en train d'être modifiée par un utilisateur du service. Au sein de chaque ministère, seul un petit nombre de personnes possède l'autorisation de modifier les mesures de sécurité. Pour diverses raisons, une personne peut décider, que ce soit de manière volontaire ou par erreur, de modifier l'un des éléments du dispositif de sécurité. Nous devons toujours être en mesure d'être alertés de ce genre d'incidents, afin de pouvoir y remédier en temps utile.

Nos pratiques ne sont pas si différentes de l'époque où nous devions gérer des centres de données. Il s'agit simplement d'une manière différente d'appliquer les mesures de sécurité adéquates.

Le président: Je vous remercie.

Vous avez largement dépassé le temps qui vous était imparti. Vous avez bien fait de ne pas m'interrompre. Les membres du Comité savent bien que, lorsqu'une bonne question est posée, j'aime entendre la réponse.

Je regrette que M. Fragiskatos ne soit pas présent aujourd'hui pour me chronométrer.

En tout cas, c'était une question pertinente, et vous y avez très bien répondu. Merci.

[*Français*]

Madame Sinclair-Desgagné, vous avez la parole pour six minutes.

Mme Nathalie Sinclair-Desgagné (Terrebonne, BQ): Merci beaucoup, monsieur le président.

Je remercie tous les témoins d'être présents aujourd'hui. En effet, c'est important de parler du sujet à l'étude.

Je vais commencer directement par une question à M. Hayes.

Manifestement, le Bureau du vérificateur général sonne l'alarme non seulement en matière de cybersécurité, mais plus encore, puisqu'on sait que la cybersécurité soulève des enjeux de sécurité qui vont au-delà du monde infonuagique.

En fait, vous avez sonné l'alarme sur deux plans. Premièrement, il est question des menaces informatiques, donc des dommages qu'on pourrait subir. Deuxièmement, vous avez souligné un manque potentiel de moyens et d'encadrement qu'on devrait normalement voir du côté du Conseil du Trésor.

Ai-je bien compris votre rapport?

● (1615)

M. Andrew Hayes: Nous avons constaté des lacunes et nous avons fait des recommandations à ce sujet au Conseil du Trésor.

Mme Nathalie Sinclair-Desgagné: C'est parfait, merci.

Je sais que certaines informations n'ont pas été incluses dans le rapport justement parce qu'elles étaient de nature délicate. Bien sûr, on ne veut pas divulguer les failles de notre système à des parties indésirables.

Avez-vous des exemples hypothétiques à donner pour informer le Comité aujourd'hui?

M. Andrew Hayes: Je pense, par exemple, à l'importance de faire des suivis en ce qui concerne les exigences. C'est un exemple d'information que nous n'avons pas inclus dans le rapport, de même que d'autres détails.

Les recommandations que nous avons faites au ministère étaient de faire les choses prévues dans les politiques.

Mme Nathalie Sinclair-Desgagné: De quel ministère parlez-vous, plus précisément?

M. Andrew Hayes: Je parle de Services publics et Approvisionnement Canada.

Mme Nathalie Sinclair-Desgagné: D'après vous, qui doit faire ce suivi?

M. Andrew Hayes: C'est nous qui devons le faire. Il était important pour nous de mettre une note dans notre rapport disant que nous avions fait cette recommandation, pour que nous puissions...

Mme Nathalie Sinclair-Desgagné: Non, excusez-moi. Je parle de la lacune que vous avez soulevée concernant le manque de suivi.

M. Andrew Hayes: Oui. Cela concernait Services publics et Approvisionnement Canada.

Mme Nathalie Sinclair-Desgagné: D'accord, merci.

Je vais maintenant poser une question à Mme Luelo à propos du Conseil du Trésor et du manque d'encadrement qui a été constaté quant aux mesures de sécurité que devraient mettre en place tous les ministères qui veulent stocker de l'information potentiellement délicate dans le nuage.

Lorsque le Bureau du vérificateur général a tiré la sonnette d'alarme, n'avez-vous pas cru bon de ralentir le processus de stockage d'information dans le nuage, en attendant d'avoir suffisamment de mesures de sécurité en place avant de continuer?

[*Traduction*]

Mme Catherine Luelo: Je vous remercie de votre question. En fait, c'est intéressant parce que pendant que le bureau de la vérificatrice générale effectuait son évaluation, beaucoup de travail était en cours. Vous ait présenté quelques éléments. Nous avons mis à jour le Plan de gestion des événements de cybersécurité du gouvernement du Canada, le PGEC GC. Nous avons également mis à jour nos rôles et responsabilités, ainsi que nos orientations politiques concernant les renseignements des Canadiens dans l'infonuagique. Nous arrivons en quelque sorte à destination ensemble, car nous avions déjà entrepris des travaux pour remédier à un grand nombre de problèmes signalés à juste titre dans le rapport de vérification. Nous avions atteint une taille critique et avions mené cette réflexion nous-mêmes.

L'auditrice générale a certes relevé certains problèmes, mais aucun, à mon avis, n'est suffisamment important, en termes d'amélioration des orientations que nous fournissons ou du suivi que nous avons mis en place, pour ralentir nos progrès. Je tiens simplement à rappeler que les progrès que nous effectuons sont très lents si on les compare à d'autres organisations pour lesquelles j'ai travaillé. Nous avançons à un rythme de tortue, mais je considère qu'il s'agit d'un risque gérable.

[*Français*]

Mme Nathalie Sinclair-Desgagné: Alors, si je comprends bien, vous avez continué de stocker de l'information potentiellement délicate dans le nuage.

Vous dites que vous avez tout mis à jour, notamment votre politique. Par la suite, faites-vous un suivi pour vous assurer que la politique est bien appliquée au sein de tous les ministères?

[*Traduction*]

Mme Catherine Luelo: En fait, nous n'en sommes qu'au début du processus. Au début avril, tous les ministères enverront leurs plans annuels sur les services et le numérique. Il serait bon que nous les vérifiions pour nous assurer qu'ils ont appliqué les directives fournies dans leurs plans.

La deuxième chose concerne les grands programmes en cours. J'ai mentionné notre programme de modernisation du versement des prestations. Nous travaillons en étroite collaboration avec ceux qui s'occupent de la mise en place du système. Ils n'ont pas encore mis les données dans l'environnement de production dans le nuage. Je pense que tous les mécanismes de contrôle nécessaires sont en place, mais il est certain, comme l'a dit M. Perron, qu'il est très important d'automatiser tout cela. Lorsqu'il y a des humains qui entrent dans l'équation pour mesurer la conformité, ce n'est pas viable. Nous ferons des vérifications périodiques auprès des ministères et nous poursuivrons le déploiement du programme de gestion des cyberattaques. Nous venons justement d'achever une vérification. Nous en faisons chaque année. Je suis convaincue que nous avons mis en place suffisamment de mesures de contrôle et de vérification. Il y a notamment une liste de contrôle que nous passons en revue quand nous passons en production, qui nous aide à bien gérer les risques.

● (1620)

[*Français*]

Le président: Merci beaucoup.

Monsieur Desjarlais, vous avez la parole pour six minutes.

[*Traduction*]

M. Blake Desjarlais (Edmonton Griesbach, NPD): Merci beaucoup, monsieur le président. Je tiens moi aussi à remercier les témoins d'être présents parmi nous aujourd'hui, et je tiens à remercier le Bureau du vérificateur général de cet audit très important.

Cela suscite bien des questions chez les Canadiens qui influencent la confiance que leur inspirent les mécanismes de sécurité mis en place pour protéger leurs renseignements personnels. Je pense qu'il s'agit là d'une des grandes responsabilités essentielles des gouvernements du monde entier à mesure que nous transformons nos systèmes en systèmes numériques. J'ai beaucoup appris, et je suis sûr que mes collègues aussi, sur le fonctionnement de ces systèmes au sein du gouvernement. J'ai été très surpris d'apprendre qu'il ne s'agissait que de 10 % des systèmes gouvernementaux. D'une certaine manière, nous n'en sommes toujours qu'à l'aube de cette nouvelle ère. J'estime extrêmement important pour nous de bien comprendre ce contexte initial. Je crois qu'il s'agit du premier ou du deuxième audit concernant les renseignements personnels stockés dans le nuage. Je ne suis pas certain qu'il y en ait déjà eu un avant celui-ci. Il s'agit peut-être du premier. Est-ce le premier, monsieur Hayes?

M. Andrew Hayes: C'est le premier que nous réalisons expressément là-dessus.

M. Blake Desjarlais: Merci beaucoup.

Sur bien des choses, nous avons dû rassembler des gens de nombreux ministères différents. Je dirais que souvent, lorsque différents ministères sont chargés de réaliser un grand projet, chacun a du mal à déterminer qui est chargé de faire quoi, surtout en ce qui concerne les aspects dont les autres s'occupent. Étant donné l'ampleur de la tâche quand plusieurs ministères doivent se mobiliser, il y a parfois des choses qui sont négligées. Certains des éléments que la vérificatrice générale a mis en lumière se retrouvent parmi les conclusions énoncées à la section « environnement ». À partir du paragraphe 7.59 jusqu'à la conclusion, il y a des recommandations portant sur l'environnement.

J'ai remarqué, en particulier, bien sûr, que le Conseil du Trésor a pour mandat de veiller à ce que les travaux du gouvernement s'assortissent de plans environnementaux et de développement durable. Il est indiqué, dans le rapport, que le ministère des Travaux publics et des Services n'a pas tenu compte des critères environnementaux dans l'approvisionnement en services infonuagiques de stockage ou de collecte de données.

Je souhaite simplement mieux comprendre le processus. Cet audit date déjà un peu, donc il s'est écoulé du temps depuis. Je pense que le ministère a accepté les conclusions de la vérificatrice générale. Je suppose donc que mes questions s'adressent à M. Thompson.

Dans ce contexte, de quels progrès pouvez-vous témoigner en matière de collaboration entre Services partagés et SPAC en vue d'harmoniser davantage le mode d'approvisionnement en services infonuagiques?

M. Paul Thompson: Merci beaucoup de cette question.

Je suis heureux d'indiquer que nous avons depuis modifié nos modalités de contrat, de sorte qu'à compter de la semaine prochaine, soit à compter du nouvel exercice financier, les arrangements en matière d'approvisionnement en services infonuagiques incluront de nouvelles exigences sur les émissions de gaz à effet de serre. Cela s'appliquera à l'ensemble des contrats d'approvisionnement, y compris pour les services infonuagiques.

Je suis heureux de dire que cette modification entrera en vigueur dès la semaine prochaine, de sorte que toute nouvelle commande subséquente à ces arrangements en matière d'approvisionnement, ou toute nouvelle activité, sera assujettie aux nouvelles exigences relatives aux émissions de gaz à effet de serre.

M. Blake Desjarlais: Si je comprends bien, ces exigences ne s'appliqueront pas aux 14 contrats actuellement en vigueur.

M. Paul Thompson: Elles s'appliqueront à toutes les nouvelles commandes passées en vertu de ces contrats, à toutes les nouvelles activités menées par des fournisseurs préqualifiés pour mener de nouvelles activités dans le cadre des arrangements existants. Ils devront donc se conformer à l'exigence de fournir des attestations sur les émissions de gaz à effet de serre.

M. Blake Desjarlais: La démarche que ces fournisseurs devront faire pour déclarer leurs émissions de gaz à effet de serre... Est-elle conforme ou semblable à la façon dont le gouvernement canadien recueille ce genre de données jusqu'à présent?

● (1625)

M. Paul Thompson: Je vous remercie également de cette question. C'est une bonne question, parce que nous sommes en train de modifier toutes sortes d'outils d'approvisionnement.

En même temps, il y a eu une annonce il y a quelques mois, je crois, sur les exigences générales en matière d'approvisionnement. Ainsi, cette attestation sera obligatoire pour tous les achats de plus de 4,5 millions de dollars; elle se fonde sur les normes reconnues pour le suivi des émissions de gaz à effet de serre et la mise en place d'un plan visant à atteindre la carboneutralité.

M. Blake Desjarlais: Dans la même veine, je crois comprendre que votre ministère a également accepté la recommandation d'envisager l'adoption de modèles comprenant des modalités normalisées. Où en êtes-vous à ce chapitre pour ce genre de contrat?

M. Paul Thompson: Sur ce point également, je suis heureux d'annoncer que nous avons normalisé le libellé des contrats. Un groupe de travail a été créé, comme l'indique le rapport de la vérificatrice générale. Il a été créé pendant l'audit. Nous disposons à présent d'un guichet unique, à toutes fins pratiques, pour travailler avec les ministères et veiller à ce que nous utilisions tous des modalités normalisées. L'équipe de mon collègue Sony Perron et la mienne ont travaillé en étroite collaboration à la création de ces nouveaux outils harmonisés.

M. Blake Desjarlais: Qui surveille actuellement l'impact environnemental des services numériques au sein du gouvernement?

Il vaudrait peut-être mieux poser cette question à Mme Luelo.

Mme Catherine Luelo: Je ne connais pas la réponse à cette question, mais j'enverrai au Comité une meilleure réponse que celle que je pourrais vous donner à brûle-pourpoint.

Je vous remercie. C'est une bonne question.

M. Blake Desjarlais: Merci. Tout document écrit à ce sujet serait également utile.

Mme Catherine Luelo: Oui.

M. Blake Desjarlais: J'aimerais m'adresser aux autres témoins, au sujet de la formation.

J'ai cru comprendre que le...

En fait, cette question s'adresse peut-être encore à la représentante du Conseil du Trésor.

Il y a une formation obligatoire, au sein de la fonction publique, sur les indicateurs environnementaux et de développement durable à déclarer pour évaluer si le gouvernement pollue ou non.

Comment vous assurez-vous que les autres ministères avec lesquels vous travaillez en partenariat se conforment bien à cette obligation de déclaration?

Mme Catherine Luelo: Encore une fois, c'est une excellente question, mais elle n'est pas de mon ressort en tant que dirigeante principale de l'information du Canada. Je vais m'assurer de la transmettre à nos responsables de l'écologisation des opérations gouvernementales, qui auront une très bonne réponse à vous donner à ce sujet.

Je vous remercie.

Le président: Merci beaucoup. Votre temps est écoulé.

Passons au deuxième tour.

Monsieur Kram, vous avez la parole pour cinq minutes.

M. Michael Kram (Regina—Wascana, PCC): Merci, monsieur le président.

Je remercie tous les témoins d'être ici aujourd'hui.

Je commencerai par Mme Luelo, du Conseil du Trésor.

Pourquoi le gouvernement du Canada transfère-t-il ses données et ses systèmes vers le nuage?

Mme Catherine Luelo: Le gouvernement du Canada est en train d'effectuer la migration de ses systèmes et ses données vers le nuage pour deux raisons que j'ai déjà évoquées.

L'une d'elles est la rapidité, l'agilité. Nous avons constaté les difficultés que nous avions à respecter les niveaux de services attendus pour les Canadiens. Nous espérons créer des environnements numériques élastiques et modifiables qui se distinguent de nos anciens systèmes plus monolithiques, si je peux utiliser ce terme.

La deuxième chose, c'est que l'infonuagique nous donne accès à une plateforme adaptée aux outils modernes dont nous avons vraiment besoin pour attirer des talents informatiques au sein du gouvernement. Je déplore souvent, à grands traits, la pénurie de talents informatiques au Canada, mais plus particulièrement au sein du gouvernement du Canada. Si nous voulons attirer de grands talents au sein du gouvernement pour effectuer ce travail essentiel, il nous faut des outils modernes à mettre à la disposition de ces professionnels.

M. Michael Kram: Vous avez d'abord évoqué la rapidité. Parlez-vous ici de rapidité dans la mise en œuvre d'un projet du début à la fin ou de rapidité d'autres points de vue également?

Mme Catherine Luelo: Oui. Il s'agit de la rapidité à laquelle on peut mettre en œuvre de nouveaux projets, mais aussi de la rapidité à laquelle on peut changer de systèmes. Imaginez qu'on lance une nouvelle politique ou un nouveau programme. Il y a des choses exceptionnelles qui ont été réalisées pendant la pandémie de COVID de manière vraiment extraordinaire. Dans une organisation normale, lorsqu'on a une bonne empreinte dans le nuage, on peut agir et construire des choses beaucoup plus vite que dans notre vieil environnement habituel.

Je souligne également qu'il y a un avantage à utiliser les très grandes organisations dont le travail consiste exclusivement à exploiter ce genre d'environnement. Les environnements en infonuagique comportent des avantages en matière de sécurité et de modernité. Je pense que l'objectif est double.

Si l'un de mes collègues souhaite faire un commentaire... mais je pense que j'ai bien résumé la situation.

● (1630)

M. Michael Kram: D'accord.

À la page 15 du rapport, il est écrit qu'il n'y a pas de modèle d'établissement des coûts. Une analyse des coûts et des avantages est-elle effectuée avant chaque projet informatique?

Est-ce qu'on peut dire cela?

Mme Catherine Luelo: Chaque projet fait l'objet d'une analyse des coûts et des avantages. Une partie de cette analyse porte sur le type de services que M. Perron fournit, en infonuagique ou par les centres de données.

Comme nous en sommes au tout début de la transition, au gouvernement du Canada, je dirais que nous n'étions pas pleinement conscients de tous les coûts associés à la migration vers l'infonuagique et que nous avons eu du mal à franchir le pas. Dans certains cas, nous n'avons pas saisi l'occasion pour simplifier et réduire nos plateformes transférées vers le nuage, ce qui coûte plus cher. En outre, nous n'avions pas une bonne idée des coûts d'exploitation et de fonctionnement d'un environnement en infonuagique parce que nous comptions sur Services partagés pour gérer tous les centres de données. Il est très difficile de distinguer ce que coûte le fonctionnement de Statistique Canada par rapport à celui du Secrétariat du Conseil du trésor, du Centre de la sécurité des télécommunications ou d'Innovation, Sciences et Développement économique Canada.

L'un des grands avantages à avoir réalisé une petite partie de ce projet, maintenant, c'est que nous disposons de données tangibles. L'autre avantage de l'infonuagique, c'est que nous pouvons désormais simplifier et réduire les environnements existants. Plus notre consommation diminue, avec un fournisseur de services infonuagiques, plus notre facture diminue. Il y a des avantages de ce type qui se traduiront par des économies de coûts si nous savons en profiter.

M. Michael Kram: Peut-on dire que lorsqu'on fait l'analyse des coûts et des avantages d'un projet, les économies de temps réalisées en amont, pour la mise en place d'un nouveau centre de données, sont prises en compte dans l'analyse?

Est-ce bien le cas?

Mme Catherine Luelo: C'est bien le cas.

M. Michael Kram: Est-ce qu'il peut arriver qu'un projet ait pour seul objectif de migrer des données vers le nuage?

Lorsque le système en place est vieux et dépassé et qu'on cherche à en construire un nouveau à partir de zéro, l'option de l'infonuagique est-elle envisagée?

Mme Catherine Luelo: Il y a deux scénarios envisagés, et je vais demander à mon collègue de Services partagés Canada de compléter ma réponse.

Le premier consiste à déplacer un ancien système vers le nuage. En termes très simples, cela comprend à la fois les fonctions du système et les données sur lesquelles il s'appuie. Le second consiste à mettre en place un tout nouveau système.

Il y a deux raisons pour lesquelles nous choisirions de passer à l'infonuagique. La première serait de nous débarrasser d'un vieux centre de données et de gérer le risque que cela représente. La seconde serait de construire quelque chose de totalement nouveau, comme nous l'avons fait pendant la COVID et nous continuerons de la faire. Il semblait plus logique alors d'utiliser le nuage, parce que nous pouvions mettre en place un environnement, soit un cadre où l'on construit quelque chose, en quelques jours plutôt qu'en quelques mois.

Le président: Votre temps est écoulé, monsieur Kram.

Nous allons maintenant passer à Mme Yip. Vous avez la parole pour cinq minutes, s'il vous plaît.

Mme Jean Yip (Scarborough—Agincourt, Lib.): Quels sont les avantages du stockage numérique de l'information pour la prestation de services aux Canadiens?

Ma question s'adresse à tous.

Mme Catherine Luelo: Si je comprends bien votre question — veuillez m'excuser si ce n'est pas le cas et reposer la question —, les avantages d'une expérience de service numérique pour les Canadiens pourraient probablement être mieux illustrés par le fait qu'il y a des Canadiens qui doivent présenter une demande papier pour renouveler leur passeport, alors qu'ils pourraient le faire dans un format entièrement numérisé, comme nous y aspirons.

Cela permet de gagner en agilité et en rapidité pour la personne qui reçoit le service, et de réduire la quantité de papier et le nombre de formulaires que les fonctionnaires doivent traiter. Il y a également un avantage environnemental à cela, qui me semble évident.

Je ne sais pas si vous voulez ajouter quelque chose, monsieur Perron.

M. Sony Perron: Si vous me permettez d'intervenir, monsieur le président, le numérique n'est pas une option. C'est là où nous hébergeons nos données, qu'elles soient dans un centre de données administré par le gouvernement du Canada ou dans le nuage, ou on peut utiliser une solution intermédiaire. En réalité, une grande partie du travail que nous effectuerons à l'avenir sera hybride. Nous utiliserons les centres de données classiques pour certains aspects de nos activités ou certains processus, et le nuage pour d'autres. Tout cela doit être étroitement interrelié.

L'analyse de rentabilité qui est réalisée au début porte sur la façon d'exploiter au mieux les différentes options d'hébergement qui existent. Comme l'a dit Mme Luelo, l'infonuagique nous offre la possibilité de nous adapter à la demande. En cas de pic de la demande (pensez à la saison des impôts, à la saison des passeports ou à la demande à la frontière), les systèmes peuvent s'adapter à une demande beaucoup plus importante s'ils sont dans le nuage, parce qu'il suffit de demander plus d'espace informatique. En cas de pic, nous payons plus, en cas de baisse, nous payons moins.

Dans un centre de données classique comme celui que je dirige, je dois construire un bloc de serveurs pour être prêt à faire face aux périodes de pointe, ce qui n'est pas forcément rentable. Quand on fait l'analyse de rentabilité, il faut également tenir compte de tout le cycle des programmes et services.

C'est pour cela qu'il faut évaluer quelle est la meilleure option d'hébergement numérique. Parfois, c'est en partie dans le nuage et en partie dans un centre de données. Tout dépend vraiment du type d'activité visé. Mme Luelo vous a donné quelques exemples. Chaque programme a son propre cycle et ses propres exigences.

Les données doivent être hébergées quelque part, et l'application qui traite les données doit être hébergée quelque part aussi, donc chaque fois, nous faisons une analyse de rentabilité.

● (1635)

Mme Jean Yip: Je vous remercie.

Madame Luelo, en réponse à la question de Mme Sinclair-Desgagné, vous avez mentionné que le rythme reste lent. Comment cela se fait-il?

Mme Catherine Luelo: Je crois, tout d'abord, qu'il y a des contraintes financières. Nous essayons de gérer d'abord les systèmes à plus haut risque au sein du gouvernement, soit les grands systèmes complexes. Je pense aux systèmes d'immigration. Je pense systèmes de versement de prestations sociales. Ce ne sont pas des choses que l'on fait rapidement. Il faut prendre le temps de bien les faire, ce qui explique en partie la lenteur du système.

Je dirais également, en m'inspirant de mon expérience du secteur privé pour quelques instants, que nous avons une grande aversion au risque au sein du gouvernement. Je pense qu'il faudrait davantage penser, dans la conversation sur l'espace numérique, au risque qu'il y a à ne pas avancer un peu plus vite et au risque qu'il y a à ne rien faire, si je peux me permettre de le dire candidement.

Il y a un certain rythme propre à la complexité de nos systèmes qui est normal et approprié, puis il y a la lourdeur générale du processus et la lourdeur de l'aversion au risque dans l'espace numérique qu'il serait bon de changer dans notre culture.

Mme Jean Yip: Comment pourrions-nous contourner ces contraintes liées à la culture afin d'accélérer les choses pour suivre le rythme du secteur privé?

Mme Catherine Luelo: C'est une excellente question. Merci.

Je pense que certains comités au sein du gouvernement sont déjà à pied d'œuvre pour voir comment on pourrait supprimer certains de ces obstacles systémiques. Je sens donc que nous réalisons certains progrès, notamment pour ce qui est des compétences et de la prise de décisions. Autant du point de vue des députés que dans une perspective ministérielle, il faut simplement faire le constat que le Canada a pris du retard par rapport au reste du monde en ce qui a trait à l'offre des services gouvernementaux par voie numérique et qu'il nous est impossible de continuer de fonctionner avec les niveaux de ressources humaines actuels.

Selon moi, lorsqu'il est question de renouveler nos politiques et nos programmes — et c'est le conseil que je donne à la ministre que j'ai le privilège d'appuyer dans son travail —, il faut s'interroger sur les moyens à prendre pour assurer une prestation des services axée sur le numérique, ce qui exige notamment de fournir des outils numériques de pointe aux fonctionnaires qui redoublent d'ardeur jour après jour pour servir les Canadiens.

Le président: Merci beaucoup.

[*Français*]

Je cède maintenant la parole à Mme Sinclair-Desgagné pour deux minutes et demie.

Mme Nathalie Sinclair-Desgagné: Merci, monsieur le président.

Lorsqu'il est question d'analyses coûts-avantages, je suis vraiment en terrain connu. J'ai des questions là-dessus.

Premièrement, une vraie analyse coûts-avantages comporte une analyse des risques assez détaillée. Pouvez-vous me confirmer qu'une telle analyse a été réalisée?

Dans l'affirmative, comment se fait-il qu'on ait mis en œuvre des systèmes pour ensuite s'apercevoir qu'ils comportaient des brèches et des lacunes importantes, en fin de compte?

[*Traduction*]

Mme Catherine Luelo: Il va de soi que des évaluations des risques ont été effectuées. Je peux vous l'assurer, et mon collègue de SPC le confirme également.

Il nous est en outre possible d'ajuster la rigueur de ces évaluations des risques dans la transition vers l'infonuagique. Devrions-nous poser des questions différentes? Devrions-nous essayer d'obtenir d'autres renseignements? Les deux principales leçons que nous avons tirées de certaines des conclusions de la vérificatrice générale concernant la mise en œuvre des mesures de sécurité touchent certes l'automatisation et la nécessité de mettre en place un cadre de conformité adéquat.

● (1640)

[*Français*]

Mme Nathalie Sinclair-Desgagné: Vous dites que le gouvernement a une grande aversion au risque et qu'une analyse des risques a donc été faite, mais cela semble contradictoire avec le fait qu'on a trouvé des brèches et des lacunes importantes.

Le coût d'une fermeture totale du système informatique du gouvernement a-t-il été pris en compte dans l'analyse? C'est un des risques auxquels nous nous exposons, en cas de cyberattaques. Si une vraie analyse coûts-avantages a été réalisée, je serais vraiment surprise qu'on ait pris en compte les risques d'une fermeture complète du système et qu'on ait quand même procédé à la mise en place du système de façon automatique et cybernétique, pour m'exprimer ainsi puisque je ne connais pas tellement les termes exacts.

Enfin, tout cela me surprend beaucoup. Il y a là une contradiction et j'aimerais vraiment avoir une réponse claire à ce propos.

Mme Catherine Luelo: Merci beaucoup pour la question.

[*Traduction*]

Si je parle d'aversion au risque, c'est parce qu'il est normal pour les organisations qui veulent se moderniser d'apprendre certaines choses au fil de ce processus, comme nous le faisons actuellement. Je veux surtout éviter que nous fassions marche arrière en affirmant qu'il est préférable de nous arrêter parce qu'une ou deux choses ne se sont pas déroulées comme on l'aurait souhaité. Nous apprenons de ces erreurs pour aller de l'avant en évitant toutefois de procéder d'abord à la transition de nos systèmes principaux comme la Sécurité de la vieillesse, l'assurance-emploi et le Régime de pensions du Canada. Le tour de ces systèmes viendra une fois que nous aurons tiré tous les enseignements nécessaires de notre expérience avec nos systèmes de moindre ampleur qui passent à l'infonuagique.

J'ajouterais que cette éventuelle fermeture de tous les systèmes gouvernementaux que vous évoquez est constamment présente à l'esprit de tous les membres de notre équipe dès qu'il est question de cybersécurité — comme M. Perron l'a d'ailleurs très bien exprimé. L'infonuagique nous permet de bénéficier de toutes les formes de protection qu'offre le Centre canadien pour la cybersécurité. Cet avantage unique pour le gouvernement du Canada me rassure grandement, car je n'avais accès à rien de tel lorsque je travaillais dans le secteur privé.

Ainsi donc, malgré les quelques écueils liés à l'apprentissage, le soutien incroyable du Centre pour la cybersécurité nous permet de compter sur le contrôle correctif dont nous avons besoin.

Le président: Merci beaucoup.

Monsieur Desjarlais, vous avez deux minutes et demie.

M. Blake Desjarlais: Merci, monsieur le président.

Je voudrais d'abord et avant tout parler à Mme Luelo de son témoignage d'aujourd'hui. Vous contribuez à notre travail de façon exceptionnelle. Trop souvent, notre comité n'a pas droit à des réponses aussi franches. C'est pourtant le genre de réponses dont les députés ont besoin pour accomplir leur travail, surtout dans un comité comme celui-ci. Je tiens donc à vous remercier sincèrement pour votre honnêteté, car nous serons ainsi mieux à même de formuler des recommandations pertinentes dans notre rapport.

J'aimerais revenir sur certains éléments que vous avez mentionnés dans vos réponses précédentes. Il y a d'abord la question de la capacité. Il s'agit de parvenir à recruter les talents nécessaires, surtout dans le contexte de la pénurie de compétences qui affecte les services numériques au Canada.

Pouvez-vous me dire ce qu'il en est exactement? Quelle est l'ampleur de cette pénurie? Est-ce qu'elle touche surtout les services informatiques? Que vouliez-vous dire en parlant d'un manque de capacité à ce chapitre?

Mme Catherine Luelo: J'aimerais bien avoir 40 minutes pour vous en parler, mais je serai brève, car je sais que nous disposons de très peu de temps.

Le taux de postes vacants se situe actuellement entre 25 % et 30 % au gouvernement. Soit dit en passant, la situation est à peu près la même partout au Canada. Nous pouvons observer des goulots d'étranglement dans les domaines de la cybersécurité, de l'infonuagique et de l'architecture. Dans certains de ces secteurs, nous devons livrer concurrence aux entreprises de tout le pays.

Nous devons mettre davantage en lumière l'apport de nos spécialistes de la technologie dans la vie des Canadiens. Nous sommes les seuls à accomplir de telles choses. J'ai pour mission de faire le nécessaire pour que les candidats soient beaucoup plus nombreux à venir constater par eux-mêmes les services offerts par les spécialistes gouvernementaux dans la sphère numérique. Il faut d'abord et avant tout que les gens comprennent mieux la complexité du travail accompli par les fonctionnaires et la diversité des tâches qu'ils doivent exécuter. Je dis cela en toute humilité, car j'ai moi-même travaillé pendant 30 ans dans le secteur privé. Je me demandais alors ce que les gens pouvaient bien faire au gouvernement. À mon arrivée, j'ai compris à quel point l'appareil gouvernemental pouvait être compliqué.

Je pense qu'il serait également bon que des employés du gouvernement travaillent dans le secteur privé pour savoir comment les choses se passent lors d'une réunion trimestrielle des actionnaires et connaître quelques-uns des paramètres qui guident les industries et une grande partie de l'effort d'innovation au Canada. C'est vraiment fondamental, non seulement pour le gouvernement du Canada, mais aussi pour le pays dans son ensemble.

● (1645)

M. Blake Desjarlais: Je vais réagir brièvement avant de tenter de vous poser une dernière question.

En fait, je vous inviterais à transmettre par écrit à notre comité aux recommandations pour régler ce problème de capacité. Je pense que c'est une considération importante. Vous n'avez peut-être pas eu droit à 40 minutes, mais vous pourrez nous en dire plus long dans une réponse écrite.

Mme Catherine Luelo: Certainement.

M. Blake Desjarlais: Merci énormément.

Monsieur le président, est-ce que mes deux minutes et demie sont écoulées?

Le président: J'ai bien peur que ce soit le cas, monsieur Desjarlais.

M. Blake Desjarlais: Au moins, j'ai eu droit à une bonne réponse

Le président: Oui, vous avez pu obtenir de nombreuses précisions.

Monsieur McCauley, vous avez la parole pour les cinq prochaines minutes.

M. Kelly McCauley (Edmonton-Ouest, PCC): Merci, monsieur le président.

Je suis tout à fait d'accord avec M. Desjarlais. Il est vraiment rafraîchissant de se présenter dans une salle de comité pour entendre des réponses aussi franches et directes, plutôt que la salade habituelle — pourvu que ça dure.

Messieurs Hayes, Goulet et Lombardi, je tiens à vous remercier pour ce rapport et pour tous les éléments d'information qu'on peut y trouver. Ma première question sera pour vous trois.

Au paragraphe 7.16 du rapport, vous notez que les exigences mises en place pour assurer la sécurité de l'information stockée dans le nuage n'ont pas été suivies. Votre audit ne portait toutefois que sur trois ministères. Ne conviendrait-il pas d'en élargir la portée compte tenu des préoccupations mises au jour en s'intéressant uniquement à ces trois ministères-là?

M. Andrew Hayes: Nos conclusions visaient en partie les responsabilités des organismes centraux, et notamment la surveillance, le contrôle et le soutien à la mise en oeuvre. Je pense que si les organismes centraux parviennent à corriger les faiblesses et à combler les lacunes que nous avons relevées, la mise en oeuvre devrait s'en trouver améliorée.

Nous comptons effectuer le suivi de ce rapport plus tôt que nous le ferions en temps normal étant donné que le processus en est encore à ses premières étapes et qu'il y a beaucoup de travail à faire.

M. Kelly McCauley: Pour ce qui est des organismes centraux... Nous avons pu voir dans d'autres rapports… L'un de vous m'a emprunté l'expression que j'utilise pour demander qui est vraiment responsable. Nous avons déjà entendu des représentants ministériels affirmer que telle ou telle chose n'est pas de leur ressort. On peut dire que tout le monde est un peu responsable, mais ils soutiennent que ce n'est pas à eux de rendre des comptes. Comme nous avons ici sous les yeux un rapport très sérieux qui exige un suivi, il faut savoir quel est le principal ministère responsable qui doit s'assurer que tout le monde suit les règles et les procédures et que les problèmes de sécurité sont pris en charge.

M. Andrew Hayes: Je suis désolé de vous avoir volé votre expression, car je crois bien l'avoir utilisé tout à l'heure.

Des voix: Ha, ha!

M. Andrew Hayes: Je dois dire à ce titre que les ministères ont des comptes à rendre relativement à l'information qui leur est confiée. Les rôles et les responsabilités des organismes centraux sont plutôt évidents. C'est le Conseil du Trésor qui imprime l'orientation stratégique. Si toutefois les rôles et les responsabilités ne sont pas clairement établis, il peut arriver en cas d'incident que cela cause des retards et que certains éléments soient omis. Il en va de même pour les activités permanentes de contrôle et de surveillance. Il faut savoir qui s'occupe de quoi. Si cela n'est pas clairement énoncé, il est possible que personne ne s'en charge

Nous voulons faire valoir que chacun devrait savoir exactement en tout temps de quoi il est responsable.

M. Kelly McCauley: D'accord.

Vous dites ensuite au paragraphe 7.17 que le gouvernement doit prendre des « mesures immédiates ». Qu'entendez-vous par « immédiates » dans le contexte de ce rapport? Nous avons vécu des situations où nous attendions encore les mesures promises neuf ans après le rapport. Qu'est-ce qui est immédiat pour vous? Est-ce un mois, un an, six mois...?

M. Andrew Hayes: Nous sommes satisfaits des dates fixées pour donner suite aux différentes recommandations. À notre point de vue, il s'agit là de délais d'intervention raisonnables. Il est bien sûr question ici d'un domaine où les choses ne cessent d'évoluer très rapidement, ce qui nous oblige à ne jamais relâcher notre vigilance.

On pourrait donc dire qu'une vigilance constante est nécessaire.

M. Kelly McCauley: Je vous remercie. Ce n'est pas un terme que je comptais utiliser; je vous le laisse volontiers.

Madame Luelo, merci pour vos commentaires. Votre nature directe est très appréciée aujourd'hui. Vous avez indiqué que les ministères vous remettent leurs plans en avril. Qui décide si ces plans sont acceptables? Est-ce que c'est vous? Est-ce qu'il arrive que l'on renvoie un plan au ministre ou au sous-ministre en disant qu'il n'est pas acceptable et que l'on doit en soumettre un autre?

Mme Catherine Luelo: Tout à fait. Ces plans font l'objet d'un examen. J'ai des responsables de portefeuille au Bureau du dirigeant principal de l'information qui s'occupent de différentes grappes de ministères. Ils peuvent ainsi examiner les plans, pas uniquement de façon isolée, mais aussi en les comparant avec ceux établis par les collègues d'une même grappe.

M. Kelly McCauley: Y a-t-il une date précise en avril avant laquelle ces plans doivent être remis?

Mme Catherine Luelo: Je crois que c'est le 6 avril, mais il est également possible que ce soit le 3 avril.

M. Kelly McCauley: Une fois que vous aurez reçu ces plans ministériels, serait-il possible d'indiquer au Comité lesquels ont été jugés acceptables?

Mme Catherine Luelo: Je le ferai avec plaisir.

M. Kelly McCauley: Merveilleux.

Je ne sais pas si c'est une question pour Mme Luelo ou pour M. Perron, mais est-ce que quelqu'un peut me dire à quelles entreprises vous faites appel pour l'hébergement infonuagique?

● (1650)

Mme Catherine Luelo: Je vais laisser M. Perron vous répondre à ce sujet. Sauf erreur de ma part, nous avons huit fournisseurs de services, simplement pour l'infonuagique.

Je crois que mon collègue de SPC pourra vous en dire plus long.

M. Kelly McCauley: Peut-être pourriez-vous simplement nous l'indiquer par écrit, monsieur Perron, car j'aimerais bien poser une dernière question.

Vous avez dit que des simulations ont été effectuées. Est-ce que vous avez les résultats ou les conclusions de ces tests?

Mme Catherine Luelo: Nous menons de telles simulations à intervalles réguliers. Il y en a eu deux depuis que je suis au gouvernement. Nous venons à peine terminer la seconde, et je devrais recevoir le rapport au cours des prochaines semaines. Généralement…

M. Kelly McCauley: Est-ce quelque chose que vous pouvez rendre accessible, peut-être pas la version intégrale du rapport, mais possiblement…

Mme Catherine Luelo: Oui, pour autant que cela ne nous expose à aucun risque.

M. Kelly McCauley: Fantastique.

Merci beaucoup.

Le président: Merci.

Monsieur Perron, est-ce que vous allez pouvoir...? M. McCauley a demandé un document ou une réponse.

M. Kelly McCauley: Je voulais juste connaître le nom des entreprises. Je peux trouver l'information dans les comptes publics, si vous ne l'avez pas à portée de la main.

M. Sony Perron: Monsieur le président, je serai ravi de donner suite à cette requête.

Le président: Nous vous en sommes reconnaissants. Je voulais seulement que vous le confirmiez.

Nous passons maintenant à M. Fragiskatos.

Vous avez cinq minutes.

M. Peter Fragiskatos (London-Centre-Nord, Lib.): Merci beaucoup, monsieur le président.

Je remercie tous les témoins de leur présence aujourd'hui.

J'aimerais examiner les choses dans une perspective plus large. De toute évidence, l'une des conclusions principales de ce rapport réside dans l'énoncé suivant: « L'information stockée numériquement, soit sur place dans des centres de données ou dans le nuage, est exposée à des risques de compromission. »

Je comprends l'importance que peuvent avoir les considérations techniques et les menus détails, comme en témoignent les questions posées par M. McCauley depuis le début de la séance et lors de réunions précédentes. Il est important que les députés aillent ainsi au fond des choses. Mais je me mets également à la place des citoyens qui veulent comprendre ce qui se passe et savoir quelles mesures sont prises sans nécessairement connaître tous ces détails. Que fait-on pour régler ce problème fondamental et ainsi donner suite à ce qui m'apparaît être l'une des conclusions les plus importantes de ce rapport?

Je pose la question à quiconque voudra bien y répondre.

M. Sony Perron: Peut-être puis-je commencer.

C'est une affirmation qui est vraie dans le cas du Canada, mais qui l'est également pour le reste de la planète. C'est la simple réalité. Dans un monde numérique, tout est toujours à risque. Nous devons partir de cette prémisse. Sans cela, nous ne ferions pas notre travail.

J'estime que le gouvernement du Canada peut compter sur une infrastructure capable de résister à bien des menaces. Nous avons mis en place un processus permettant d'intervenir lorsqu'un problème a été détecté grâce à des informations préalables ou directement dans notre système. Nous disposons de mécanismes permettant d'isoler le problème, de le contenir, de le traiter et de le régler, mais notre travail n'est jamais terminé. C'est un peu ce que je disais tout à l'heure. Je pense que la mise au point faite par la vérificatrice générale au début du rapport est très importante. Tout est à risque, et nous devons sans cesse confirmer la pertinence de nos mesures de protection et en améliorer l'efficacité.

Je suis persuadé que Mme Luelo et M. Gupta pourraient vous en dire davantage.

M. Peter Fragiskatos: Avant cela, je pense qu'il est important que nous comprenions tous que l'on n'atteindra jamais un niveau de protection de 100 %. C'est non seulement vrai au Canada, mais c'est également ce que constatent d'autres démocraties. Il est futile de s'imaginer qu'un système pourrait être sans faille.

M. Sony Perron: Tout à fait. Je crois que c'est le point de départ de tout le travail que nous accomplissons. Si nous sommes trop sûrs de nous en estimant que nous avons pris toutes les mesures nécessaires et qu'il n'y a plus aucun risque, nous aurons tôt fait d'être surpris parce que les acteurs malveillants font montre d'une grande créativité. C'est là qu'interviennent le Centre de la sécurité des télécommunications et le Centre canadien pour la cybersécurité en lançant l'alerte et en nous fournissant les informations nécessaires pour que nous puissions nous préparer à la prochaine menace qui nous guette.

M. Rajiv Gupta: J'abonde dans le même sens. Je présume que ce commentaire tiré du rapport part du principe que des mesures de sécurité et des dispositions semblables ont été mises en place. Il faut cependant que cela ait bel et bien été fait dans le cadre d'un processus concret de mise en œuvre pour obtenir le résultat souhaité, à savoir la protection du système. Pour pouvoir aller de l'avant, il est crucial que ces contrôles de sécurité efficaces soient effectivement en place.

Je crois que cela a déjà été dit, mais nous continuons d'offrir nos conseils et nos directives pour que chacun puisse bien se protéger contre les menaces. À ma connaissance, nous sommes sans doute le seul pays à avoir des capteurs connectés au nuage et un organisme de sécurité surveillant l'environnement nuagique. Si de telles menaces planent au niveau du nuage, elles existent également pour les informations conservées sur les lieux mêmes. C'est une chose que je voulais signaler. Il est très important que nous le gardions à l'esprit.

M. Peter Fragiskatos: Monsieur Perron, j'aimerais savoir comment nous pouvons soutenir le rythme de ces « acteurs malveillants » dont vous avez parlé?

Quelles approches sont utilisées pour assurer une surveillance constante des nouvelles tactiques et techniques déployées par ceux qui essaient de mettre à mal nos systèmes? Comment pouvons-nous les avoir à l'œil?

● (1655)

M. Sony Perron: Quelqu'un voulait savoir tout à l'heure qui est vraiment responsable. En fait, c'est un effort d'équipe que nous déployons, et il arrive qu'au sein d'une équipe, les responsabilités soient partagées.

C'est toutefois d'abord et avant tout au Centre canadien pour la cybersécurité qu'il incombe de déterminer ce que l'avenir peut nous réserver en termes de nouvelles menaces que nous devons nous préparer à affronter et à mieux voir venir. C'est ainsi que le Centre peut nous aviser de ce qui nous attend — mon organisation et moi — à titre de responsables du bon fonctionnement du système. On nous indique alors les correctifs à apporter en prévision de l'émergence d'un nouveau risque qui n'avait pas été envisagé par le passé. C'est un apport vraiment important, et le tout doit absolument être géré de concert avec nos ressources stratégiques pour optimiser nos interventions.

Nous avons la chance de pouvoir compter sur un tel mécanisme au Canada. Il faut investir sans cesse dans ce système, car nous avons besoin de pratique. C'est une bonne chose de tenir des simulations, mais les événements concrets nous offrent aussi l'occasion de mesurer notre capacité à bien travailler tous ensemble.

M. Peter Fragiskatos: Merci, monsieur Perron.

Notre temps est limité. J'allais poser une question sur la collaboration entre les organismes, pour comprendre où vous vouliez en venir, mais je me contenterai de dire que je pense qu'il y a un bon travail de collaboration et de communication.

Permettez-moi de poser une autre question, qui porte sur les ressources humaines.

Êtes-vous en mesure de recruter les meilleures personnes et les plus brillantes dans la fonction publique pour mener à bien ce travail? Je sais qu'il y a beaucoup d'intérêt chez les jeunes...

Le président: Monsieur Fragiskatos, je vais attendre que l'on vous réponde. Vous avez dépassé le temps prévu, mais je veux que les témoins répondent. Je vais donc leur permettre de le faire.

M. Peter Fragiskatos: Pas de problème.

Dites-moi, êtes-vous capables de trouver des gens?

Mme Catherine Luelo: Nous avons actuellement un poste à pourvoir dans le domaine de la cybersécurité et nous sommes extrêmement satisfaits du nombre de candidatures que nous avons reçues. Le Centre canadien pour la cybersécurité est un employeur de choix. Beaucoup de techniciens veulent y travailler.

Nos difficultés ont à voir avec la capacité d'intégrer les gens dans le système et les exigences relatives à l'autorisation de sécurité, en particulier pour les postes dans le domaine de la cybersécurité. Nous cherchons à améliorer l'efficacité de la politique sur le filtrage de sécurité, qui fait également partie de mon portefeuille, pour voir ce que nous pouvons faire pour éliminer les entraves du système afin d'intégrer de nouveaux fonctionnaires, tout en nous assurant, en particulier dans le secteur de la cybersécurité, que nous ne créons pas de risque relativement à ces nouveaux employés. C'est extrêmement important.

Le président: Merci beaucoup.

Nous entamons maintenant notre troisième série de questions, qui sera probablement la dernière, compte tenu de l'heure, mais tout de même, six membres du Comité poseront des questions.

Monsieur Kram, la parole est à vous.

M. Michael Kram: Merci, monsieur le président.

J'aimerais maintenant revenir aux vérificateurs.

Dans le rapport, il y a une partie intitulée « La promotion de la responsabilité environnementale et du développement durable », qui couvre quelques pages.

Monsieur Hayes, je crois que vous en avez parlé dans votre déclaration préliminaire et j'aimerais que vous m'aidiez à comprendre.

Si j'ai toute une série de dossiers que je veux sauvegarder en ayant recours à un service infonuagique ou à un autre ou à un serveur interne, dans quelle mesure leur incidence sur l'environnement ou leur empreinte carbone diffère-t-elle?

M. Andrew Hayes: Cela dépend du type de services que vous allez obtenir.

Je vais donner un exemple hypothétique. Dans le contexte infonuagique, si l'on prend un service d'analyse de grande puissance, il utilise de l'énergie. Comment l'entreprise qui fournit ce service gère-t-elle l'aspect environnemental du service qu'elle fournit?

Ce que nous demandons, c'est que des renseignements soient fournis au gouvernement, afin qu'il puisse avoir une bonne idée de ce qu'il achète et savoir s'il existe des options préférables sur le plan environnemental. Il s'agit essentiellement pour lui de procéder en toute connaissance de cause.

M. Michael Kram: D'accord.

Je vais peut-être maintenant m'adresser aux représentants du ministère.

J'aimerais lire un extrait du rapport. Au milieu de la page 24, on peut lire ceci: « 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. »

Je me demandais quels renseignements avaient été fournis et quelles étaient les différences d'une option à l'autre.

M. Sony Perron: Monsieur le président, cela ne s'applique qu'à l'établissement de l'accord-cadre infonuagique, pour lequel nous avons huit fournisseurs qualifiés. Nous leur avions demandé au départ, au moment où ils ont été qualifiés — parmi les choses que nous validions — quel était leur engagement en matière d'environnement et s'ils avaient un engagement concernant l'atteinte de la carboneutralité pour 2050. C'est ce que nous avons fait. Nous l'avons inscrit dans les livres pour sept des fournisseurs qui étaient qualifiés à la fin. Ce que nous n'avons pas nécessairement, c'est une attestation, et je pense que nous y travaillons, afin que nous soyons en mesure de montrer les résultats.

Comme l'a fait remarquer l'équipe de la vérificatrice générale, toutes les charges de travail et toutes les applications que nous plaçons dans le nuage ne consomment pas et ne sollicitent pas l'infrastructure de la même manière. Nous devons être en mesure de comparer ce que nous faisons dans le nuage par rapport à ce que nous faisons dans un centre de données d'entreprise. Est-ce que je consomme plus d'énergie et est-ce que je produis plus d'émissions? Quelle sera la différence? C'est quelque chose que nous ne pourrons pas faire sans ajouter une clause dans le contrat et c'est la direction que nous devons prendre. Autrement, si vous me demandez dans cinq ans si nous consommons et produisons moins ou plus selon qu'il s'agit d'un centre de données ou du nuage, je n'aurais pas les données et, franchement, si nous voulons progresser vers ces objectifs, nous devons les avoir.

Nous n'en sommes qu'au début. Ce qui se trouve dans le nuage est vraiment très limité. De nombreux ministères utilisent actuellement le nuage à des fins d'expérimentation et il ne s'agit donc pas d'un système informatique majeur. Certains ministères sont plus avancés que d'autres, mais une grande partie du travail que nous effectuons dans le nuage est vraiment minime. Cette situation va changer à l'avenir et c'est pourquoi nous devons mettre en œuvre ces contrôles.

● (1700)

M. Michael Kram: D'accord.

À la page 22 du rapport, les vérificateurs parlent d'une « occasion ratée ». N'est-ce pas un peu exagéré? Si un pourcentage aussi minime de données et d'applications a été transféré dans le nuage, l'expression « occasion ratée » est-elle un peu forte? Ne serait-il pas plus approprié de parler d'une « occasion possible à l'avenir »?

M. Sony Perron: Eh bien, monsieur le président, je ne peux pas vraiment dire quoi que ce soit sur la décision d'utiliser ces mots ou non. Je dirais que vous avez probablement raison de dire que les possibilités dans l'avenir sont plus importantes que ce que nous avons fait jusqu'à présent et dans le passé, mais si nous ne prenons pas les mesures nécessaires dès maintenant...

Modifier ces clauses et inclure celles-ci signifient que mon équipe — et M. Theophilos en faisait partie — travaille avec les gens de l'industrie pour déterminer comment nous pouvons le faire et demande leur avis sur la façon dont cela pourrait fonctionner. C'est que nous ne voulons pas inventer des exigences et des clauses qui ne fonctionneront pas pour eux, qui ne pourront pas être établies et qui ne pourront pas être respectées à l'avenir. Au cours des derniers mois, nous avons beaucoup travaillé avec SPAC pour nous assurer que les fournisseurs de services infonuagiques nous donnaient leur avis sur la question de savoir si cela fonctionnerait.

C'est pourquoi nous sommes sur le point de publier ces nouvelles pratiques: parce que l'industrie nous a dit que c'était la bonne façon de procéder, qu'elle pouvait se conformer à ces exigences.

Monsieur Theophilos, je ne sais pas si vous voulez ajouter quelque chose.

M. Michael Kram: Je pense que je n'ai plus de temps de toute façon...

M. Sony Perron: D'accord.

Le président: Votre temps est écoulé, monsieur Kram.

Madame Shanahan, vous avez la parole pour cinq minutes.

Mme Brenda Shanahan (Châteauguay—Lacolle, Lib.): Merci beaucoup, monsieur le président.

Je tiens moi aussi à remercier les témoins de leur présence aujourd'hui.

En fait, monsieur Perron, j'ai déjà siégé au Comité permanent des opérations gouvernementales et des prévisions budgétaires et je crois me souvenir d'avoir parlé, en 2016, de Services partagés Canada et du fait qu'il y avait encore des serveurs dans les placards de certains ministères. Ai-je raison?

M. Sony Perron: Monsieur le président, c'est la personne qui m'a précédé qui l'a dit, mais c'est exact.

Mme Brenda Shanahan: Voilà. Nous avons parcouru un long chemin depuis ce temps.

Il est certain que les exigences en matière de prestation de services aux Canadiens et de protection des données contre les menaces internationales et les cybermenaces, ainsi que l'équilibre entre ces exigences et les coûts, sont des facteurs très importants. En ce qui concerne la prestation des services, une chose que j'ai trouvée très intéressante dans le budget de 2023, c'est que nous nous orientons vers des services automatisés, par exemple en permettant aux Canadiens de produire leur déclaration de revenus de manière automatique. Pensez-vous que nous sommes en mesure de fournir ce service?

M. Sony Perron: C'est une question à laquelle l'Agence du revenu du Canada serait mieux en mesure de répondre.

Je dois dire que l'adaptation au numérique est essentielle. De nos jours, si nous voulons fournir des services souples et faire face à la demande dans les périodes de pointe, nous devons utiliser le numérique. Nous devons utiliser la bonne infrastructure. À l'heure actuelle, une grande partie de l'infrastructure de l'Agence du revenu du Canada dépend de ce que nous appelons un « ordinateur central ». C'était ce qu'il y avait de mieux à l'époque où le nuage n'existait pas. Aujourd'hui, le nuage peut apporter le type de capacité informatique élevée et la rapidité que nous ne pouvions avoir qu'avec l'ordinateur central dans le passé. L'ordinateur central est un superordinateur fonctionnant dans un centre de données.

Je pense que le nuage — si nous restons dans le thème de l'audit — nous offre beaucoup plus de possibilités de le faire. Parfois, ce n'est pas seulement avec un grand programme. Pensez à l'Agence du revenu du Canada. Elle a probablement les plus grands programmes qui dépendent de la technologie au sein du gouvernement du Canada. Maintenant, avec le nuage, nous pouvons avoir ce type de rapidité pour quelque chose de bien moins grande envergure, ainsi que... et le travail analytique. Il y a là un grand potentiel.

Sommes-nous en mesure de le faire? Mme Luelo a dit que nous avons beaucoup de défis à relever sur le plan des talents et des multiples priorités au sein du gouvernement du Canada, mais je crois que nous avons fait le travail de base. Il est à espérer que nous aurons moins de serveurs cachés dans les placards.

Ce que je veux éviter, dès le départ, dans le travail que nous effectuons concernant le nuage... Il existe des instances infonuagiques que nous, autour de cette table, ne connaissons pas. Notre organisation doit gérer cela afin de ne pas retomber dans le désordre qui existait dans le passé, en ce qui concerne la présence de centre de données et de serveurs partout. Nous avons fait ce nettoyage. Il reste encore beaucoup de travail à faire. Nous devons être très organisés quant à la manière dont nous utilisons le nuage afin de ne pas créer... Nous tirons parti de l'expertise et nous la créons. Nous sommes organisés. Nous avons des règles communes afin de ne pas nous exposer. Si un incident se produit quelque part, nous savons ce qui est là et nous savons comment reprendre le contrôle afin d'éviter qu'il y ait des dommages et des conséquences.

Il s'agit d'être organisé à l'échelle de l'organisation. Les acteurs présents ici présents sont essentiels pour y parvenir.

● (1705)

Mme Brenda Shanahan: C'est excellent.

Madame Luelo, voulez-vous intervenir?

Mme Catherine Luelo: Je pense que c'est une très bonne question.

Nous n'avons pas le choix. Les Canadiens s'y attendent. Dans tous les autres aspects de leur vie, ils communiquent par voie numérique avec des entreprises partout au Canada.

À mon avis — pour revenir à ce qui disait M. Perron —, nous sommes prêts à relever le défi, mais il nous reste encore beaucoup de chemin à parcourir. Je pense qu'il est question ici de mettre en place les bonnes fondations et de ne pas avoir peur d'avoir appris certaines choses... de continuer, mais de continuer d'une manière plus intelligente et mieux organisée.

Mme Brenda Shanahan: Excellent.

Je vous remercie d'avoir tenu compte de l'analyse des coûts et des avantages. On en a déjà parlé au cours de cette réunion.

J'aimerais que les Canadiens comprennent quelles sont les menaces auxquelles nous faisons face.

Monsieur Gupta, combien de cybermenaces et d'activités malveillantes sont dirigées contre nous au quotidien, selon vous?

M. Rajiv Gupta: La menace contre le gouvernement du Canada est élevée depuis longtemps. Nous parlons toujours des blocages que nous effectuons au gouvernement du Canada. En ce qui a trait aux activités, nous disons qu'il s'agit de quatre à sept milliards de blocages par jour. Il s'agit en grande partie d'activités de reconnaissance et d'autres types de menaces, mais les menaces sont toujours là.

Nous avons également énuméré les évaluations internationales des cybermenaces. La cybercriminalité s'est réellement perfectionnée ces dernières années. Les États-nations sont toujours présents. La Chine, la Russie, l'Iran et la Corée du Nord sont les principaux pays qui nous préoccupent. Non seulement les moyens utilisés par les acteurs malveillants parrainés par des États se sont perfectionnés, mais la cybercriminalité a pris de l'ampleur dans cet espace. Cela s'est avéré très lucratif, je dirais, du point de vue des rançongiciels, par exemple. Cela alimente vraiment la menace dans cet espace.

Il est très important que nous tirions des leçons de ces menaces, ce que nous faisons quotidiennement. Nous sommes [*inaudible*] et nous voyons donc ce qui se passe partout au Canada dans une certaine mesure. Nous travaillons également avec nos partenaires pour nous assurer que nous utilisons tout ce que nous apprennent les menaces pour fournir des avis et des conseils. Nous travaillons avec nos partenaires pour nous assurer que nous formulons les meilleures recommandations et que nous les intégrons dans nos analyses de la sécurité et dans les types de solutions défensives que nous utilisons pour le gouvernement.

Nous ajoutons à cela, bien sûr, ce que nous avons appris grâce à nos activités liées au renseignement électromagnétique. Le CST a la chance de disposer d'un centre pour la cybersécurité et de capacités de renseignement électromagnétique étranger. Il s'agit de suivre les auteurs de cybermenace partout dans le monde et de nous fournir des renseignements que nous pouvons utiliser pour donner des avis et des conseils aux Canadiens.

Le président: Merci beaucoup.

[*Français*]

Madame Sinclair-Desgagnés, vous avez la parole pour deux minutes et demie.

Mme Nathalie Sinclair-Desgagné: Merci, monsieur le président.

On semble ne pas avoir inclus dans le processus un autre aspect d'une analyse coûts-avantages réalisée selon les meilleures pratiques, et c'est préoccupant. Selon le rapport, « 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 ». Normalement, de vraies bonnes analyses coûts-avantages incluent les répercussions environnementales et sociales.

Est-ce que cette recommandation a été prise en compte? À la suite de la publication du rapport, avez-vous commencé à évaluer les répercussions environnementales dans le cadre de contrats avec des compagnies?

M. Sony Perron: Merci pour la question.

Comme je l'ai mentionné un peu plus tôt, Services partagés Canada ainsi que Services publics et Approvisionnement Canada se sont engagés à travailler avec l'industrie pour déterminer quelle est la meilleure façon d'exiger, dans les soumissions qui seront présentées pour des services infonuagiques, l'information nécessaire pour évaluer l'impact environnemental des propositions de services. Les consultations sont terminées et, dans quelques semaines, en avril, les critères seront intégrés dans les véhicules contractuels que nous avons pour les appels d'offres compétitifs.

● (1710)

Mme Nathalie Sinclair-Desgagné: Pouvez-vous nous donner des exemples de critères qui y seront intégrés?

M. Sony Perron: Monsieur Theophilos, avons-nous des détails concernant les critères qui ont été ajoutés?

[*Traduction*]

M. Costas Theophilos (directeur général, Gestion des produits et des services infonuagiques, Services partagés Canada): Je vous remercie de la question.

Pour y répondre directement, cela cadre avec l'engagement du Canada de réduire les émissions de gaz à effet de serre et d'atteindre la carboneutralité...

[*Français*]

Mme Nathalie Sinclair-Desgagné: Je suis désolée de vous interrompre, monsieur Theophilos, mais j'aimerais savoir quels sont les critères, concrètement.

[*Traduction*]

M. Costas Theophilos: En ce qui concerne l'exactitude des renseignements qui sont fournis, des entreprises comme Google rendent publics leurs engagements en matière d'émissions de gaz à effet de serre pour leurs activités. Sept des huit fournisseurs avec lesquels nous traitons concernant l'infonuagique à Services partagés Canada ont atteint ou dépassé ces objectifs. Nous assurons le suivi auprès du huitième.

[*Français*]

Mme Nathalie Sinclair-Desgagné: Pourriez-vous nous faire parvenir la liste des critères qui seront ajoutés aux contrats pour évaluer l'impact environnemental des propositions et, surtout, nous indiquer la date à laquelle seront mis en place ces nouveaux contrats pour lesquels des évaluations environnementales seront réalisées?

M. Sony Perron: En ce qui concerne la deuxième partie de la question, la mise en place de ces contrats se fera au début avril. Donc, nous y sommes.

Pour ce qui est des clauses qui seront ajoutées dans les contrats et dans les appels d'offres, je suis sûr que Services partagés Canada ou Services publics et Approvisionnement Canada seront en mesure de fournir cette information au greffier dans les prochaines semaines.

Mme Nathalie Sinclair-Desgagné: Merci beaucoup.

Le président: Merci beaucoup, madame Sinclair-Desgagné.

[*Traduction*]

Monsieur Desjarlais, vous avez la parole pour deux minutes et demie.

M. Blake Desjarlais: Merci, monsieur le président.

Je crois que c'est notre dernier tour, et je tiens donc à remercier tous les témoins de leur présence aujourd'hui.

Je vous remercie de votre travail. Je pense qu'il est important que les Canadiens comprennent la valeur de l'infrastructure numérique. Vous avez été très patients à notre égard, étant donné que nous ne sommes pas des spécialistes du domaine. Je tiens à vous remercier de participer à cette discussion.

Je voudrais revenir sur la question du renseignement électromagnétique qui a été mentionnée à plusieurs reprises. Un fait qui a été présenté aujourd'hui, si j'ai bien compris, et je ne me souviens plus quel témoin l'a mentionné, c'est que le Canada est le seul pays à utiliser les renseignements électromagnétiques à l'heure actuelle. Est-ce exact?

M. Rajiv Gupta: Non, je dirais que ce n'est pas exact. Je pense qu'on parlait des capteurs au niveau du nuage, ce qui est en quelque sorte notre définition. Nous avons inventé le terme...

Des voix: Ha, ha!

M. Rajiv Gupta: ..., donc c'est probablement facile à dire. En même temps, nous n'avons pas vu le type de capacité analogue chez les partenaires avec lesquels nous travaillons, et c'est pourquoi j'ai des réserves à l'égard d'une telle affirmation.

M. Blake Desjarlais: Je vois. D'accord.

Qu'est-ce que c'est exactement?

M. Rajiv Gupta: Essentiellement, l'une des mesures de sécurité, qui est très importante, est que, lorsqu'un organisme du gouvernement met en œuvre une location infonuagique, nous devons y être intégrés dès le départ afin d'obtenir les données de télémétrie. Nous obtenons une analyse des journaux et d'autres types de données nous permettant de procéder à des analyses dès le début de l'instanciation de cette location infonuagique. Au CST, nous pouvons examiner ces données et détecter les menaces à l'échelle de l'organisation. Cela nous donne une norme commune pour la surveillance du nuage de l'organisation et une visibilité des locations infonuagiques dès le départ.

Les erreurs surviennent souvent au début, lorsque les gens ne savent pas comment configurer leurs locations infonuagiques, alors il est très important que nous soyons intégrés.

M. Blake Desjarlais: Oui, c'est certain. Je peux comprendre à quel point c'est important afin de s'assurer que nous ayons les mesures de sécurité appropriées.

Je crois que vous avez mentionné, en réponse, je pense, à une question de M. Fragiskatos, que la menace qui pèse sur le Canada est grande. Que devrions-nous recommander en vue de réduire cette menace? Quelle est votre principale recommandation à l'intention du Canada afin de maîtriser cette menace? Je pense que c'est quelque chose qui fait peur aux Canadiens.

M. Rajiv Gupta: Pardonnez-moi. Quelle menace est grande?

M. Blake Desjarlais: Je pense que la question de M. Fragiskatos portait sur le risque qui existe au Canada, et vous avez mentionné que la menace qui pèse sur le Canada est assez grande en ce qui a trait à la cybersécurité des renseignements.

M. Rajiv Gupta: Nous avons observé un niveau élevé d'activités de cybermenace visant le gouvernement du Canada. Le risque et les activités sont deux choses différentes. Cela fait plus de dix ans que j'occupe cet emploi, et je peux vous dire que durant cette période nous avons toujours observé un niveau élevé d'activités de cybermenace visant le gouvernement du Canada. Nous représentons une cible intéressante pour de nombreux pays et cybercriminels. Nous avons toujours observé un niveau très élevé d'activités.

M. Blake Desjarlais: Que pouvons-nous faire pour limiter le risque?

M. Rajiv Gupta: Vous savez, nous sommes un pays prospère. Nous avons des choses que d'autres pays souhaitent avoir. Notre pays offre des possibilités aux cybercriminels, et c'est en grande partie la source de leur motivation. En même temps, nous ne voulons pas être une cible facile, alors nous devons intégrer les moyens de défense dont nous disposons pour nous assurer que les cybercriminels ne s'enrichissent pas sur notre dos et que les auteurs de menaces parrainés par un État n'obtiennent pas l'information qu'ils recherchent.

Continuer d'améliorer nos moyens de défense constitue sans doute la meilleure chose à faire.

M. Blake Desjarlais: Cela implique des investissements.

M. Rajiv Gupta: Oui, comme nous avons investi dans le passé dans nos services de cyberdéfense.

Le président: Merci beaucoup.

Deux autres députés ont des questions à poser.

Monsieur McCauley, vous avez la parole pour cinq minutes.

● (1715)

M. Kelly McCauley: Merci, monsieur le président.

Monsieur Hayes, je veux revenir à vous. Au paragraphe 7.19, vous mentionnez que vous ne pouvez pas publier certaines constatations « parce que le faire révélerait des vulnérabilités et poserait un risque à la sécurité nationale », ce que je comprends, et vous dites « nous les avons plutôt signalées directement aux ministères ».

Les ministères vous ont-ils donné l'assurance qu'ils vont y donner suite? Aussi, est-ce que ces ministères vous ont informé qu'ils y donnent suite?

M. Andrew Hayes: Oui, les ministères nous ont dit qu'ils vont donner suite à nos recommandations, et nous allons faire un suivi pour nous assurer que c'est le cas. C'est l'une des raisons pour lesquelles nous voulions mentionner cela dans le rapport, c'est-à-dire pour faire preuve de transparence et pour que vous puissiez ainsi nous demander si nous avons fait notre travail.

M. Kelly McCauley: Ont-ils établi un échéancier à cet égard?

M. Andrew Hayes: Compte tenu des recommandations que nous avons formulées, il est important qu'ils y donnent suite immédiatement. À l'heure actuelle, je ne pense pas qu'un échéancier a été établi, mais nous allons vérifier si des mesures ont été prises.

M. Kelly McCauley: Êtes-vous en mesure d'expliquer la nature du problème?

M. Andrew Hayes: Il s'agissait d'un problème de surveillance et de supervision du côté de l'organisme central.

M. Kelly McCauley: D'accord.

L'un de mes collègues à la Chambre avait inscrit une question au Feuilleton à propos des atteintes à la sécurité des données. On a présenté un document de 2 400 pages faisant état d'atteintes à la sécurité des données au sein du gouvernement. C'était en novembre 2021, il y a un an et demi. Certaines de ces atteintes à la sécurité des données pourraient-elles être liées directement aux lacunes que vous avez relevées sur le plan de la sécurité?

M. Andrew Hayes: Je ne suis pas en mesure de le dire. Ce que je peux vous répondre, c'est que nous mettons l'accent dans notre rapport sur la prévention, la détection et l'intervention. Pour être en mesure de faire tout cela, il faut se doter de mesures de contrôle et effectuer la surveillance et la supervision d'une manière efficace. C'est ce qu'il faut faire.

M. Kelly McCauley: D'accord.

Madame Luelo, vous avez mentionné que nous devons investir davantage pour cesser de perdre du terrain. Quelles sommes devons-nous investir? Parlez-vous seulement pour le SCT ou parlez-vous au nom de M. Perron, qui a lui aussi besoin de plus d'argent, ou pour l'ensemble des ministères? Combien?

Mme Catherine Luelo: En ce qui a trait au montant, pour l'ensemble du gouvernement, je pense que nous investissons des sommes considérables, et le principal enjeu est de livrer la marchandise. Il s'agit moins de dépenser davantage que de se concentrer plus sur les projets qui doivent aller de l'avant, d'y consacrer les ressources nécessaires et...

M. Kelly McCauley: Pardonnez-moi. Est-ce que je vous ai bien compris? Je croyais vous avoir entendu dire que nous devons investir davantage pour cesser de perdre du terrain.

Mme Catherine Luelo: Nous devons investir d'une manière plus constante. Le modèle de financement... D'après ce que je comprends — et je ne suis pas du tout une experte en la matière — le gouvernement octroie du financement annuellement ou par programme. Il le fait aussi d'une manière très décentralisée, et c'est ce qui pose problème, je dirais.

Du point de vue des dépenses, pour revenir à ce que M. Gupta a dit, nous devons certes continuer à investir dans la cybersécurité et nous devons investir aussi dans les compétences. Toutes ces dépenses font partie d'une même enveloppe, mais nous n'avons pas établi de prévisions des dépenses, si c'est ce que vous voulez savoir.

M. Kelly McCauley: D'accord.

Permettez-moi de vous poser la question suivante, car le budget principal des dépenses vient d'être publié: les sommes prévues dans ce budget sont-elles suffisantes à vos yeux compte tenu du travail que nous devons effectuer?

M. Rajiv Gupta: Du point de vue du Centre pour la cybersécurité, le budget de 2022 a fourni des sommes considérables au CST.

M. Kelly McCauley: Des sommes suffisantes?

M. Rajiv Gupta: Du point de vue de l'infonuagique, une grande partie de la surveillance que nous effectuons est directement proportionnelle à la transition des ministères vers le nuage. À mesure que les ministères migrent vers le nuage, nos besoins vont éventuellement augmenter, mais, actuellement, nous sommes en mesure de surveiller...

M. Kelly McCauley: J'ai une dernière question à poser. Je ne suis pas certain, mais elle concerne peut-être M. Perron.

Cela fait sept ans que les centres de données font l'objet de discussions aux réunions du comité des opérations gouvernementales. Je me souviens de M. Parker qui venait en parler.

Expliquez-moi les choses en des termes simples. Est-ce que nous procédons à la migration de certaines données vers le nuage? Si oui, est-ce que cela permettra aux centres de données de réaliser des économies, ou est-ce qu'on mêle les pommes et les oranges?

M. Sony Perron: Je vous remercie pour cette question, monsieur le président. C'est très compliqué, mais je pense que je peux commencer à répondre.

Lorsque nous fermons d'anciens centres de données et que nous confions letravail à un centre de données d'entreprise, oui, nous réalisons des économies, parce que la taille et l'infrastructure du centre de données d'entreprise nous procurent une plus grande fiabilité et sécurité.

● (1720)

M. Kelly McCauley: En procédant à la migration vers le nuage, est-ce que...?

M. Sony Perron: Habituellement, pour que...

Le président: Donnez-moi un instant, monsieur McCauley.

Vous avez dépassé votre temps de parole. Je vais laisser M. Perron parler, mais si vous l'interrompez, j'aurai à réduire le temps de parole.

Monsieur Perron, je sais que vous avez dit que c'est une réponse compliquée, alors vous avez la parole pour environ 30 secondes.

Je vous remercie.

M. Sony Perron: Nous essayons d'éviter le réhébergement, c'est-à-dire la pratique qui consiste à prendre une charge de travail d'un ancien centre de données et à la déplacer vers le nuage. Il y a, d'une part, un élément de modernisation et, d'autre part, un aspect opérationnel. Je pense, comme mon collègue l'a expliqué un peu plus tôt, que l'analyse de chaque cas dépend de l'effort que nous allons consacrer à la modernisation et de la façon dont nous allons répartir... Je peux vous en dire plus, si cela vous intéresse.

Dans le dernier budget supplémentaire des dépenses (C), nous avons réalisé des économies à SPAC, ce qui a permis de financer son transfert vers Services partagés Canada. Cela s'explique par le fait que nous consommons moins d'espace et que nous fermons d'anciens centres de données. La consolidation permet donc de réaliser des économies, du moins sur le plan de l'infrastructure.

Je vous remercie.

Le président: Merci beaucoup.

Monsieur Sidhu, vous avez le dernier tour de cinq minutes. La parole est à vous, monsieur.

M. Maninder Sidhu: Merci, monsieur le président.

Je remercie les témoins d'être des nôtres aujourd'hui.

Je sais que la cybersécurité est un sujet que le gouvernement prend très au sérieux. De nombreux ministères et ministres sont concernés.

Monsieur Gupta, vous avez dit que nous devions continuer à investir dans la cybersécurité. La cybersécurité est incluse dans la Stratégie pour l'Indo-Pacifique que nous avons récemment annoncée et qui s'élève à 2,3 milliards de dollars. Je ne sais pas si vous pouvez nous éclairer un peu plus... relativement aux alliés ou aux amis qui font du bon travail et qui ont des pratiques exemplaires dont nous pouvons nous inspirer.

Y a-t-il des pays que nous pouvons prendre comme modèles dans le domaine de la cybersécurité?

M. Rajiv Gupta: Il est certain que nous travaillons en étroite collaboration avec nos partenaires du Groupe des cinq. Nous comprenons très bien ce qu'ils font tous.

En même temps, au Centre pour la cybersécurité, nous travaillons avec des alliés du monde entier qui partagent les mêmes idées, et nous faisons de notre mieux pour apprendre de leurs pratiques exemplaires afin de nous assurer d'être à la hauteur. Nous étendrons cette collaboration à la région indo-pacifique afin d'établir de nouveaux alliés et de nouvelles relations là-bas.

M. Maninder Sidhu: Merveilleux.

Y a-t-il des mesures adoptées aux États-Unis, en Australie, au Royaume-Uni, ou dans un de ces autres pays, qui vous semblent remarquables et que nous pourrions, à votre avis, transposer au Canada?

M. Rajiv Gupta: Évidemment, nous échangeons beaucoup de renseignements et nous nous entraidons. C'est très important. Je pense que, du point de vue du gouvernement, nous sommes assez bien placés grâce à la façon dont nous avons construit notre écosystème. Nous continuerons à tirer des leçons dans le domaine des infrastructures critiques au fur et à mesure que nous avancerons. C'est un peu [*inaudible*].

M. Maninder Sidhu: Je vous remercie.

Madame Luelo, vous avez dit qu'il y a environ 800 services hébergés dans le nuage à l'heure actuelle. Vous avez dit qu'il s'agissait d'une toute petite fraction. Combien y a-t-il de programmes à intégrer?

Mme Catherine Luelo: À ce stade-ci, une partie du travail que nous effectuons consiste à en déterminer le bon nombre. Je peux dire que 50 % des applications iront dans le nuage et 50 % resteront dans les centres de données, mais nous n'avons pas encore complètement défini cela. Je pense que c'est une approximation raisonnable. Encore une fois, tous les systèmes ne sont pas égaux.

L'infonuagique offre une certaine souplesse: nous pouvons y transférer des données, puis les retirer lorsque nous n'en avons plus besoin. C'est un peu différent du centre de données traditionnel. Le travail de modélisation financière que nous allons effectuer nous éclairera en partie, car nous voulons être sûrs d'obtenir le meilleur rapport qualité-prix pour les Canadiens.

M. Maninder Sidhu: Je vous remercie.

Pour ce qui est des économies, je sais que, dans une salle de serveurs, l'équipement vieillit, ce qui nécessite plus d'entretien. Je suppose que c'est l'une des raisons pour lesquelles nous nous tournons vers l'infonuagique. C'est pour la longévité et les économies.

Est-ce là votre approche?

Mme Catherine Luelo: Oui, tout à fait. Il n'est pas nécessaire d'acheter, d'installer et de mettre à jour notre propre équipement. C'est la responsabilité du fournisseur de services infonuagiques. Nous nous engageons ainsi sur la voie d'une modernisation sans cesse renouvelée, ce qui est une très bonne chose.

M. Maninder Sidhu: Monsieur le président, combien de temps me reste-t-il?

Le président: Il vous reste deux minutes.

M. Maninder Sidhu: D'accord. Je vais donner un peu de temps à nos témoins, puisque c'est le dernier tour.

Monsieur Perron, on a dû vous interrompre tout à l'heure. Y a-t-il quelque chose que vous voulez souligner avant la fin de notre réunion d'aujourd'hui?

M. Sony Perron: Monsieur le président, pour poursuivre sur la lancée de la dernière question, nous avons quelques cas d'utilisation. Il s'agit d'un travail pionnier en infonuagique. Nous faisons des choses inédites. Nous ne prenons jamais de risque en ce qui concerne la qualité, la sécurité, la confidentialité — les trois étant toujours liées —, mais en matière d'activités opérationnelles, nous expérimentons dans une certaine mesure, et c'est pourquoi il est très important de commencer de façon modeste, notamment pour apprendre avant de passer à l'échelle supérieure.

Nous travaillons avec un de nos clients en fonction des périodes de pointe qui font partie de son cycle de production. Nous construisons une infrastructure, puis, après un certain temps, nous devons la démanteler parce qu'elle n'est plus nécessaire. Nous travaillons donc avec ce client pour chercher à comprendre à quoi ressembleront ses prochaines activités, parce que nous nous appuierons davantage sur l'infonuagique et moins sur l'infrastructure traditionnelle. Nous faisons également l'évaluation des coûts à cet égard.

À l'avenir, nous serons en mesure de répondre un peu plus en détail à ce genre de questions sur le mode de fonctionnement.

De mon point de vue, l'un des avantages de l'infonuagique est la possibilité d'agir rapidement et d'augmenter ou de diminuer l'échelle. Le gouvernement du Canada n'a pas l'obligation de déclasser... On a installé tout cet équipement qui fonctionne depuis un an ou deux. Nous n'avons pas à l'acheter. Ce que nous allons payer, c'est le service.

Bien sûr, il s'agit d'un modèle différent, car nous ne dépenserons pas de capitaux; nous dépenserons plutôt au chapitre des coûts de fonctionnement. Il y aura une déviation passagère de nos dépenses, mais nous n'aurons pas à investir dans l'infrastructure ni dans l'infrastructure installée.

Il existe de nombreuses études de cas où cette approche est judicieuse, mais nous commençons à petite échelle, nous apprenons comment cela fonctionne, nous découvrons les défis à relever et nous nous adaptons. C'est ce modèle qui a porté ses fruits. Je suis très heureux que le CST ait ouvert la voie. Nous avons ainsi appris beaucoup de choses. Cette équipe prend très au sérieux la sécurité; il était donc normal de commencer l'aventure infonuagique avec une organisation qui accorde autant d'attention à la sécurité, parce que nous avions besoin de tirer des leçons. Nous devons nous sentir en sécurité avant de transférer quoi que ce soit d'autre vers le nuage. C'est pourquoi il est très important de commencer par le bon cas d'utilisation.

● (1725)

Mme Catherine Luelo: J'ai une dernière observation à faire. J'espère que le Comité a pu constater aujourd'hui un peu l'esprit d'équipe qui existe au sein du gouvernement dans ce dossier très important. Il faut toute une collectivité pour mettre en œuvre le numérique au gouvernement. Nous sommes en retard; il faut donc accélérer la cadence.

Nous allons apprendre des points que la vérificatrice générale a mis en évidence. Comme nous l'avons dit, nous soutenons ce travail et nous continuerons à tirer des leçons au fur et à mesure que nous avancerons sur cette voie.

J'espère vraiment que s'il y a une chose productive à retenir de la séance d'aujourd'hui, c'est le fait que nous travaillons sur ce dossier dans un esprit collectif.

Le président: Merci beaucoup.

Je n'ai que quelques brèves questions à poser.

Monsieur Gupta, je ne cherche pas une longue explication. Les centres de données sont-ils plus sécuritaires que l'infonuagique en général?

M. Rajiv Gupta: Nous fournissons les contrôles nécessaires pour garantir une sécurité équivalente, mais en même temps, il faut tenir compte du personnel, des compétences, de la disponibilité et peut-être, en partie, de l'échelle que les fournisseurs de services infonuagiques pourraient devoir appliquer au problème. Il s'agit davantage d'une question opérationnelle.

Le président: D'accord. Vous dites donc qu'on peut s'arranger pour qu'ils soient équivalents.

Monsieur Perron, j'ai l'impression que vous préférez le nuage, car il est plus efficace. On peut augmenter ou diminuer son utilisation et on paie pour ce qu'on utilise. Est-ce une évaluation juste?

M. Sony Perron: C'est une évaluation juste.

C'est plus rapide. Si on me demande de mettre en place 25 serveurs, il me faudra des jours ou même des semaines pour les obtenir et les installer. Cela pourrait être fait demain soir si nous utilisions l'infrastructure hyperscaler.

Le président: Vous pensez que cela permet de réaliser des économies de coûts. Est-ce exact? Je ne veux pas vous faire dire ce que vous n'avez pas dit.

M. Sony Perron: Monsieur le président, il n'y a pas d'économies de coûts dans tous les cas.

Il y a des économies si nous adoptons ce que Mme Luelo a décrit comme un modèle ou une approche « intelligente », ou un certain type de… Je pourrais utiliser les mots « charge de travail », car c'est plus facile à décrire que les mots « application de données ». Il est possible de réaliser des économies de coûts, mais il faut procéder à une analyse détaillée avant de se lancer, car il est difficile de revenir sur ses pas. On ne peut pas changer d'avis si on construit un centre de données. Si on souhaite amortir l'investissement, il faut être présent pendant un certain temps.

Si nous allons dans le nuage, nous devons aussi apprendre à ne pas rester liés avec un fournisseur donné et rester souples. Mme Luelo a été très directe avec le Comité plus tôt, et je serai donc aussi direct sur ce point. J'ai dit à l'hyperscaler que ces entreprises ne nous ont pas encore donné le bon prix. Si nous nous organisons ensemble comme entreprise et que nous sommes en mesure de nous approvisionner dans le cadre de cette demande consolidée du gouvernement du Canada, nous pourrons obtenir un meilleur prix. Nous n'avons donc pas encore atteint la limite des économies possibles, car nous n'avons pas nécessairement obtenu le meilleur prix jusqu'à présent.

Le président: Je vous remercie.

Ma dernière question s'adresse à M. Hayes.

Le rapport me semble suggérer qu'en réalité, le budget n'a pas été adéquatement établi. Je vais vous donner la chance de formuler un dernier commentaire à ce sujet, juste pour expliquer un peu, car vous n'avez pas eu beaucoup de questions à ce sujet. Je suis curieux d'entendre votre réponse, car il semble qu'il s'agit d'une grande entreprise composée de nombreux ministères différents qui travaillent ensemble.

M. Andrew Hayes: Je vous remercie beaucoup. C'est un point important que je voulais souligner si j'en avais l'occasion.

Ce que nous voulions vraiment accomplir avec la recommandation sur le modèle de prévision des coûts ou le cadre de financement, c'était de permettre aux ministères qui intègrent le nuage de voir non seulement les coûts à court terme, mais aussi les coûts à moyen et long terme, parce qu'un grand ministère peut absorber les coûts supplémentaires que pourraient entraîner la nécessité d'augmenter les compétences, les outils ou la surveillance, mais c'est beaucoup plus difficile pour les plus petits ministères. Ils doivent parfois réaffecter des fonds provenant d'ailleurs, ce qui met en péril d'autres programmes ou même la sécurité.

Il s'agit là d'un élément important de l'analyse coûts-avantages. Lorsqu'on ne connaît pas les coûts à court, moyen et long terme, on ne peut pas se faire une idée précise de la situation. Je pense que nous sommes tous d'accord sur l'importance de ce point, et cela permettra de cerner les éléments qui devraient être transférés dans le nuage et ceux qui ne devraient pas l'être.

● (1730)

Le président: Je vous remercie beaucoup.

Je vais maintenant permettre à tous les témoins de partir. Je vous remercie d'être venus aujourd'hui.

La séance est levée.

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la Loi sur le droit d'auteur. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre des communes.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante : https://www.noscommunes.ca

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the Copyright Act. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the Copyright Act.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: https://www.ourcommons.ca