Non classifié

Audit du réseau étendu – Planification de la capacité et de la disponibilité

27 mai 2022

Bureau de la vérification et de l’évaluation

TABLE DES MATIÈRES

Contenu

Résumé exécutif

L'un des facteurs essentiels pour le gouvernement du Canada (GC), selon le *Plan stratégique des opérations numériques de 2018 à 2022*, est de construire un réseau fiable qui est disponible en tout temps, de n'importe où, à partir de n'importe quel appareil, et qui évolue en fonction des besoins changeants. Le réseau étendu (RE) est une composante essentielle de ce *plan.* Services partagés Canada (SPC) gère les services du RE du gouvernement du Canada qui permet la connectivité entre les principaux centres de données et les édifices fédéraux. Le RE du gouvernement du Canada est le conduit qui permet aux fonctionnaires de se connecter aux applications opérationnelles qui sont essentielles à la prestation de programmes et de services aux Canadiens et Canadiennes.

L'objectif de cet audit visait à certifier que des processus efficaces étaient en place pour gérer la capacité et la disponibilité du RE, conformément aux instruments de politique du Conseil du Trésor et aux priorités de SPC.

Voici les constations générales :

- la haute direction, dirigée par le Conseil exécutif de surveillance (CES) et d'autres comités de gouvernance, exerçait la surveillance nécessaire pour assurer la conformité aux objectifs stratégiques signalés dans les instruments de politique du Conseil du Trésor et les priorités de SPC;

- des indicateurs de rendement clés étaient utilisés pour suivre l'avancement des services du RE. La grande majorité des normes de service pour la disponibilité des services de RE étaient respectées, avec une disponibilité de 99,965 % en octobre 2020, dépassant la norme de service établie par la direction de 99,15 %;

- les contrats de services gérés du RE faisaient l'objet d'une surveillance suffisante pour s'assurer que les services soient fournis conformément aux modalités de leurs contrats et de leurs accords de niveau de service respectifs. Les rapports des fournisseurs étaient examinés tous les mois et des crédits de service étaient demandés lorsque cela était justifié;

- SPC tenait des registres des risques distincts pour surveiller les risques liés au RE aux niveaux du projet, de la direction générale et des opérations. L'équipement du RE n'avait pas fait régulièrement l'objet d'un balayage, ce qui limitait l'identification des risques opérationnels;

- la Direction générale des réseaux, de la sécurité et des services numériques (DGRSSN) disposait d'une ébauche de plan des ressources humaines (RH) pour 2020-2021. La planification de la relève, qui comprend le partage des connaissances, la documentation et le jumelage avec un agent expérimenté, était limitée et pourrait ne pas combler l'écart découlant du nombre d'employés qui devraient prendre leur retraite dans un proche avenir. La Direction générale n'avait pas entrepris d'analyse pour déterminer les lacunes entre les compétences disponibles et les compétences nécessaires pour appuyer les services de RE;

- le processus de planification de la capacité des services de RE n'avait pas été documenté et n'incluait pas l'utilisation du RE et les mesures des tendances, l'intégration opérationnelle et les

commentaires des partenaires, pour gérer efficacement la capacité disponible et pour prévoir la croissance des services de RE;

- les plans de continuité des activités (PCA) n'avaient pas été mis à jour et à l'essai de façon uniforme conformément à la Directive sur la gestion de la sécurité du Conseil du Trésor. Les plans de continuité de TI inclus dans les PCA étaient incomplets et les procédures opérationnelle normalisées (PON) n'avaient pas été établies pour tous les services de RE. On se fiait aux systèmes de reprise automatisés des fournisseurs pour faire face aux interruptions de service;
- aucun programme rigoureux de mise à l'essai des services de RE n'était en place. Des évaluations de la vulnérabilité, des essais de capacité et de disponibilité et des essais marginaux ont été effectués dans un laboratoire avant la mise en œuvre, pour les circuits et l'équipement du RE. Des essais supplémentaires après la mise en œuvre n'étaient pas effectués régulièrement;
- le programme de renouvellement de la TI n'avait pas été priorisé adéquatement pour remplacer l'équipement du RE qui avait dépassé sa durée de vie utile et qui ne bénéficiait pas du soutien des fournisseurs;
- il n'y avait pas d'approche uniforme pour évaluer de manière proactive le rendement du service de RE. Il n'y avait pas de données de référence sur le RE du GC, les indicateurs de rendement clés (IRC) variaient d'un fournisseur à l'autre et différentes équipes utilisaient différents outils.

Begonia Lojk

Dirigeante principale de la vérification et de l'évaluation

A. Présentation

1. Contexte

La Politique du Conseil du Trésor (CT) sur les services et le numérique et les instruments de soutien constituent un ensemble intégré de règles qui énoncent la façon dont les organismes du gouvernement du Canada (GC) gèrent la prestation de services, l'information et les données, la technologie de l'information et la cybersécurité à l'ère numérique.

Pour concrétiser sa vision numérique, le gouvernement du Canada a élaboré des normes numériques et publié le *Plan stratégique des opérations numériques de 2018 à 2022*, qui donne la priorité aux besoins des utilisateurs et tire parti des dernières technologies numériques pour offrir des services de grande valeur aux Canadiens et Canadiennes. Pour faire de la transformation numérique une réalité, SPC s'est vu confier une partie importante du plan stratégique des opérations numériques. Dans cette optique, SPC a mis en œuvre SPC 3.0, une approche d'entreprise pour l'ensemble du gouvernement. SPC 3.0 a défini trois priorités, dont l'une est « l'optimisation du réseau et le renforcement de la sécurité ».

L'un des facteurs essentiels du gouvernement du Canada, selon le *Plan stratégique des opérations numériques de 2018 à 2022*, est de construire un réseau fiable qui est disponible en tout temps, de n'importe où, à partir de n'importe quel appareil, et qui évolue en fonction des besoins changeants.

Un réseau étendu (RE) est un réseau qui utilise diverses technologies, comme la commutation multiprotocole par étiquette (CME), les réseaux privés virtuels (RPV), le sans-fil (cellulaire) et l'Internet, pour se connecter aux centres de données, aux édifices du GC et à d'autres endroits. Le RE du GC connecte les utilisateurs à partir de sites nationaux et internationaux, tout en prenant en charge les applications opérationnelles pour la transmission simultanée de la voix, des données et de la vidéo. Le RE du GC, par l'entremise d'un RPV, est également le conduit qui permet aux fonctionnaires de se connecter aux applications opérationnelles qui sont essentielles à la prestation de programmes et de services aux Canadiens et Canadiennes. L'annexe B donne un aperçu de la topologie du RE du GC.

SPC assure le fonctionnement des services du RE qui relient plus de 80 services offerts dans 3 500 édifices pour 43 ministères et organismes partenaires (y compris SPC) au Canada et à l'étranger. Les services du RE fonctionnent indépendamment les uns des autres avec des infrastructures de réseau, des normes d'exploitation, des procédures et des mesures de sécurité différentes. Bon nombre de ces réseaux sont vieillissants et certains ne disposent pas de normes de sécurité avancées pour les protéger contre les cybermenaces.

SPC a lancé le projet des services de réseau étendu du gouvernement du Canada (RE du GC) pour remplacer l'ensemble des 18+ contrats actuels par un seul service de réseau national et un service international. Le projet de services de RE du GC visait à améliorer l'efficacité de la façon dont SPC fournit ce service de télécommunications. Les gains d'efficacité comprendront la réduction des coûts de fonctionnement par la convergence, la consolidation et la normalisation des services de RE, ainsi que la réduction des ressources opérationnelles requises pour gérer la prestation de ces services. Ces gains

d'efficacité s'inscrivent dans le mandat de SPC qui consiste à réaliser des économies tout en améliorant les services d'infrastructure de TI.

SPC mesure régulièrement la satisfaction de la clientèle à l'égard de ses services au moyen de l'Initiative de rétroaction sur la satisfaction de la clientèle (IRSC), qui utilise une échelle de 1 à 5. La cote de satisfaction de la clientèle de l'IRSC obtenue pour les services de RE en avril 2021 était de 3,79, ce qui est supérieur à la cible de 3,60 établie par la direction.

En mars 2020, le Canada et le reste du monde étaient au cœur d'une pandémie mondiale (COVID-19) qui se poursuit à la date du présent rapport. Des millions de Canadiens et Canadiennes, y compris la plupart des employés du gouvernement du Canada, ont été obligés de rester à la maison pour contrôler la propagation du virus de la COVID-19. En réponse à ces conditions sanitaires et économiques éprouvantes, le gouvernement fédéral a réagi en mettant en œuvre des programmes d'urgence pour aider les entreprises et les travailleurs mis à pied, à gérer la pandémie mondiale. En tant que facilitateur de TI dans le développement et la mise en œuvre de programmes d'aide aux Canadiens et Canadiennes, les priorités de SPC ont changé immédiatement pour appuyer la réponse du gouvernement du Canada à la COVID-19. SPC a développé une solution approuvée par le Conseil du Trésor pour permettre à plus de 250 000 fonctionnaires fédéraux de continuer à assumer leurs responsabilités tout en travaillant à domicile.

Le réseau du GC a été conçu pour tirer parti des capteurs et du système de surveillance actuels sur le réseau pour assurer une visibilité et une conformité totales de tout le trafic destiné à l'Internet. La capacité de la bande passante n'était pas suffisante pour permettre à tout le personnel du GC de travailler à distance au début de la pandémie. Il a donc fallu mettre en œuvre de nouvelles initiatives et de nouveaux outils en matière de TI pour améliorer la connectivité au réseau et assurer la continuité des opérations essentielles du GC.

Afin d'optimiser la performance du réseau tout en maintenant la sécurité du réseau et des actifs, SPC a mis en œuvre l'initiative de tunnellisation partagée inversée pour rediriger le trafic Internet sélectionné vers des destinations approuvées par le GC. Cette initiative a permis aux utilisateurs à distance d'accéder à un domaine approuvé en utilisant leur accès Internet local tout en réduisant l'utilisation de la bande passante sur le réseau ministériel du GC. SPC a déployé l'outil logiciel collaboratif M365 au sein de 43 ministères et organismes. M365 a amélioré l'environnement de télétravail et soutenu la collaboration continue entre les employés. Ces initiatives ont permis d'assurer la continuité des services aux Canadiens et Canadiennes et de soutenir la santé et la sécurité des fonctionnaires fédéraux.

2. Justification de l'audit

Le RE du gouvernement du Canada (GC) fournit une connectivité d'entreprise au réseau étendu pour les centres de données et les immeubles et emplacements du GC. Il connecte en toute sécurité les utilisateurs et les ordinateurs aux emplacements nationaux et internationaux tout en soutenant les applications opérationnelles permettant la transmission simultanée de la voix, des données et de la vidéo.

La faible bande passante dans les emplacements régionaux et internationaux est l'une des trois principales raisons citées pour expliquer les faibles résultats obtenus dans le cadre de l'Initiative de rétroaction sur la satisfaction de la clientèle (IRSC) de SPC. En outre, à mesure que SPC migre vers les centres de données d'entreprise (CDE), le calcul de haute performance (CHP) et les services infonuagiques, il se peut que la dépendance aux services de RE et la demande pour ces services augmentent. À ce titre, la capacité et la disponibilité des services de RE doivent être soigneusement planifiées et gérées pour s'assurer qu'elles soutiennent la migration vers les CDE, le CHP et les services infonuagiques, et contribuent en fin de compte à atteindre les objectifs de SPC 3.0 et du *Plan stratégique des opérations numériques du GC*.

3. Autorité de l'audit

L'audit figure dans le Plan de vérification axé sur les risques 2019-2022 de SPC, approuvé par le président le 5 mars 2019. Cet audit a été effectué sous l'autorité du Bureau de la vérification et de l'évaluation (BVE).

4. Objectif de l'audit

Le présent audit visait à certifier que des processus efficaces étaient en place pour gérer la *capacité et la disponibilité* du RE, conformément aux politiques du gouvernement du Canada (GC) et aux priorités de SPC.

5. Portée

Cette mission de certification était axée sur la planification de la disponibilité et de la capacité des services de RE et son impact sur les secteurs de services actuels et émergents (par exemple, le calcul de haute performance, les services infonuagiques et les centres de données d'entreprise) ainsi que sur l'architecture d'entreprise. La portée couvre la période du 1er juillet 2019 au 31 octobre 2020, dont une partie reflète l'impact de la pandémie de COVID-19 qui a entraîné le travail à distance des employés du gouvernement au début de mars 2020. La pandémie a provoqué un changement dans les priorités de SPC et a affecté les opérations normales. Le Wi-Fi, les réseaux locaux, les satellites, les appareils mobiles et le projet de services de RE du GC ont été exclus de la portée.

6. Méthode

L'audit a été mené conformément aux Normes internationales pour les missions d'audit interne de l'Institut des auditeurs internes et à la Politique sur l'audit interne du Conseil du Trésor du Canada. Les procédures d'audit suivantes ont été menées :

Procédures d'audit

1. entrevues auprès de la haute direction et du personnel opérationnel;
2. examens de documents;
3. revue générale des systèmes, processus et procédures clés;
4. détermination des contrôles clés;
5. sollicitation de commentaires auprès d'un échantillon de dirigeants principaux de l'information (DPI) de ministères partenaires concernant les opérations du RE soutenant leurs secteurs d'activité;
6. sélection d'un échantillon de contrats de services de RE gérés par les fournisseurs pour s'assurer du suivi des contrats et de la prestation de services conforme aux modalités du contrat;
7. vérification des contrôles.

7. Énoncé de conformité

Selon mon jugement professionnel en tant que dirigeant principal de la vérification, des procédures d'audit appropriées ont été suivies et des éléments probants ont été recueillis pour confirmer l'exactitude de l'opinion formulée dans le présent rapport. Cette opinion est fondée sur une comparaison effectuée entre les conditions en vigueur au moment de l'audit et les critères préétablis d'audit ayant été convenus avec la gestion. Elle ne s'applique qu'à l'organisation examinée. La mission été réalisée conformément aux exigences de la Politique sur l'audit interne, à la directive connexe, aux Normes relatives à l'audit interne au sein du gouvernement du Canada et au Code d'éthique de l'Institut des auditeurs internes. Les éléments de preuve ont été recueillis en conformité avec les procédures et les pratiques qui satisfont aux normes d'audit et corroborés par les résultats du programme d'assurance de la qualité et d'amélioration du Bureau de la vérification et de l'évaluation de SPC. Les preuves recueillies étaient suffisantes pour fournir à la haute direction une preuve d'opinion fondée sur l'audit interne.

B. Constatations, recommandations et réponses de la direction

1. Gouvernance

1.1 Surveillance

Critère d'audit : SPC veille à ce que les services de RE s'harmonisent avec les objectifs stratégiques définis dans la *Politique et la Directive du Conseil du Trésor (CT) sur les services et le numérique*, le *Plan stratégique des opérations numériques du Secrétariat du Conseil du Trésor (SCT)* et SPC 3.0.

L'équipe d'audit s'attendait à ce qu'il y ait une surveillance efficace et efficiente pour veiller à ce que les services de RE s'harmonisent aux objectifs stratégiques définis dans la *Politique et la Directive du CT sur les services et le numérique, le Plan stratégique des opérations numériques du SCT* et SPC 3.0. Cela comprend l'élaboration et la mise en œuvre d'indicateurs de rendement clés (IRC) qui permettent de suivre les progrès réalisés dans l'atteinte de ces buts et objectifs.

L'équipe d'audit a constaté ce qui suit :

- le RE du gouvernement du Canada (GC) et les initiatives de réseau connexes conformes à SPC 3.0 et à la vision numérique du GC figuraient dans le plan triennal de TI approuvé par SPC pour 2019-2022;
- les services de RE faisaient l'objet de discussions régulières au sein des comités de la haute direction, notamment le Conseil d'examen de l'architecture de service (CEAS) et le Conseil exécutif de surveillance (CES) de SPC. Pendant la pandémie, la Direction générale des services de réseaux et de sécurité (DGSRS) a fait le point aux membres du CES sur les initiatives de tunnellisation partagée inversée et M365, les améliorations à l'accès à distance sécurisé, ainsi que sur la capacité du réseau, l'utilisation de la bande passante et les risques connexes;
- on avait également discuté des initiatives en matière de TI au Conseil d'examen de l'architecture intégrée (CEAI) du gouvernement du Canada, coprésidé par le dirigeant principal de la technologie (DPT) de SPC et le dirigeant principal de l'information (DPI) du gouvernement du Canada. Pour faciliter le suivi des progrès et assurer l'harmonisation avec les instruments de politique du CT et SPC 3.0, SPC a mis à jour le Cadre ministériel des résultats (CMR) avec des IRC révisés qui portent sur les télécommunications et les opérations de réseau, y compris les services de RE. La DGSRS a commencé à faire le point, tous les mois, sur les IRC du RE du GC à la Direction générale de la stratégie et de la mobilisation (DGSM) dans le cadre de l'exercice de synthèse du CMR.

En conclusion, il y avait une surveillance suffisante pour veiller à ce que les services de RE s'harmonisent avec les objectifs stratégiques définis dans la *Politique et la Directive du Conseil du Trésor sur les services et le numérique*, le *Plan stratégique des opérations numériques du Secrétariat du Conseil du Trésor* et SPC 3.0.

2. Risques

2.1 Gestion des risques

Critère d'audit : La Direction générale des réseaux, de la sécurité et des services numériques a élaboré et mis en œuvre un registre des risques qui détermine les risques, le niveau de risque, la responsabilité du risque et la réponse au risque, pour les services de RE.

L'équipe d'audit s'attendait à trouver un registre des risques complet et centralisé, incluant les risques liés aux services de RE. Nous nous attendions également à trouver de la documentation décrivant le processus de gestion des risques, y compris la participation des intervenants et leurs contributions au registre des risques.

L'équipe d'audit a trouvé plusieurs documents du Ministère et de la Direction générale détaillant les risques qui pourraient avoir une incidence sur les services de RE. Cela comprenait un exercice de classement des risques à l'échelle de SPC (novembre 2018) réalisé par le Comité de mesure du rendement et de l'évaluation (CMRE) qui a permis de cerner huit (8) risques pour le Ministère, notamment le vieillissement des systèmes de TI et la gestion des RH.

Les risques liés au vieillissement des systèmes de TI et à la capacité des RH avaient déjà été relevés dans le plan triennal (2019-2022) de TI de SPC et dans la version provisoire du plan d'activités (2020-2021) de la Direction générale des réseaux, de la sécurité et des services numériques (DGRSSN). L'évaluation des risques menée par l'équipe d'audit a également démontré que la capacité des RH et le vieillissement des systèmes et de l'équipement de TI constituaient des risques élevés susceptibles de nuire à la prestation des services de RE. Ces risques sont examinés plus en détail dans les critères d'audit 3.1 et 3.3, respectivement.

L'équipe d'audit a trouvé des registres de risques complets au niveau du projet (c'est-à-dire le projet de RE du GC) qui contenaient des éléments clés y compris l'identification, la description, les répercussions, la probabilité, le classement, les responsabilités, le plan d'atténuation et l'état des risques. L'équipe d'audit a trouvé un registre des risques au niveau de la direction générale. Il manquait des éléments clés dans ce registre des risques, notamment les répercussions, la probabilité, le classement et l'état des risques. L'équipe d'audit a également trouvé un registre des risques au niveau opérationnel. Ce registre des risques ne comprenait pas la description des répercussions des risques.

L'une des principales méthodes d'identification des risques opérationnels consiste à balayer l'équipement du RE pour détecter les risques potentiels, comme les vulnérabilités relatives à la sécurité ou les configurations inadéquates. L'équipe d'audit a constaté que le balayage du réseau était limité. Les responsables de la Direction générale du dirigeant principal de la technologie (DGDPT) ont mentionné que certains partenaires n'autorisaient pas SPC à balayer certains appareils de réseau, et que certaines marques d'appareils de réseau ne pouvaient pas être balayées avec les outils existants. Cette situation a limité les capacités d'identification des risques pour les services de RE. Il est à noter que le projet de Gestion de la vulnérabilité et de la conformité organisationnelle (GVCO), qui en était à la phase initiale,

devait s'attaquer aux limites du balayage de l'équipement du RE une fois qu'il serait pleinement opérationnel.

En l'absence d'un registre complet des risques, notamment la criticité des risques, les mesures d'atténuation, la responsabilité et la surveillance de l'état des risques, les risques urgents risquent d'être mis de côté. Cela pourrait avoir des répercussions négatives sur les opérations de réseautage, y compris les services de RE. L'absence de balayage des appareils de réseau a restreint la capacité de SPC à cerner les vulnérabilités liées aux services de RE et à maintenir une posture de sécurité ministérielle à un niveau correspondant à son mandat et à ses exigences opérationnelles.

En conclusion, SPC tenait des registres des risques pour surveiller les risques liés au RE aux niveaux du projet, de la direction générale et des opérations. Ces registres n'étaient pas intégrés, ce qui limitait la capacité de la direction d'élaborer des stratégies d'atténuation des risques et de surveiller leur efficacité.

L'équipement du RE n'a pas fait régulièrement l'objet d'un balayage, ce qui limitait l'identification des risques opérationnels.

Recommandation 1	**Priorité**	**Modérée**
Le sous-ministre adjoint de la Direction générale des services de réseaux et de sécurité devrait élaborer un registre complet des risques pour y consigner les attributs des risques et suivre l'évolution des risques liés au réseau étendu.		
Réponse de la direction		
La direction est d'accord avec la recommandation. Actuellement, les risques de la direction générale qui font aussi un suivi des risques liés aux services de RE sont contrôlés dans plusieurs endroits dans l'ensemble du Ministère, en fonction du contenu : • Registre des risques de la direction générale • Registre des risques opérationnels de TI • Registre des risques du projet et cahiers d'information À mesure que le Ministère évolue vers une organisation fondée sur l'entreprise qui est plus intégrée, il serait bénéfique d'explorer l'utilisation d'un outil existant en vue de créer une approche normalisée pour l'enregistrement et le suivi des risques, étant donné que cela a été un problème relevé dans plusieurs audits récents.		

Recommandation 2	**Priorité**	**Modérée**
Le sous-ministre adjoint de la Direction générale des services de réseaux et de sécurité devrait aborder les limitations au balayage et effectuer régulièrement le balayage des appareils de réseau gérés par SPC afin de cerner les risques opérationnels potentiels.		
Réponse de la direction		
La direction est d'accord avec la recommandation. Le projet de Gestion de la vulnérabilité et de la conformité organisationnelle (GVCO) a été clôturé le 31 mars 2021 et est désormais en phase opérationnelle. Cela permettra une détection continue des vulnérabilités qui comprend une capacité de journalisation et d'audit. La solution fournira des rapports sur les cyber vulnérabilités en temps opportun, abordera les limitations au niveau du balayage ainsi que la capacité d'évaluer la conformité et de répondre aux exigences d'audit par la mise en œuvre de services de gestion des vulnérabilités (SGV) et de services de gestion de la conformité (SGC). Il convient toutefois de noter que nous ne pouvons pas imposer le balayage de l'équipement appartenant à un partenaire. En janvier 2022, la GVCO a mis en place une couverture continue en matière de balayage et de production de rapports d'évaluation des vulnérabilités pour 38 des 43 ministères, ce qui couvre les appareils gérés par SPC. Au cours des deux prochaines années, la GVCO continuera sa progression vers une couverture complète de l'évaluation des vulnérabilités des 43 ministères et atteindra un niveau de maturité permettant une production de rapports plus ciblée pour les appareils de réseau gérés par SPC. Cela permettra de cerner les risques opérationnels potentiels et d'alimenter le registre des risques dès la première recommandation, afin que les vulnérabilités soient traitées.		

3. Contrôles internes

3.1 Planification des ressources humaines

Critère d'audit : La Direction générale des réseaux, de la sécurité et des services numériques a élaboré un plan complet et approuvé de ressources humaines (RH) qui précise les exigences en matière de compétences requises, les plans de relève et la formation afin d'assurer une dotation en personnel appropriée pour la prestation des services de RE du gouvernement du Canada (GC).

L'équipe d'audit s'attendait à trouver un plan complet et approuvé de RH qui préciserait les exigences en matière de compétences, les plans de relève et la formation afin d'assurer une dotation en personnel appropriée pour la prestation des services de RE. Une planification efficace des RH permettrait aux organisations de mieux répondre aux besoins futurs en dotation et d'établir un équilibre entre la disponibilité des ressources et les ensembles de compétences spécialisées.

La capacité des RH a été désignée comme un risque important pour SPC, et comme un risque spécifique pour la prestation de services de réseautage. L'équipe d'audit a constaté que la Direction générale des

réseaux, de la sécurité et des services numériques (DGRSSN) disposait, en février 2020, d'un plan provisoire en matière de RH pour 2020-2021. En raison de la COVID-19, la charge de travail a considérablement augmenté et la formation a été reportée à de nombreuses reprises. La direction avait des inquiétudes quant à l'épuisement et au bien-être général des employés, ce qui pourrait avoir une incidence supplémentaire sur la capacité des RH et sur la prestation de services de RE, en particulier si les parties prenantes s'attendent à ce que les niveaux de service en place pendant la pandémie de COVID-19 soient maintenus sur une base continue.

On estime à 35 % les effectifs de la DGRSSN qui seront admissibles à la retraite au cours des cinq prochaines années. Il y avait des preuves de planification de la relève pour les postes de direction et les personnes interrogées ont déclaré qu'une certaine planification de la relève avait lieu au niveau opérationnel. Les besoins opérationnels ont restreint le temps alloué au jumelage, à la formation croisée et au mentorat, et de nombreux postes essentiels ont une capacité de remplacement limitée. Si le personnel clé devait quitter l'organisation ou être indisponible pendant une période prolongée, SPC pourrait ne pas être en mesure de soutenir certaines fonctions essentielles des services de RE.

Assurer la disponibilité de toutes les compétences requises au sein d'une organisation est un élément essentiel de la planification des RH qui nécessite une analyse approfondie des lacunes en matière de compétences. SPC avait une liste générique de compétences qui avait été élaborée par le Secrétariat du Conseil du Trésor pour la conversion de la classification des CS, mais pas d'un inventaire spécifique des compétences techniques requises pour les services de RE. Sans une analyse adaptée aux besoins de SPC, il sera difficile de déterminer si SPC possède les compétences requises pour soutenir les services de RE.

La Direction générale avait diverses initiatives en matière de RH en cours, y compris un programme de perfectionnement des CS, qui permettaient de s'attaquer à certains problèmes visant les RH notés plus haut. Le Programme de perfectionnement des CS est conçu pour améliorer et uniformiser les aptitudes et les compétences au sein de la communauté de TI à l'échelle de SPC. L'adoption précoce du Programme avait eu lieu au sein de la DGRSSN sur une base limitée, avec 30 personnes au quatrième trimestre de 2019-2020.

Les risques et les problèmes en matière de RH qui sont liés à la capacité, à la planification de la relève et aux lacunes en matière de compétences pourraient mettre en péril la prestation des services de RE et la continuité des opérations. La Direction générale pourrait bénéficier d'un plan complet de RH pour la prestation des services de RE qui comprend :

- la planification de la capacité prenant en compte les répercussions de la COVID-19,
- la planification de la relève qui comprend le partage des connaissances et la formation réciproque,
- un plan de dotation en personnel qui cerne les lacunes en matière de compétences.

En conclusion, la DGRSSN disposait d'une ébauche de plan des ressources humaines (RH) pour 2020-2021. La planification de la relève, qui comprend le partage des connaissances et la documentation, ainsi que le jumelage avec un agent expérimenté, était limitée et pourrait ne pas combler l'écart découlant du nombre d'employés qui devraient prendre leur retraite dans un proche avenir.

Recommandation 3	**Priorité**	**Élevée**
Le sous-ministre adjoint de la Direction générale des services de réseaux et de sécurité devrait élaborer et approuver un plan complet de ressources humaines, conformément aux politiques du Secrétariat du Conseil du Trésor, qui comprend la planification de la relève ainsi qu'un plan de dotation en personnel qui aborde les questions de capacité et tient compte des compétences et de la formation requises pour s'assurer que les besoins en personnel sont satisfaits pour la prestation des services de RE.		
Réponse de la direction		
La direction est d'accord avec la recommandation et continuera de se conformer à toutes les exigences ministérielles en matière de planification des RH et de production de rapports, le tout conformément aux politiques du Secrétariat du Conseil du Trésor. Les gammes de service de RE, de RL, de Wi-Fi et de câblage relèvent toutes des Services de réseau qui bénéficieraient d'un plan de RH intégré, le travail étant effectué à la fois par la Direction des services de réseau (principalement dans la région de la capitale nationale) et la Direction de la prestation des services régionaux (principalement à l'extérieur de la région de la capitale nationale). Les Services de réseau respectent l'ensemble de la planification des RH dans le cadre des processus ministériels, conformément aux politiques du Secrétariat du Conseil du Trésor. Les sections portant sur les ressources humaines des documents de planification du Ministère, y compris les plans d'activités de la direction générale (PADG), sont remplies et approuvées par le sous-ministre adjoint dans le cadre du cycle de planification ministériel. Le PADG 2022-2023 élabore davantage la planification intégrée des ressources humaines et de l'effectif et comprend la planification de l'effectif, le recrutement, la planification de la relève, la gestion des talents, l'apprentissage et le perfectionnement et le mieux-être en milieu de travail. En plus du PADG, les Services de réseau fournissent de l'information pour d'autres activités ministérielles de planification des RH, y compris la planification de la relève officiellement documentée dans le cadre du cycle de gestion du rendement au niveau de la direction; les possibilités de formation dans le cadre de l'exercice d'analyse des besoins en apprentissage; les plans d'atténuation des risques liés aux RH du Ministère; et la planification de la capacité en ce qui a trait aux affectations budgétaires annuelles.		

3.2 Stratégie sur la capacité et la disponibilité du RE

Critère d'audit : La Direction générale des réseaux, de la sécurité et des services numériques dispose d'une stratégie de gestion de la capacité du RE du gouvernement du Canada (GC), y compris des exigences relatives à la réalisation d'évaluations de routine des services de RE en tenant compte de la

disponibilité, de la capacité, de la gestion et de l'engagement des partenaires, et de la planification de la continuité des activités et de la TI.

L'équipe d'audit s'attendait à trouver une stratégie pluriannuelle de gestion de la capacité et de la disponibilité qui comprendrait des objectifs, des plans d'action et des mesures du rendement. La stratégie aurait dû tenir compte de la capacité, des commentaires des partenaires, de la disponibilité, de la planification de la continuité des activités et de la continuité de la TI pour pouvoir fixer des objectifs et les satisfaire.

Nous avons constaté que les responsabilités relatives au soutien de la capacité des services de RE étaient réparties entre les groupes suivants :

- L'équipe de la Planification, ingénierie et services gérés de réseau (PISGR) était chargée de veiller à ce que la Direction générale dispose d'un plan de capacité du RE documenté. L'équipe de la PISGR était également responsable de la gestion du cycle de vie des services, de la planification et de la gestion des services, de l'architecture et de la conception des services, ainsi que de l'ingénierie des services de RE.

- La Direction des opérations des réseaux était responsable de la mise en œuvre et du soutien continu des services de RE et de l'infrastructure connexe, y compris Wi-Fi, câblage, satellite, Internet, réseau de circuits dynamiques (RCD), services fondamentaux et service géré de transfert sécurisé de fichiers (SGTSF), sauf lorsque ces services étaient pleinement impartis.

- L'équipe des Opérations de l'infrastructure des services de police (OISP) était responsable de la gestion des services de RE pour la Gendarmerie royale du Canada (GRC).

L'équipe d'audit n'a pas trouvé de stratégie globale de gestion de la capacité du RE traitant de la planification et des prévisions annuelles des services de RE.

La Direction générale des réseaux, de la sécurité et des services numériques (DGRSSN) avait mis en place un outil de surveillance de la bande passante de l'entreprise, qui regroupait l'information quotidienne sur l'utilisation et le rendement de la bande passante pour les services Internet fournis à l'ensemble des partenaires, et qui fournissait une visibilité de la bande passante au niveau de l'entreprise. Cependant, l'outil se limitait à la bande passante pour les services Internet et il n'était pas clair comment cette information servait à la planification de la capacité à long terme. Aucun processus documenté n'a permis d'établir une méthode de planification et des prévisions pour les services de RE, y compris l'utilisation de la bande passante. La prévision actuelle de la bande passante n'était pas fondée sur les données d'utilisation de la bande passante, les exigences des applications, les demandes opérationnelles (DO), les projets de migration de la charge de travail (MCT) et les besoins de migration vers le nuage. En ce qui concerne une stratégie de disponibilité, l'équipe d'audit a reçu des plans de continuité des activités (PCA) et des plans de gestion des urgences de plusieurs équipes des opérations du RE et a constaté que certains plans étaient incomplets, n'étaient pas examinés ou mis à l'essai régulièrement et n'étaient pas entièrement conformes à la *Directive sur la gestion de la sécurité du Conseil du Trésor*. Les plans ne comportaient pas d'exigences en matière de formation et de sensibilisation. Il n'y avait pas suffisamment

de preuves qu'une analyse des répercussions sur les activités avait été effectuée pour appuyer les PCA. Il n'est pas clair comment tous les PCA et les plans de gestion des urgences étaient interreliés. Ces plans n'étaient ni hiérarchisés ni priorisés. Les PCA comprenaient des éléments de gestion de la continuité de la TI à l'appui des services de RE. Les éléments de la continuité de la TI qui manquaient comprenaient la communication avec les partenaires susceptibles d'être touchés par les perturbations, les mesures visant à respecter les stratégies de rétablissement et les priorités de restauration définies, ainsi que la mise à l'essai régulière des mécanismes de gestion de la continuité de la TI.

L'équipe d'audit a constaté que la Direction générale se fiait aux systèmes de reprise automatisés des fournisseurs pour faire face aux interruptions de service. La DGRSSN a fourni une procédure opérationnelle normalisée (PON) pour l'un des ministères échantillonnés pour cette audit. Des procédures opérationnelles documentées sont essentielles au rétablissement des services essentiels. L'absence de procédures de reprise documentées pose un risque important pour la disponibilité des services de RE et les activités opérationnelles.

L'équipe d'audit a également constaté que les exercices de simulation n'étaient pas effectués régulièrement pour s'assurer que les PCA et les PON étaient à jour et que le personnel savait comment les appliquer. Il convient de noter que, malgré les lacunes relevées dans la planification de la continuité des activités, SPC a fourni une réponse efficace à la pandémie pour les services de RE en mettant en œuvre diverses initiatives, comme la tunnellisation partagée et le logiciel de collaboration M365, pour aider à atténuer les répercussions de la pandémie sur le RE.

En conclusion, il n'y avait pas de stratégie d'ensemble de gestion de la capacité du RE pour les services de RE. Il n'y avait pas de processus documenté qui tenait compte des données d'utilisation de la bande passante, des exigences des applications, des demandes opérationnelles (DO), des projets de migration de la charge de travail (MCT) et des besoins de migration vers le nuage pour la prévision des services de RE. Les PCA n'étaient pas systématiquement mis à jour et à l'essai, les plans de continuité de la TI inclus dans les PCA étaient incomplets et les PON n'avaient pas été établies pour tous les services de RE. Les services de réseau gagneraient à avoir une stratégie de gestion de la capacité et de la disponibilité du RE qui tienne compte des observations notées par l'équipe d'audit, y compris les exigences relatives à la réalisation d'évaluations de routine des services de RE.

Recommandation 4	**Priorité**	**Modérée**
Le sous-ministre adjoint de la Direction générale des services de réseaux et de sécurité devrait élaborer, documenter et mettre en œuvre un processus qui intègre l'utilisation du RE, les mesures des tendances, l'intégration opérationnelle et les commentaires des partenaires dans l'équation de planification pour prévoir la croissance des services de RE d'une année sur l'autre.		
Réponse de la direction		
La direction est d'accord avec la recommandation.		

Les Services de réseaux disposent déjà d'une grande partie de ces renseignements pour les services de RE, comme l'utilisation, les normes et les mesures du RE, et travaillent avec les partenaires afin d'établir des calendriers réalistes pour la prestation des services de RE.

Les Services de réseaux disposent actuellement de divers rapports liés au RE qui sont préparés ou reçus chaque semaine, aux deux semaines, chaque mois, aux deux ans ou de façon ponctuelle. Ces rapports portent notamment sur la croissance, l'utilisation, la réception, la satisfaction de la clientèle, la gestion des contrats, les demandes de service, la prestation de services, la gestion des services, l'état d'avancement des projets, le rendement et la capacité des services, la surveillance, etc. Les équipes continueront de travailler à un processus qui intègre toute cette information dans un modèle prévisionnel.

Dans l'intervalle, nous continuerons d'utiliser les mesures que nous avons et de les communiquer aux clients et aux partenaires, dans la mesure du possible, afin de faciliter le processus de planification.

Recommandation 5	**Priorité**	**Modérée**
Le sous-ministre adjoint de la Direction générale des services de réseaux et de sécurité devrait mettre en œuvre un ensemble commun d'outils pour la collecte de mesures du RE.		
Réponse de la direction		
La direction est d'accord avec la recommandation. Alors que des mesures existent déjà pour les services gérés et qu'il existe divers outils pour recueillir ces mesures, les Services de réseaux élaboreront et mettront en œuvre un ensemble commun d'outils pour recueillir les mesures du RE. Les Services de réseaux sont en train d'élaborer une stratégie visant à établir une approche normalisée pour la mise en œuvre de capacités proactives de surveillance et de gestion de la performance des réseaux dans l'ensemble des réseaux de SPC.		

Recommandation 6	**Priorité**	**Élevée**
Le sous-ministre adjoint de la Direction générale des services de réseaux et de sécurité devrait s'assurer que les plans de continuité des activités sont mis à jour et à l'essai, et que les procédures opérationnelles normalisées et les plans de continuité de la TI sont documentés pour toutes les opérations du RE.		
Réponse de la direction		
La direction est d'accord avec la recommandation.		

Conformément à la *Directive sur la gestion de la continuité des activités de Services partagés Canada*, la Direction générale est responsable de la tenue à jour des plans de continuité des activités (PCA) pour les services et les activités essentiels et clés dont elle est responsable sur le plan de la gestion. La Direction générale des services de réseaux et de sécurité suit les directives de l'équipe de la gestion des urgences et de la planification de la continuité des activités (responsable ministériel des PCA) pour assurer la mise à l'essai régulière de ces processus.

Les PON et les plans de continuité de la TI doivent être examinés et mis à jour pour refléter les effectifs des services de réseaux, qui sont répartis dans l'ensemble du pays.

Les plans de continuité de la TI seront examinés. Dans le contexte des services de RE, la majorité de l'équipement est détenue et gérée par les fournisseurs et les employés de SPC ne gèrent ainsi que l'infrastructure de cet équipement de RE.

La Direction générale des services de réseaux et de sécurité (DGSRS) s'efforcera de mettre ces documents à jour afin de veiller à ce que les opérations du RE continuent d'appuyer les fonctions essentielles à la mission. La DGSRS veillera aussi à ce que les processus et procédures connexes soient bien documentés, testés et compris par les secteurs de services touchés, conformément aux politiques ministérielles.

3.3 Disponibilité du RE

Critère d'audit: La disponibilité du RE de SPC est assurée par la mise en œuvre d'essais rigoureux, d'un programme de renouvellement de la TI et d'un investissement continu pour soutenir l'innovation des services de RE.

L'équipe d'audit s'attendait à trouver un programme rigoureux pour mettre à l'essai l'équipement et les circuits du RE, des technologies novatrices utilisées pour le RE et un programme de renouvellement de la TI.

L'équipe d'audit a constaté que SPC n'avait pas de programme rigoureux de mise à l'essai des services de RE en place. SPC a effectué des évaluations de la vulnérabilité du RE du GC, des essais de capacité et de disponibilité, ainsi que des essais marginaux en laboratoire pour les circuits et l'équipement avant la mise en œuvre. Des essais supplémentaires après la mise en œuvre n'étaient pas effectués régulièrement en raison de difficultés à obtenir les fenêtres d'entretien requises pour les essais auprès des partenaires. L'absence d'essais réguliers augmente les risques de défaillance et pourrait entraîner des problèmes de résilience et de disponibilité du RE. Les méthodes fondées sur les pratiques exemplaires recommandent que les organisations mettent en œuvre un programme de mise à l'essai de l'infrastructure du RE pour assurer la capacité et la disponibilité des services essentiels de RE.

SPC a mis en œuvre un programme de renouvellement de la TI pour identifier et remplacer l'équipement de TI vieillissant afin de réduire les risques opérationnels et liés à la cybersécurité. Les directions générales

étaient responsables de la collecte et de la diffusion des données et du remplacement des biens. Les équipes de soutien des services de RE ont créé une liste, revue chaque année, de l'équipement de TI vieillissant qui n'était plus pris en charge par le fournisseur ou qui ne répondait pas aux exigences technologiques.

La liste des équipements de TI vieillissants pour les services de RE n'avait pas été entièrement priorisée. Le risque n'avait pas été évalué pour tout l'équipement figurant sur la liste. Certains équipements ayant dépassé la fin de leur vie utile ne comprenaient pas de justification du niveau de risque et de l'indicateur de priorité. De nombreux composants du réseau figurant sur la liste n'avaient pas de soutien de fournisseur et avaient dépassé leur durée de vie utile. Sur les 12 923 composants du réseau, 1 790 (14 %) présentaient un risque élevé et n'étaient plus pris en charge par le fournisseur. En l'absence d'un programme de renouvellement de l'équipement de TI qui remplace l'équipement vieillissant avant qu'il n'atteigne la fin de sa vie utile ou la fin du soutien du fournisseur, il y a de fortes chances que l'équipement tombe en panne, ce qui pourrait avoir une incidence sur les services de RE.

La vision et la stratégie en matière de réseau et de sécurité de 2020 décrit plusieurs technologies novatrices que SPC devrait mettre en œuvre pour répondre aux demandes futures du réseau. Cette stratégie vise à accroître l'efficacité opérationnelle, la souplesse, la sécurité et la fiabilité du réseau de SPC dans le but de relever les défis actuels en matière de réseau et de sécurité, tels que les processus de gestion manuelle, les dédoublements des réseaux et les réseaux vieillissants. SPC a désigné le RE défini par logiciel (REDL) comme une technologie novatrice et un élément essentiel pour exploiter un réseau résilient et disponible. Le REDL utilise un logiciel pour contrôler la connectivité, la gestion et les services du réseau, et améliorer la vitesse et la connectivité du réseau, tout en offrant aux organisations de meilleures performances et une plus grande flexibilité. SPC avait récemment mis en œuvre le REDL avec l'un de ses partenaires et prévoyait procéder au lancement de projets pilotes liés au REDL avec d'autres partenaires dans un proche avenir. L'équipe d'audit n'a trouvé aucun document à l'effet que des fonds avaient été alloués à des solutions novatrices, telles que les initiatives de REDL. Toutefois, la direction a informé l'équipe d'audit qu'il y avait une demande de financement à cet effet dans le prochain budget.

En conclusion, SPC ne disposait pas d'un programme rigoureux pour mettre à l'essai les services de RE, d'un programme robuste de renouvellement de la TI et d'un investissement continu soutenant l'innovation des services de RE. Un programme rigoureux de mise à l'essai des services de RE et un programme de renouvellement de la TI qui sont priorisés adéquatement réduiraient les risques potentiels pour la disponibilité des services de RE. Enfin, l'obtention de financement permanent pour des technologies novatrices, comme le REDL, permettrait de maintenir ou d'améliorer la disponibilité des services de RE.

Recommandation 7	Priorité	Modérée
Le sous-ministre adjoint de la Direction générale des services de réseaux et de sécurité devrait développer, documenter et mettre en œuvre un programme complet pour mettre à l'essai les services de RE.		

Réponse de la direction

La direction est d'accord avec la recommandation.

Le rapport d'audit fait référence à un manque d'essais en cours de production. Bien que certains services disposent déjà des essais en cours de production (p. ex. l'Internet d'entreprise est testé une fois par semaine), cela n'est pas possible pour tous les environnements de production du RE en raison de la criticité du service fourni et, dans certains cas, les clients ne nous permettent pas d'effectuer ces essais. La direction accepte le risque de ne pas faire d'essais dans les environnements de production, car il est plus risqué de procéder à des essais en cours de production que de ne pas le faire.

La gestion des réseaux internationaux est un exemple d'essai de performance des services de RE. Le processus consiste à vérifier l'approvisionnement en RE après la mise en œuvre d'un changement de transporteur et à tester le rendement dans le cadre de la gestion des incidents de façon ponctuelle.

Compte tenu de ces restrictions, nous examinerons les options de mise à l'essai au sein des secteurs d'activité touchés et mettrons en œuvre un programme pour mettre à l'essai l'infrastructure des services de RE. Plusieurs options sont actuellement à l'étude.

Recommandation 8	Priorité	Modérée
Le sous-ministre adjoint de la Direction générale des services de réseaux et de sécurité devrait veiller à ce que le remplacement de l'équipement de TI vieillissant soit adéquatement classé par ordre de priorité en fonction du financement disponible et à ce que des mécanismes de surveillance, de suivi et de production de rapports soient mis en place.		

Réponse de la direction

La direction est d'accord avec la recommandation.

Le programme de renouvellement et de remplacement de la TI (RRTI) est géré de façon centralisée au sein de SPC. Il permet d'obtenir et de distribuer des fonds pour réparer et remplacer (ou moderniser lorsque c'est possible) les composants de l'infrastructure de TI de SPC dont la défaillance pourrait entraîner une interruption de service mettant en péril les opérations gouvernementales et les services aux Canadiens et Canadiennes.

À mesure que des fonds du programme de RRTI (ou des allocations spéciales) sont fournis à la DGSRS, l'équipement vieillissant est remplacé. L'équipement est classé par ordre de priorité de sorte que celui

qui est le plus urgent/essentiel soit remplacé en premier. Les exigences de la Direction générale pour la RRTI sont recueillies une fois par année au troisième trimestre au moyen d'une lettre d'appel aux directeurs de la DGSRS responsables de l'infrastructure afin d'élaborer des listes de priorités conformément aux normes du programme de RRTI; l'établissement des priorités est fondé sur de multiples variables, comme le risque, l'incidence sur les partenaires, l'incidence sur le projet, le rôle et l'âge. Les listes de priorités sont ensuite utilisées par le programme de RRTI pour établir l'ordre de priorité des équipements vieillissants au sein du ministère en fonction des fonds disponibles.

À l'heure actuelle, il existe un processus à l'échelle du ministère qui comprend la surveillance, le suivi et la production de rapports. La surveillance et le suivi sont effectués au niveau de la DG en suivant les lignes directrices et le calendrier du programme de RRTI. Les feuilles de calcul de suivi sont mises à jour par la Direction générale à mesure que les activités d'approvisionnement avancent pour indiquer l'état de l'approvisionnement (soumis, commandé, annulé, etc.). Le Programme de RRTI présente régulièrement des rapports au SCT pour montrer les progrès réalisés en matière d'investissement dans l'infrastructure tout au long de l'année. La gouvernance (y compris le Comité des opérations et des services et le Conseil de gestion des finances, des investissements et de la gestion interne) est en place pour veiller à ce que les fonds soient attribués et priorisés correctement dans l'ensemble du Ministère. La planification est également en cours à la Direction générale de la gestion des opérations pour transférer ces fonctions à une solution de données ministérielles (c.-à-d. le magasin de données opérationnelles (MDO) ou Onyx) à l'avenir.

3.4 Surveillance des obligations des fournisseurs

Critère d'audit : La Direction générale des réseaux, de la sécurité et des services numériques veille à ce que les fournisseurs de services externes respectent leurs obligations et s'assure que les services gérés de RE sont fournis conformément aux modalités des contrats et aux accords de niveau de service.

L'équipe d'audit s'attendait à ce que la Direction générale des réseaux, de la sécurité et des services numériques (DGRSSN) surveille les modalités des contrats des fournisseurs, le rendement des fournisseurs[1] et la qualité des services fournis par les fournisseurs, et à ce qu'elle demande des crédits de service lorsque les cibles de niveau de service (CNS) ne sont pas atteintes.

L'équipe d'audit a constaté que la DGRSSN surveillait adéquatement les contrats des fournisseurs.

SPC fait appel aux entreprises de télécommunication pour fournir les services gérés de RE à l'appui de ses partenaires. Ces services de RE soutiennent de nombreux services essentiels offerts aux Canadiens et Canadiennes. Les services de réseau externalisés comprennent les télécommunications, la surveillance, la production de rapports et la sécurité. Étant donné qu'il y avait un certain nombre de contrats de

[1] COBIT 5.0, Politique du CT sur les services et le numérique, Directive de SPC sur la gestion des services de la technologie de l'information

télécommunications actifs évalués à des centaines de millions de dollars, il était important que SPC surveille les contrats pour assurer le respect des modalités.

Pour évaluer le processus de conformité de SPC, l'équipe d'audit a sélectionné un échantillon de quatre contrats de fournisseurs d'une population de dix-huit (18) contrats. L'équipe d'audit a constaté que les contrats des fournisseurs et les énoncés de travail définissaient les CNS utilisées pour surveiller le rendement des services de RE et soulignaient les conséquences en cas de non-conformité. Pour répondre aux exigences contractuelles, les fournisseurs ont présenté des rapports mensuels sur les services gérés de RE pour la majorité des CNS mentionnés dans les contrats, les énoncés de travail (EDT) et les accords de niveau de service (ANS), sauf pour le contrat du volet 3 du RE du GC où l'on rendait compte des CNS seulement lorsque ces derniers n'étaient pas respectés. Les rapports mensuels fournissaient également des informations sur les CNS non satisfaits et sur certains paramètres d'utilisation de la bande passante. L'équipe d'audit a constaté que les CNS variaient d'un contrat à l'autre.

La plupart des contrats d'entreprise étaient suivis par l'équipe de la Planification, ingénierie et services gérés de réseau (PISGR) (à l'exception du volet 3 du RE du GC), et la plupart des anciens contrats étaient supervisés par les équipes des opérations du RE. Les CNS sont examinés chaque mois et des crédits de service pour le non-respect des CNS étaient documentés, discutés et demandés aux fournisseurs. Des discussions avaient lieu tous les mois avec les fournisseurs dans le cadre des examens de rendement des services de RE. Les comptes rendus de ces réunions étaient consignés, mis en application et examinés aux fins de conformité du contrat. Cependant, pour certains des anciens contrats ou des contrats à l'étape de la migration, des réunions mensuelles n'étaient pas toujours organisées. Les équipes des opérations du RE consignaient et employaient les données d'utilisation de la bande passante du RE et les données d'incident générées en interne dans le cadre de la validation mensuelle de la facturation et de l'exercice de crédit de service.

En conclusion, les contrats des services gérés de RE faisaient l'objet d'une surveillance suffisante pour s'assurer que les services étaient fournis conformément aux modalités des contrats et aux accords de niveau de service.

3.5 Performance des services de RE

Critère d'audit : La Direction générale des réseaux, de la sécurité et des services numériques met en œuvre un plan efficace de gestion de la capacité et de la disponibilité du RE, y compris l'établissement d'une base de référence et l'utilisation d'indicateurs de rendement clés (IRC) pertinents pour évaluer la performance des services de RE.

L'équipe d'audit s'attendait à ce que la Direction générale des réseaux, de la sécurité et des services numériques (DGRSSN) ait mis en œuvre un plan et un processus de gestion de la capacité et de la

disponibilité du RE, incluant des informations de base et l'utilisation d'IRC pour évaluer la performance des services de RE[2].

Les processus de gestion de la performance et de la capacité du RE sont des éléments essentiels à la prestation des services essentiels du gouvernement du Canada (GC). La performance des services de RE doit être surveillée et faire l'objet de rapports, et tout incident de non-conformité des services doit être discuté avec les fournisseurs (comme indiqué dans le critère d'audit 3.4). De plus, la capacité du RE et des circuits doit être surveillée pour s'assurer qu'elle satisfait aux exigences opérationnelles des partenaires, ainsi qu'à la norme de service de SPC pour la disponibilité du RE de 99,15 %.

L'équipe d'audit a constaté qu'il existait une norme de service de disponibilité définie pour chacune des 80+ offres de services au sein des services de RE. En date d'octobre 2020, toutes les normes de service relatives à la disponibilité, sauf quatre, ont été respectées, et la disponibilité globale a été déclarée à 99,965 %, ce qui dépasse la norme de service de 99,15 %.

L'équipe d'audit a également constaté que les équipes des opérations du RE utilisaient différentes approches et différents outils de surveillance des services pour saisir les normes de service et les IRC du RE et en faire rapport. L'information n'était pas analysée de façon proactive pour déterminer le rendement et les goulots d'étranglement du RE ainsi que pour planifier les besoins futurs en matière de bande passante des services du RE. Certaines équipes d'exploitation du RE utilisaient uniquement les outils et les rapports du fournisseur pour cerner les problèmes de rendement du RE et l'analyse de la bande passante. Les rapports fournis par le fournisseur étaient utilisés pour déterminer si les normes de service étaient respectées, mais ils n'étaient pas suffisamment détaillés pour déterminer les causes des pointes de bande passante ou des augmentations de l'utilisation de la bande passante, et pour fournir une analyse des tendances précise.

SPC a examiné les données de référence sur l'utilisation des services, l'utilisation de la bande passante, le rendement et les paramètres de disponibilité à l'aide des rapports mensuels fournis par le fournisseur. L'équipe d'audit a constaté que les mesures correctives des problèmes de rendement du RE n'étaient pas toujours prises en temps opportun et qu'aucune base de référence d'entreprise qui regrouperait les données recueillies sur les services de RE à l'échelle du GC n'avait été établie pour le RE du GC. Sans une vue d'ensemble du rendement des services de RE, il est difficile d'évaluer le rendement des services de RE à l'échelle de l'entreprise et les besoins futurs en matière de capacité.

En conclusion, bien que la majorité des normes de service était respectée, il n'y avait pas d'approche uniforme pour évaluer de manière proactive le rendement des services de RE. Il n'y avait pas de données de référence sur le RE du GC, les indicateurs de rendement clés (IRC) variaient d'un fournisseur à l'autre et différentes équipes utilisaient différents outils.

[2] BITI version 3.0 et Cobit version 5.0

Recommandation 9	Priorité	Modérée
Le sous-ministre adjoint de la Direction générale des services de réseaux et de sécurité devrait élaborer une approche uniforme pour évaluer de façon proactive la performance des services de RE, avec la base de référence, les IRC et les outils nécessaires pour cerner les problèmes de performance potentiels et y remédier en temps opportun.		
Réponse de la direction		
La direction est d'accord avec la recommandation. Le rendement du service est actuellement mesuré et les outils existants sont utilisés pour cerner les problèmes de rendement. Cela dit, nous convenons que les données n'ont pas été recueillies de façon uniforme ou avec les mêmes outils. Au moment de la rédaction de la présente réponse, une approche uniforme a été élaborée au moyen du RE du GC et des mécanismes de passation de marchés des Services de réseau du gouvernement du Canada (SRGC). Quatre-vingt-dix pour cent des partenaires ont migré vers les contrats de RE du GC et utilisent un seul système avec les mêmes IRC. Les autres services de RE seront fournis par l'entremise des SRGC.		

C. Conclusion

Il y avait une surveillance suffisante pour veiller à ce que les services de RE s'harmonisaient avec les objectifs stratégiques définis dans la *Politique et la Directive du Conseil du Trésor sur les services et le numérique*, le *Plan stratégique des opérations numériques du Secrétariat du Conseil du Trésor* et SPC 3.0.

Il y avait une surveillance suffisante des contrats de services de RE gérés pour s'assurer que les services étaient fournis conformément aux modalités de leurs contrats et des accords de niveau de service. La majorité des normes de service liées à la disponibilité des services de RE étaient respectées.

SPC tenait des registres des risques distincts pour surveiller les risques liés au RE aux niveaux du projet, de la direction générale et des opérations. Ces registres n'étaient pas intégrés, ce qui limitait la capacité de la direction d'élaborer des stratégies d'atténuation des risques et de surveiller leur efficacité.

La Direction générale des réseaux, de la sécurité et des services numériques disposait d'une ébauche de plan des ressources humaines (RH) pour 2020-2021. La planification de la relève, qui comprend le partage des connaissances et la documentation, ainsi que le jumelage avec un agent expérimenté, était limitée et pourrait ne pas combler l'écart découlant du nombre d'employés qui devraient prendre leur retraite dans un proche avenir. La Direction générale n'avait pas entrepris d'analyse pour déterminer les lacunes entre les compétences disponibles et les compétences nécessaires pour appuyer les services de RE.

Il n'y avait pas de stratégie d'ensemble de gestion de la capacité du RE pour les services de RE. Il n'y avait pas non plus de processus documenté qui tenait compte des données d'utilisation de la bande passante, des exigences des applications, des demandes opérationnelles (DO), des projets de migration de la charge de travail (MCT) et des besoins de migration vers le nuage pour la prévision des services de RE. Les plans de continuité des activités (PCA) n'étaient pas systématiquement mis à jour et à l'essai, les plans de continuité de la TI inclus dans les PCA étaient incomplets et les procédures opérationnelles normalisées (PON) n'avaient pas été établies pour tous les services de RE.

SPC ne disposait pas d'un programme rigoureux de mise à l'essai des services de RE et d'un programme de renouvellement de la TI priorisé adéquatement pour l'équipement de RE.

Il n'y avait pas d'approche uniforme pour évaluer de manière proactive le rendement des services de RE. Il n'y avait pas de données de référence sur le RE du GC, les indicateurs de rendement clés (IRC) variaient d'un fournisseur à l'autre et différentes équipes utilisaient différents outils.

Annexe A – Secteurs d'intérêt et critères d'audit

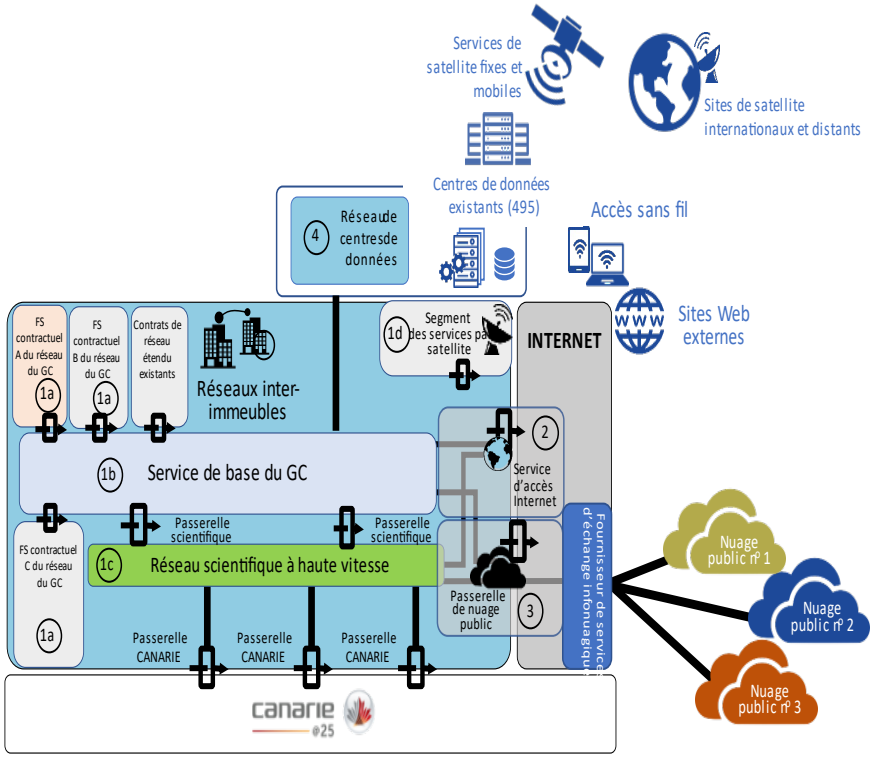
Audit du réseau étendu – Planification de la capacité et de la disponibilité	
Titre du critère	**Critère d'audit**
Secteur d'intérêt 1 : Gouvernance[1,2,3,6]	
1.1 Surveillance	SPC veille à ce que les services de RE s'harmonisent avec les objectifs stratégiques définis dans la *Politique et la Directive du Conseil du Trésor (CT) sur les services et le numérique*, le *Plan stratégique des opérations numériques du Secrétariat du Conseil du Trésor (SCT)* et SPC 3.0.
Secteur d'intérêt 2 : Risques[1,5]	
2.1 Gestion des risques	La Direction générale des réseaux, de la sécurité et des services numériques a élaboré et mis en œuvre un registre des risques qui détermine les risques, le niveau de risque, la responsabilité du risque et la réponse au risque, pour les services de RE.
Secteur d'intérêt 3 : Contrôles internes [1,2,3,4,6]	
3.1 Planification des ressources humaines	La Direction générale des réseaux, de la sécurité et des services numériques, a élaboré un plan complet et approuvé de ressources humaines (RH) qui précise les exigences en matière de compétences requises, les plans de relève et la formation afin d'assurer une dotation en personnel appropriée pour la prestation des services de RE du gouvernement du Canada (GC).
3.2 Stratégie sur la capacité et la disponibilité du RE	La Direction générale des réseaux, de la sécurité et des services numériques dispose d'une stratégie de gestion de la capacité du RE du gouvernement du Canada (GC), y compris des exigences relatives à la réalisation d'évaluations de routine des services de RE en tenant compte de la disponibilité, de la capacité, de la gestion et de l'engagement des partenaires, et de la planification de la continuité des activités et de la TI.
3.3 Disponibilité du RE	La disponibilité du RE de SPC est assurée par la mise en œuvre d'essais rigoureux, d'un programme de renouvellement de la TI et d'un investissement continu pour soutenir l'innovation des services de RE.
3.4 Surveillance des obligations des fournisseurs	La Direction générale des réseaux, de la sécurité et des services numériques veille à ce que les fournisseurs de services externes respectent leurs obligations et s'assure que les services gérés de RE sont fournis conformément aux modalités des contrats et aux accords de niveau de service.
3.5 Performance des services de RE	La Direction générale des réseaux, de la sécurité et des services numériques, met en œuvre un plan efficace de gestion de la capacité et de la disponibilité du RE, y compris l'établissement d'une base de référence et l'utilisation d'indicateurs de rendement clés (IRC) pertinents pour évaluer la performance des services de RE.

Sources des critères

[1] Cobit version 5.0
[2] BITI version 3
[3] Politique sur les services et le numérique du SCT
[4] Directive de SPC sur la gestion des services de TI
[5] Guide de gestion intégrée du risque du SCT
[6.] Directive sur les services et le numérique du SCT

Annexe B – Topologie du réseau étendu

Le réseau E2E du GC



Services de réseau de bout en bout et segments de services du GC

1. **Réseaux de données inter-immeubles** (réseaux étendus [RE])
   - 1a **Accès inter-immeubles** (réseaux [connectant les immeubles et les sites du GC au service de base])
   - 1b **Service de base du GC** (interconnexion haute vitesse des centres de données avec les réseaux d'accès)
   - 1c **Réseau scientifique du GC** (accès réseau spécialisé destiné aux applications et aux utilisateurs scientifiques du GC)
   - 1d **Services par satellite du GC** (services de connectivité distants et spécialisés aux réseaux secrets)
2. **Service d'accès Internet d'entreprise** (SIE)
3. **Services d'accès infonuagiques d'entreprise** (connectivité sécuritaire haute vitesse aux fournisseurs de services infonuagiques et d'échange infonuagique)
4. **Réseaux de centres de données** (connectivité réseau à l'intérieur des centres de données d'entreprise et existants)

Annexe C – Ordre de priorité des recommandations faisant suite à l'audit

Le BVE attribue une note d'évaluation aux recommandations relatives à la mobilisation interne pour indiquer la priorité de chaque recommandation à la direction. Cette évaluation correspond à l'exposition au risque attribué aux observations indiquées dans l'audit et aux conditions sous-jacentes à la recommandation selon le contexte organisationnel.

Légende des recommandations	
Note	**Explication**
Priorité ÉLEVÉE	• Devrait être traitée en priorité par la direction dans les 6 à 12 mois. • Les contrôles sont inadéquats. On a relevé des problèmes importants qui pourraient nuire à l'atteinte des objectifs organisationnels. • Pourrait entraîner une importante exposition aux risques (p. ex. réputation, contrôle financier ou capacité à atteindre les objectifs ministériels). • Apporte de grandes améliorations à l'ensemble des processus opérationnels.
Priorité MODÉRÉE	• Devrait être réglé au cours de l'année ou dans un délai raisonnable. • Des contrôles ont été mis en place, mais ils ne sont pas suffisamment respectés. On a relevé des problèmes qui pourraient nuire à l'efficacité et à l'efficience des activités. • Les éléments observés pourraient entraîner une exposition aux risques (p. ex. réputation, contrôle financier ou capacité d'atteindre les objectifs de la direction générale) ou nuire à l'efficacité. • Apporte des améliorations à l'ensemble des processus opérationnels.
Priorité FAIBLE	• Des changements sont souhaitables dans un délai raisonnable. • Des contrôles sont en place, mais le degré de conformité varie. • Les éléments observés indiquent la nécessité d'améliorer l'atténuation des risques ou les contrôles d'un aspect précis. • Apporte de petites améliorations à l'ensemble des processus opérationnels.

ANNEXE D – Liste des acronymes

Acronyme	Description
ANS	Accord de niveau de service
BVE	Bureau de la vérification et de l'évaluation
CDE	Centre de données d'entreprise
CEAI	Conseil d'examen de l'architecture intégrée
CEAS	Conseil d'examen de l'architecture de service
CES	Conseil exécutif de surveillance
CHP	Calcul de haute performance
CME	Commutation multiprotocole par étiquette
CMR	Cadre ministériel des résultats
CMRE	Comité de mesure du rendement et de l'évaluation
CNS	Cible de niveau de service
CT	Conseil du Trésor du Canada
DGDPT	Direction générale du dirigeant principal de la technologie
DGRSSN	Direction générale des réseaux, de la sécurité et des services numériques
DGSM	Direction générale de la stratégie et de la mobilisation
DGSRS	Direction générale des services de réseaux et de sécurité
DO	Demande opérationnelle
DPI	Dirigeant principal de l'information
DPT	Dirigeant principal de la technologie
EDT	Énoncé de travail
GC	Gouvernement du Canada

Acronyme	Description
GRC	Gendarmerie royale du Canada
GVCO	Gestion de la vulnérabilité et de la conformité organisationnelle
IRC	Indicateur de rendement clé
IRSC	Initiative de rétroaction sur la satisfaction de la clientèle
ITIL	Bibliothèque d'infrastructure des technologies de l'information
MCT	Migration de la charge de travail
MDO	Magasin de données opérationnelles
OISP	Opérations de l'infrastructure des services de police
PADG	Plan d'activités de la direction générale
PCA	Plan de continuité des activités
PISGR	Planification des réseaux, ingénierie et services gérés de réseau
PON	Procédure opérationnelle normalisée
RCD	Réseau de circuits dynamiques
RE	Réseau étendu
RE du GC	Réseau étendu du gouvernement du Canada
REDL	Réseau étendu défini par logiciel
RH	Ressources humaines
RL	Réseau local
RPV	Réseau privé virtuel
RRTI	Renouvellement et remplacement de la TI
SCT	Secrétariat du Conseil du Trésor du Canada
SGC	Services de gestion de la conformité
SGTSF	Service géré de transfert sécurisé de fichiers

Acronyme	Description
SGV	Services de gestion des vulnérabilités
SPC	Services partagés Canada
SRGC	Services de réseau du gouvernement du Canada
TI	Technologie de l’information

Annexe E – Glossaire

Le tableau suivant définit les termes utilisés et adaptés au contexte de cette vérification :

Expression	Définition
Appareils de réseau	Les appareils de réseau sont les commutateurs, les routeurs et les autres dispositifs de télécommunications connexes qui prennent en charge les services de RE. Ce terme doit être interprété au sens large pour désigner les actifs du RE qui doivent être gérés tout au long de leur cycle de vie et pour lesquels les risques de sécurité et de disponibilité doivent être atténués afin de garantir l'intégrité des services de RE.
Balayage	Le balayage est le processus qui consiste à obtenir des renseignements sur les actifs du RE pour détecter les risques opérationnels potentiels, comme les vulnérabilités relatives à la sécurité ou les configurations inadéquates.
Bande passante	La bande passante est le débit maximal de données qui peut être transmis sur un réseau.
Capacité des RH	La capacité des RH est la mesure visant à garantir qu'une organisation dispose d'un nombre suffisant de personnes qualifiées, au bon endroit et au bon moment, pour atteindre ses objectifs.
Capacité du RE	La capacité du RE est le trafic qu'un RE peut soutenir à tout moment.
Continuité de la TI	La continuité de la TI est une approche globale de la gestion des systèmes de TI en cas de perturbation majeure. La continuité de la TI comprend la prévention, l'atténuation et le rétablissement relatifs aux perturbations des systèmes de TI.
Contrat de fournisseur	Un contrat de fournisseur est un accord entre une organisation et un fournisseur pour l'acquisition de biens ou de services.
Données de référence	Instantané utilisé comme point de référence. De nombreux instantanés peuvent être pris et enregistrés au fil du temps, mais seuls quelques-uns seront utilisés comme données de référence. Par exemple, une référence de rendement peut être utilisée pour mesurer les changements dans le rendement au cours de la durée de vie d'un service de TI.

Expression	Définition
Équipement de TI vieillissant	L'équipement de TI qui est utilisé depuis longtemps et qui risque de tomber en panne à long terme, nécessitant des mises à niveau ou des remplacements pour rétablir les fonctionnalités.
Indicateur de rendement clé	Mesure du rendement qui permet aux organisations d'obtenir des renseignements sur de nombreux facteurs pertinents, comme l'efficacité et l'efficience de leurs processus. La principale fonction des IRC est d'aider les entreprises à trouver de meilleures façons de gérer et d'optimiser leurs activités internes.
Planification de la capacité	La planification de la capacité est le processus de détermination de la capacité nécessaire pour répondre aux exigences actuelles et futures convenues en matière de capacité et de performance, de manière rentable et en temps voulu.
Programme de renouvellement de la TI	Le programme de renouvellement de la TI est une initiative visant à maintenir à jour les actifs actuels de l'infrastructure de TI, au moyen de mises à jour de l'équipement et des logiciels ainsi que de processus permettant d'établir la nécessité de mettre à niveau ou de remplacer un actif de TI.
Registre des risques	Un registre des risques est un référentiel des risques et des mesures d'atténuation pour un système, un service ou une entité.
Rendement des services de RE	La performance des services du RE est la qualité des services fournis par un RE.
Service de RE	Un service de RE est un service de réseau pleinement géré qui interrelie les installations des partenaires et des clients à l'échelle métropolitaine, régionale, nationale ou internationale.
Service essentiel de RE	Un service essentiel de RE est un service dont la compromission, du point de vue de la disponibilité ou de l'intégrité, porterait un grave préjudice à la santé, à la sûreté ou au bien-être économique des Canadiens et Canadiennes, ou encore au fonctionnement efficace du gouvernement du Canada.
Surveillance	La surveillance est un processus continu visant à détecter les problèmes en matière de conformité et de risque.

Expression	Définition
Systèmes de TI vieillissants	Les systèmes de TI qui sont utilisés depuis longtemps et qui risquent de tomber en panne à long terme, nécessitant des mises à niveau ou des remplacements pour rétablir les fonctionnalités.