Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Feuille de route pour la migration vers la cryptographie post-quantique au sein du gouvernement du Canada (ITSM.40.001)

GSTI

Canada

Avant-propos

La présente publication est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir plus d'information ou suggérer des modifications, veuillez communiquer avec le Centre pour la cybersécurité :

- par courriel : cryptography-cryptographie@cyber.gc.ca;
- par téléphone : 613-949-7048 ou 1-833-CYBER-88.

Date d'entrée en vigueur

Le présent document entre en vigueur le 23 juin 2025.

Historique des révisions

Révision	Modifications	Date
1	Première version.	23 juin 2025

ISBN 978-0-660-77915-7
CAT D97-4/40-001-2025E-PDF

Vue d'ensemble

Tous les organismes qui gèrent des systèmes de technologies de l'information (TI) doivent procéder à la migration des composants de cybersécurité afin de résister aux attaques quantiques. Ils pourront ainsi se protéger contre la menace cryptographique posée par de futurs ordinateurs quantiques. Pour atténuer cette menace, le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) recommande l'adoption d'une cryptographie post-quantique (CPQ) normalisée.

La présente publication décrit la feuille de route que le Centre pour la cybersécurité recommande au gouvernement du GC en ce qui a trait à la migration des systèmes de TI non classifiés[1] vers la CPQ. Elle comprend des jalons, des livrables et des conseils à l'intention des ministères en matière de planification et d'exécution.

Les jalons et les livrables pour les ministères et organismes fédéraux sont les suivants :

- avril 2026 – développement d'un plan ministériel initial de migration vers la CPQ;
- début d'avril 2026 et chaque année par la suite – rapport sur les progrès réalisés relativement à la migration vers la CPQ;
- fin de 2031 – achèvement de la migration des systèmes hautement prioritaires vers la CPQ;
- fin de 2035 – achèvement de la migration des autres systèmes vers la CPQ.

[1] Par systèmes de TI non classifiés, on entend les systèmes qui ne contiennent, ne transfèrent et ne gèrent aucune information classifiée. Au gouvernement du Canada, les systèmes non classifiés traitent l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B. En ce qui concerne les systèmes classifiés et les systèmes traitant l'information PROTÉGÉ C, les ministères doivent communiquer avec le Centre pour la cybersécurité pour obtenir des conseils sur la migration vers de l'équipement commercial.

Table des matières

1 Introduction

Le Centre pour la cybersécurité recommande aux organismes qui gèrent des systèmes de TI de les migrer vers la CPQ de manière à remplacer la cryptographie à clé publique vulnérable à de futurs ordinateurs quantiques[2]. Toutes les instances de la cryptographie à clé publique doivent être migrées pour protéger les systèmes de TI du GC et les données des Canadiennes et Canadiens contre cette menace.

Le National Institute of Standards and Technology (NIST) des États-Unis a collaboré avec des spécialistes en cryptographie à travers le monde pour normaliser les algorithmes CPQ susceptibles de remplacer la cryptographie à clé publique vulnérable que nous utilisons actuellement. Le Centre pour la cybersécurité a publié ses recommandations en matière d'algorithmes CPQ dans le document *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* (ITSP.40.111). Comme les normes associées aux protocoles de sécurité des réseaux prennent en charge les algorithmes CPQ, le Centre pour la cybersécurité mettra à jour la publication *Conseils sur la configuration sécurisée des protocoles réseau* (ITSP.40.062). Les fournisseurs intègrent la CPQ dans leurs produits afin de se conformer rapidement aux besoins du gouvernement et de l'industrie.

La migration vers la CPQ au sein du GC exigera un engagement important et prendra plusieurs années. Le Centre pour la cybersécurité travaille avec le Secrétariat du Conseil du Trésor du Canada (SCT) et Services partagés Canada (SPC) pour apporter les mises à jour nécessaires aux conseils, au soutien et aux politiques du GC. Les ministères devront bien comprendre l'utilisation qu'ils font de la cryptographie. L'infrastructure de TI, tant logicielle que matérielle, et les données devront être analysées dans tout l'organisme. Il est important de commencer la migration vers la CPQ pour tirer avantage, autant que possible, des budgets existants relatifs au cycle de vie des TI.

Cette publication constitue la feuille de route recommandée par le Centre pour la cybersécurité en ce qui concerne la migration des systèmes de TI non classifiés vers la CPQ au sein du GC. Elle fait mention des parties prenantes, des phases d'exécution, des jalons et de la gouvernance qui orientent l'activité de cybersécurité à travers le GC. L'intention est de fournir les principales activités et les principaux échéanciers qui faciliteront la coordination des activités de planification des ministères en ce qui a trait à la migration vers la CPQ dans le GC. La présente est destinée aux directrices, aux directeurs et aux gestionnaires des systèmes de TI au sein des ministères et organismes fédéraux, ainsi qu'aux personnes qui devront prendre des décisions par rapport à la migration vers la CPQ.

[2] Pour plus d'information sur la menace que l'informatique quantique fait peser sur la cryptographie, prière de consulter le document *Préparez votre organisation à la menace que pose l'informatique quantique pour la cryptographie* (ITSAP.00.017) : https://www.cyber.gc.ca/fr/orientation/preparez-votre-organisation-menace-pose-informatique-quantique-itsap-00017.

2 Parties prenantes et planification

Le Centre pour la cybersécurité est la principale autorité technique en matière de sécurité des technologies de l'information (TI) dans le GC[3]. Relevant du Centre de la sécurité des télécommunications Canada, l'organisme cryptologique du Canada, le Centre pour la cybersécurité :

- sensibilise les ministères du GC à la menace que l'informatique quantique fait peser sur la cryptographie;
- fournit une orientation quant à la formulation de recommandations en matière de cryptographie, comme le recours à la CPQ;
- offre des recommandations sur l'intégration de la cryptographie dans une posture de cybersécurité robuste.

Le Centre pour la cybersécurité continuera de fournir des avis et des conseils pertinents pour soutenir les ministères et organismes du GC dans le cadre de la migration vers la CPQ.

Le SCT est responsable de l'établissement et de l'encadrement d'une approche pangouvernementale à la gestion de la sécurité, dont la cybersécurité. Pour mener à bien cette responsabilité, il exerce son leadership en matière de politique, fournit une orientation stratégique et assure la supervision. En mai 2024, le SCT a publié la Stratégie intégrée de cybersécurité du gouvernement du Canada dans laquelle il fait mention d'une action clé de la migration des systèmes du GC vers l'utilisation d'une CPQ normalisée visant à protéger l'information et les biens du GC contre la menace quantique. Le SCT livrera les instruments de politique nécessaires pour faire en sorte que les cadres responsables puissent élaborer un plan ministériel de migration vers la CPQ et faire état des progrès réalisés dans le cadre des processus ministériels existants en matière de production de rapports.

SPC gère l'infrastructure et les services de TI au nom de plusieurs ministères et organismes du GC. En raison du rôle crucial qu'il joue dans la modernisation des systèmes du GC, SPC prend déjà part à l'élaboration d'un plan de migration vers la CPQ et collabore directement avec le Centre pour la cybersécurité et le SCT pour fournir des conseils sur la faisabilité de la mise en œuvre.

Les ministères et organismes fédéraux du GC sont responsables de la gestion des risques liés à la cybersécurité dans leurs secteurs de programme. Il leur incombera d'assurer la maintenance des logiciels hébergés sur l'infrastructure de TI gérée par SPC et de toute infrastructure de TI dont la gestion ne relève pas de SPC, y compris les services infonuagiques externalisés. Les ministères et organismes devront élaborer un plan ministériel de migration sur mesure vers la CPQ, qui tient compte de la migration des systèmes pour lesquels ils doivent utiliser la CPQ. Ils seront également tenus d'exécuter ce plan, d'en faire le suivi et de faire rapport des progrès réalisés. Cette publication contient les premières considérations qui peuvent être utilisées dans l'élaboration d'un plan ministériel de migration vers la CPQ, mais des conseils et du soutien supplémentaires seront fournis par le SCT, SPC et le Centre pour la cybersécurité.

[3] *Politique sur la sécurité du gouvernement* du Secrétariat du Conseil du Trésor du Canada : https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=16578

3 Phases d'exécution

Cette feuille de route aborde les trois phases visant à assurer la mise en œuvre de la migration vers la CPQ. Il est probable que ces phases se chevauchent.

3.1 Préparation

Au cours de la phrase de préparation, les ministères et organismes seront responsables de l'élaboration d'un plan ministériel de migration vers la CPQ visant à assurer la migration des systèmes sous leur responsabilité de manière à utiliser la CPQ. Pour ce faire, il est recommandé de mettre sur pied un comité et d'identifier une personne qui sera responsable de la migration. Le comité devrait être composé de parties prenantes provenant de tout l'organisme et compter au moins une ou un membre de la haute direction pour s'assurer que la direction adhère au plan et le soutienne. En plus des secteurs techniques responsables de la gestion des systèmes de TI, il est recommandé d'inclure des parties prenantes de secteurs non techniques, comme les finances, la gestion de projets, l'approvisionnement et la gestion des biens.

Le plan ministériel de migration vers la CPQ doit constamment être revu et développé lors de l'exécution des phases subséquentes. La version initiale du plan de migration du GC vers la CPQ devrait déterminer les personnes responsables de ce qui suit :

- l'exécution du plan;
- la planification financière;
- la stratégie de formation visant à informer le personnel de la menace quantique et de l'avancement de cette migration au sein de l'organisme;
- l'élaboration des politiques d'approvisionnement pour le nouvel équipement;
- les approches adoptées pour repérer les systèmes vulnérables afin de dresser un inventaire pour la transition.

3.1.1 Rôles et responsabilités

Le plan ministériel de migration vers la CPQ doit identifier les personnes chargées d'accomplir les diverses tâches associées à l'exécution du plan. Finalement, il incombe à l'agente ou agent désigné pour la cybersécurité (ADCS) d'atténuer le risque que l'informatique quantique fait peser sur la cybersécurité. On recommande d'attribuer à l'ADCS, ou à une ou un cadre délégué, le rôle de responsable général de la migration vers la CPQ pour les questions de :

- surveillance;
- responsabilisation;
- soutien organisationnel à l'exécution du plan ministériel de migration vers la CPQ.

La coordination et l'engagement interministériel peuvent être assurés par une ou un responsable technique de la migration vers la CPQ. La ou le responsable technique aurait pour tâche de faciliter la coordination au sein de l'organisme, ce qui pourrait comprendre la prestation de service, la gestion de réseau et l'acquisition de produits de TI, et de gérer les autres domaines pertinents pour la migration. On peut également faire appel au comité mis en place pour élaborer le plan ministériel de migration vers la CPQ afin de gérer l'exécution du plan.

3.1.2 Planification financière

Les ministères et organismes devraient s'attendre à remplacer plusieurs systèmes de TI existants ou à mettre en place de nouveaux contrats de service pour prendre en charge la CPQ. L'exécution de la migration vers la CPQ aura une incidence sur le personnel dans la mesure où il pourrait être nécessaire de procéder à de nouvelles embauches, d'obtenir les services d'entrepreneures et entrepreneurs externes ou de réorganiser les rôles susceptibles d'avoir des répercussions sur d'autres projets ou activités professionnelles. Le plan ministériel de migration vers la CPQ doit fournir une estimation des coûts et faire mention de l'attribution des ressources nécessaires pour assurer son exécution. L'estimation des coûts figurant dans la version initiale du plan ne sera pas exhaustive, mais les estimations financières peuvent être ajustées au fil des phases de détermination et de transition.

Il est possible de réduire les coûts associés à cette migration vers la CPQ en faisant appel aux cycles de vie existant de l'équipement de TI et aux plans de modernisation des systèmes. Pour ce faire, il est primordial d'exécuter sans tarder les phases initiales de ce plan afin de déterminer les gains d'efficience possibles. Les délais résultant d'un approvisionnement précipité augmenteront les coûts.

3.1.3 Stratégie de formation

Il est important que les membres du personnel de l'organisme soient toutes et tous au courant de la menace quantique et des répercussions qu'elle pourrait avoir sur les systèmes qu'ils utilisent ou dont ils sont responsables. La plateforme GCÉchange du SCT facilitera la mise en commun des artéfacts avec les ministères et organismes, dont les documents produits par le Centre pour la cybersécurité. On y retrouve notamment des présentations et des publications destinées à divers publics. Le Carrefour de l'apprentissage du Centre pour la cybersécurité offrira du matériel didactique sur la menace que l'informatique quantique fait peser sur la cryptographie. Les cadres supérieures et supérieurs doivent être au courant des répercussions qu'aura la migration vers la CPQ sur leurs activités.

À mesure qu'avance la migration vers la CPQ, il est important d'informer les membres de la haute direction des développements et des progrès réalisés, notamment des nouveaux défis ou obstacles que les équipes doivent surmonter.

3.1.4 Politiques d'approvisionnement

Pour maximiser la durée de vie des nouveaux systèmes, les ministères et organismes devraient veiller à ce que les nouvelles acquisitions aient les exigences nécessaires pour prendre en charge la CPQ. Le Centre pour la cybersécurité recommande fortement que les systèmes se conforment aux normes établies en matière de cybersécurité. Le respect de ces normes fournit l'assurance d'un examen indépendant de la sécurité et favorise l'interopérabilité pour éviter la dépendance envers un fournisseur. Certaines normes de cybersécurité sont toujours en cours d'examen pour ce qui est de la prise en charge de la CPQ. Le Centre pour la cybersécurité met à jour le document *Conseils sur la configuration sécurisée des protocoles réseau* (ITSP.40.062), puisque la prise en charge de la CPQ est déjà intégrée dans les normes énoncées. On s'attend à ce que certaines catégories de produits ne permettent pas encore la prise en charge de la CPQ.

Le Centre pour la cybersécurité a recommandé que des clauses soient ajoutées aux contrats pour les systèmes comportant des modules cryptographiques. Ces derniers sont disponibles sur demande et seront offerts à plus grande échelle. En règle générale, les ministères et organismes devraient envisager d'adopter les pratiques exemplaires suivantes en matière d'approvisionnement :

- ajouter des clauses aux contrats pour veiller à ce que le fournisseur assure une prise en charge de la CPQ qui est conforme aux recommandations du Centre pour la cybersécurité énoncées dans l'ITSP.40.111, *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B*;
- certifier les modules cryptographiques dans le cadre du Programme de validation des modules cryptographiques;
- prendre en compte le soutien nécessaire à l'agilité cryptographique pour permettre d'éventuels changements de configuration.

Plus tôt la CPQ est incluse dans les clauses d'approvisionnement, plus bas seront les coûts pour les ministères lors de la migration.

3.1.5 Approches du plan en matière de détermination

La prochaine phase de cette feuille de route consiste à déterminer où la cryptographie est utilisée dans les systèmes de TI. Parfois appelée la découverte de produits cryptographiques, cette détermination est nécessaire pour dresser l'inventaire des systèmes devant faire l'objet de la migration. Le plan ministériel de migration vers la CPQ doit tenir compte des approches à adopter pour repérer les systèmes et en faire l'inventaire. On retrouve à la section suivante de plus amples détails sur la détermination.

3.2 Détermination

Déterminer où et comment la cryptographie est utilisée est une étape essentielle au processus de migration vers la CPQ. Parmi les systèmes faisant appel à la cryptographie, on retrouve notamment :

- les services réseau;
- les systèmes d'exploitation;
- les applications;
- les filières de développement de code;
- tous les biens de TI physiques, comme :
    - les bâtis de serveurs;
    - les ordinateurs de bureau;
    - les ordinateurs portables;
    - les téléphones mobiles;
    - les dispositifs réseau;
    - les imprimantes;
    - la téléphonie voix sur protocole IP;
    - les modules de sécurité matériels;
    - les cartes à puce;
    - les jetons d'authentification matériels.

Ces systèmes peuvent être hébergés sur site ou sur des plateformes de TI externalisées, être fournis par un fournisseur de services infonuagiques ou être en possession d'une employée ou un employé. Comme la portée est vaste, la détermination n'est pas une tâche facile.

L'information collectée au cours de cette phase sera utilisée pour dresser un inventaire qui devrait inclure ce qui suit au sujet de chaque système :

- les composants de systèmes faisant appel à la cryptographie;
- le fournisseur et la version de produit de chacun des composants;
- les contrôles de sécurité qui dépendent de la cryptographie relevée[4];
- les zones de sécurité de réseau applicables;
- les configurations cryptographiques actuelles;
- la plateforme hôte;
- les dépendances du système;
- les marchés de services pertinents et les dates d'expiration;
- l'année d'actualisation prévue du système ou de ses composants;
- la personne-ressource responsable au sein du ministère;
- la priorité à accorder à la migration du système.

Il pourrait être pertinent d'inclure d'autres renseignements techniques dans l'inventaire. Le Centre pour la cybersécurité fournira de plus amples conseils aux ministères à mesure que l'expérience grandit au sein du GC.

Les ministères doivent établir les systèmes qu'il convient de migrer en priorité vers la CPQ. Les systèmes qui assurent la confidentialité de l'information acheminée par l'intermédiaire de zones de réseaux publics[5] pourraient être à risque plus tôt que prévu en raison de la menace posée par les attaques de type « récolter maintenant, déchiffrer plus tard » (HNDL pour *Harvest Now, Decrypt Later*). Dans le cadre d'une telle attaque, un auteur de menace intercepte et stocke de l'information chiffrée, puis la déchiffre plus tard, à l'arrivée d'ordinateurs quantiques suffisamment puissants. Il est recommandé d'accorder une priorité élevée aux systèmes vulnérables à la menace HNDL et de les migrer en premier. Parmi les autres facteurs à considérer, on retrouve la durée de vie de l'information, le soutien nécessaire pour assurer l'agilité cryptographique et les répercussions d'une compromission. Il pourrait être utile de procéder à une évaluation des risques liés à la menace quantique afin de confirmer que les systèmes ont été hiérarchisés adéquatement.

La découverte des systèmes faisant appel à une cryptographie vulnérable devrait être réalisée au moyen de multiples méthodes. Un moyen efficace de produire l'inventaire ministériel initial consiste à tirer avantage des processus de gestion des services de TI (GSTI) existants au sein de l'organisme. Les comités responsables de la gestion du cycle de vie et des changements devraient avoir une bonne partie de l'information requise pour procéder à la saisie dans un système d'inventaire. Dans la pratique, la maturité de la GSTI pourrait toutefois varier d'un ministère à l'autre.

---

[4] *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33) : *Annexe 3A - Catalogue des contrôles de sécurité* : https://www.cyber.gc.ca/fr/orientation/annexe-3a-catalogue-des-controles-de-securite-itsg-33

[5] *Exigences de base en matière de sécurité pour les zones de sécurité de réseau* (ITSP.80.022) : https://www.cyber.gc.ca/fr/orientation/exigences-de-base-en-matiere-de-securite-pour-les-zones-de-securite-de-reseau-version

Des outils et services logiciels seront nécessaires pour effectuer la découverte des produits cryptographiques. On peut faire appel aux services de cybersécurité existants, comme les solutions de gestion des informations et des événements de sécurité (GIES), la surveillance et l'inspection des réseaux, et les technologies de détection et d'intervention au point d'extrémité (EDR pour *Endpoint Detection and Response*). Ces services pourraient exiger des changements de configuration, des modules d'extension tiers ou des filtres additionnels pour déterminer l'utilisation de la cryptographie. Les outils indépendants de découverte de produits cryptographiques feront appel à la technologie pour analyser les réseaux, les hôtes, les fichiers journaux ou le code source. Le programme de capteurs du Centre pour la cybersécurité est un outil qui devrait aider les ministères à procéder à la phase de détermination. De plus amples conseils sur les outils et services de découverte de produits cryptographiques seront fournis aux ministères par le comité tripartite sur la sécurité des TI composé du SCT, de SPC et du Centre pour la cybersécurité.

Il est important de ne pas se laisser dépasser par l'ampleur du travail nécessaire à la découverte. Il est préférable de commencer par un inventaire initial incomplet, puis de prendre des mesures pour améliorer graduellement les données.

Au cours de la phase de détermination, les ministères devraient utiliser l'inventaire pour mobiliser les fournisseurs, les entrepreneures et les entrepreneurs de TI appropriés afin d'élaborer leurs plans et de mettre en œuvre la CPQ dans leurs produits et leurs services. Pour faciliter la prochaine étape de l'élaboration d'un plan de transition, il convient de comprendre quels composants de systèmes seront admissibles aux mises à niveau et quels composants devront être remplacés.

3.3 Transition

La phase de transition utilise l'inventaire dressé au cours de la phase de détermination pour planifier et réaliser les mises à niveau, le remplacement, la tunnellisation et/ou l'isolation des systèmes.

En plus des données de l'inventaire, le plan doit tenir compte des ressources ministérielles afin de déterminer et d'évaluer les solutions, d'assurer l'approvisionnement nécessaire, de les tester et de les mettre en œuvre. Le plan pour chaque système exigera généralement plusieurs étapes et devrait être intégré aux processus existants de gestion des changements de TI pour garantir une bonne préparation, notamment :

- une évaluation des répercussions;
- un guide opérationnel sur la restauration;
- un environnement intermédiaire pour la mise à l'essai des changements;
- une surveillance pour assurer le bon fonctionnement après la transition.

Pour chaque système, les équipes techniques doivent déterminer et évaluer les solutions afin d'intégrer la CPQ, ou atténuer la menace quantique de toute autre manière. La disponibilité des produits avec capacité CPQ peut être limitée dans les premières phases, mais les fournisseurs adoptent rapidement la CPQ dans la foulée des mises à jour qui sont apportées aux normes des protocoles. Les solutions devraient satisfaire toutes les exigences en matière d'approvisionnement établies à la phase de préparation (Politiques d'approvisionnement 3.1.4).

Plusieurs systèmes devront maintenir une rétrocompatibilité pour permettre un fonctionnement continu avec les systèmes non migrés pendant quelque temps. La première étape de la transition d'un système peut consister à prendre en charge la CPQ, puis sera suivie par une deuxième étape dans le cadre de laquelle les produits cryptographiques anciens et vulnérables seront désactivés.

Il pourrait être impossible de migrer certains systèmes anciens de manière à utiliser la CPQ sans avoir à les remplacer entièrement. Pour atteindre les jalons fixés pour la migration, il pourrait être nécessaire d'isoler de tels systèmes sur le réseau ou de mettre en tunnel le trafic dans une couche d'encapsulation protégée par CPQ. Ces décisions devraient être prises lors de la planification de la phase de transition.

Les premières versions du plan ministériel de migration vers la CPQ peuvent fournir des détails limités sur la phase de transition. Cette section devrait toutefois être étoffée pour illustrer les progrès réalisés par rapport à la détermination.

4 Jalons et livrables

Les jalons et les livrables pour les ministères et organismes fédéraux sont les suivants :

- avril 2026 – développement d'un plan ministériel initial de migration vers la CPQ;
- début d'avril 2026 et chaque année par la suite – rapport sur les progrès réalisés relativement à la migration vers la CPQ;
- fin de 2031 – achèvement de la migration des systèmes hautement prioritaires vers la CPQ;
- fin de 2035 – achèvement de la migration des autres systèmes vers la CPQ.

Les jalons relatifs à l'achèvement de la migration sous-entendent que les algorithmes vulnérables à l'informatique quantique ont été désactivés, isolés ou mis en tunnel. Ainsi, plutôt que de se limiter à la prise en charge de la CPQ, il est possible d'atténuer la menace posée par l'informatique quantique. Il sera primordial pour les ministères et organismes de créer, de réviser et de suivre leur plan ministériel de migration vers la CPQ de manière à migrer les systèmes le plus tôt possible et à respecter les dates des jalons.

On retrouve à la section suivante de plus amples renseignements concernant les attentes en matière de rapports sur les progrès réalisés.

5 Gouvernance et coordination

5.1 Organes de gouvernance pertinents du gouvernement du Canada

Les ministères et organismes sont responsables de la gestion des risques liés à la cybersécurité dans leurs secteurs de programme. Par contre, les initiatives à l'échelle du GC, comme la présente migration vers la CPQ, exigent une approche pangouvernementale gérée au niveau de l'organisme conformément aux responsabilités décrites dans les instruments de politique du SCT.

Le comité tripartite sur la sécurité des TI est composé du SCT, de SPC et du Centre pour la cybersécurité. Le comité est un organe centralisé qui fournit des avis, des conseils, une supervision et une orientation sur les initiatives pangouvernementales en matière de cybersécurité, comme la migration du GC vers la CPQ. Le comité tripartite soutient les ministères et organismes conformément aux pouvoirs qui lui ont été conférés par le SCT.

Le Conseil d'examen de l'architecture intégrée du gouvernement du Canada (CEAI GC) fournit un mécanisme de gouvernance pour évaluer si les systèmes d'entreprise proposés s'inscrivent dans le cadre de l'architecture d'entreprise du GC. Le cadre permet de s'assurer que les domaines des architectures organisationnelles, d'information, des applications, des technologies, de la sécurité et de la protection de la vie privée sont conformes à l'architecture intégrée cible des services et du numérique. Les exigences liées à la cybersécurité, comme la conformité aux recommandations du Centre pour la cybersécurité en matière de cryptographie, font partie de l'architecture intégrée cible du GC, qui s'aligne avec l'orientation stratégique globale du SCT et aux instruments de politique du SCT.

Le GC a mis en place des comités de coordination ministériels de la science et des technologies quantiques au niveau des cadres supérieures et supérieurs afin de synchroniser les efforts déployés et d'assurer le leadership du Canada dans ce domaine. Ces comités supervisent les mesures prises par le gouvernement fédéral pour soutenir la Stratégie quantique nationale du Canada (SQN), y compris la feuille de route de la SQN sur les communications quantiques et la cryptographie post-quantique.

5.2 Rapports sur les progrès réalisés

Il est essentiel de suivre les progrès de la migration du GC vers la CPQ pour assurer une supervision et une gouvernance efficaces. Il sera ainsi possible d'assurer la responsabilisation et de franchir les étapes. Le SCT supervise la conformité à ses instruments de politique conformément au Cadre stratégique sur la gestion de la conformité du Conseil du Trésor. Il suit également les progrès réalisés par rapport au plan ministériel sur les services et le numérique, ce qui comprend la cybersécurité, comme l'exige la *Politique sur les services et le numérique*. Il est impératif de faire rapport des progrès réalisés par le ministère et des activités nécessaires à la migration vers la CPQ. Ces rapports seront recueillis par le SCT dans le cadre de la soumission annuelle des plans ministériels sur les services et le numérique.

5.3 Ressources supplémentaires et soutien

La plateforme GCéchange sera utilisée pour mettre en commun les artéfacts avec les ministères et organismes fédéraux et faciliter la migration vers la CPQ. Le Centre pour la cybersécurité continuera de publier des conseils et des recommandations à l'intention des organismes sur le site Web du Centre pour la cybersécurité.

Veuillez utiliser les coordonnées du Centre pour la cybersécurité qui se trouvent au haut de cette page pour demander de plus amples renseignements sur la menace quantique, la CPQ ou la présente feuille de route.