FINAL v1.0 Approbation du CEAI GC 2018-03-22

Gouvernement du Canada

Rôles et responsabilités en matière d’informatique en nuage

27 septembre 2022

Sommaire

L’informatique en nuage a le potentiel d’offrir un moyen flexible de fournir des services de systèmes d’information et offre un modèle de prestation de services optionnels permettant au GC de soutenir son programme de transformation numérique. L’adoption de l’informatique en nuage peut aider le GC à maintenir l’excellence de ses services d’information dans une période où les Canadiens demandent de plus en plus de services en ligne et de renseignements exacts en temps opportun. Cette évolution aura une incidence sur la façon dont nous nous procurons, sécurisons et utilisons les systèmes d’information qui soutiennent les programmes et services du GC et des ministères.

Il faut veiller à atténuer les risques liés à l’utilisation des services infonuagiques. L’adoption de ce modèle nécessitera une diligence raisonnable et une prudence de la part du GC dans la sélection du fournisseur de services infonuagiques (FSI) approprié, ainsi qu’une délimitation claire des rôles et responsabilités entre le GC et le FSI pour la mise en œuvre, l’exploitation et le maintien des contrôles de sécurité qui soutiennent les obligations du GC en matière de protection des données et de la confidentialité. Des rôles et des responsabilités clairs doivent également être définis au sein du CG afin de garantir une utilisation rentable et gérée des risques de l’informatique en nuage pour soutenir la prestation des programmes et des services.

Afin d’assurer une utilisation rentable et gérée des risques de l’informatique en nuage pour soutenir la prestation des programmes et des services, le présent document décrit les rôles et les responsabilités des divers acteurs du GC qui participeront à la gouvernance, à la planification, à l’orchestration, à la mise en œuvre, à l’exploitation et à la maintenance des services informatiques en nuage.

Historique des révisions

|  |  |  |
| --- | --- | --- |
| N° de la version du document | Modifications | Date |
| 0.1 | Projet initial préparé par la DDPI du SCT, Cyber Sécurité. | 29 septembre 2017 |
| 0.2 | Mise à jour sur la base des commentaires reçus de l’équipe de Cloud Ninja et de la consultation du groupe de travail sur l’informatique en nuage du GC | 27 novembre 2017 |
| 0.3 | Transfert de la DDPI du SCT Cyber à la DDPI-DTI du SCT | 10 décembre 2017 |
| 0.4 | Mise à jour pour tenir compte du CE en informatique en nuage du GC comme groupe de travail et la description associée | 19 décembre 2017 |
| 0.5 | Approuvé par le CEAI GC | 22 mars 2018 |
| 2.0 | Transduction et les barrières de sécurité | 27 sept 2022 |

Table des matières

[1. Introduction 1](#_Toc114841909)

[1.1 Contexte 1](#_Toc114841910)

[1.2 Objectif du document 1](#_Toc114841911)

[1.3 Destinataires 2](#_Toc114841912)

[1.4 Définitions des termes clés 2](#_Toc114841913)

[2. Contexte 3](#_Toc114841914)

[2.1 Responsabilité partagée 3](#_Toc114841915)

[2.2 Profils de l’informatique en nuage du GC 4](#_Toc114841916)

[2.3 Mise en œuvre de services infonuagiques 6](#_Toc114841917)

[3. Intervenants de l’informatique en nuage 8](#_Toc114841918)

[3.1 Portée du GC 8](#_Toc114841919)

[3.2 Portée ministérielle 10](#_Toc114841920)

[4. Matrice des responsabilités de l’informatique en nuage du GC 13](#_Toc114841921)

[5. Références 15](#_Toc114841922)

Liste des tableaux

[Tableau 3— 1 Intervenant de l’informatique en nuage - Portée du GC 8](#_Toc114841923)

[Tableau 3— 2 Intervenant de l’informatique en nuage - Portée ministérielle 10](#_Toc114841924)

[Tableau 4— 1 Matrice RACI de l’informatique en nuage du GC — Vue d’ensemble 13](#_Toc114841925)

Liste des figures

[Figure 2— 1 Champ de responsabilité 4](#_Toc114841926)

[Figure 2— 2 Portée des profils d’informatique en nuage du GC 5](#_Toc114841927)

[Figure 2— 3 Modèle théorique de partage de la responsabilité de la mise en œuvre et des opérations 7](#_Toc114841928)

Liste d’abréviations et d’acronymes

|  |  |
| --- | --- |
| DPI | Directeur principal de l’information |
| DDPI | Direction du dirigeant principal de l’information |
| DSIC | Direction de la sécurité industrielle du Canada |
| CST | Centre de sécurité des télécommunications |
| FSI | Fournisseur de services infonuagiques |
| SDSM | Sous-direction de la sécurité ministérielle |
| AI | Architecture intégrée |
| ASI | Architecture de sécurité intégrée |
| GC | Gouvernement du Canada |
| IaaS | Infrastructure comme service |
| GIJIA | Gestion de l’identité, des justificatifs d’identité et de l’accès |
| TI | Technologies de l’information |
| RUF | Réseaux et utilisateurs Finaux |
| NIST  | National Institute of Standard and Technology |
| CER | Centre d’exploitation du réseau |
| PaaS | Plateforme en tant que service |
| EFVP | Évaluation des facteurs relatifs à la vie privée |
| SPAC | Services publics et Approvisionnement Canada |
| RACI | Responsable, approbateur, consulté, informé |
| GRC | Gendarmerie royale du Canada |
| SaaS | Modèle SaaS |
| CDS | Cycle de développement du système |
| IS | Ingénierie des systèmes |
| COS | Centre des opérations de sûreté |
| EDT | Énoncé des travaux |
| LVERS | Liste de vérification des exigences relatives à la sécurité |
| SPC | Services partagés Canada |
| ISS | Ingénierie de sécurité des systèmes |
| EM | Évaluation des menaces |
| SCT  | Secrétariat du Conseil du Trésor du Canada |

# Introduction

## Contexte

L’informatique en nuage a le potentiel d’offrir un moyen flexible de fournir des services de systèmes d’information et offre un modèle de prestation de services optionnels permettant au gouvernement du Canada (GC) de soutenir son programme de transformation numérique. Ce modèle alternatif de prestation de services permet aux personnes et aux organisations (ou « locataires ») d’utiliser des logiciels, du matériel et des services hébergés à l’extérieur des installations du GC et gérés par des organisations du secteur privé, y compris des logiciels (p. ex., gestion des relations avec la clientèle, etc.), des plateformes (p. ex., système d’exploitation, base de données) et des infrastructures (p. ex., serveurs, stockage et réseaux).

L’adoption de l’informatique en nuage peut aider le GC à maintenir l’excellence de ses services d’information dans une période où les Canadiens demandent de plus en plus de services en ligne et de renseignements exacts en temps opportun. Cette évolution aura une incidence sur la façon dont nous nous procurons, sécurisons et utilisons les systèmes d’information qui soutiennent les programmes et services du GC et des ministères. L’adoption de ce modèle nécessitera une diligence raisonnable et une prudence de la part du GC dans la sélection du fournisseur de services infonuagiques (FSI) approprié, ainsi qu’une délimitation claire des rôles et responsabilités entre le GC et le FSI pour la mise en œuvre, l’exploitation et le maintien des contrôles de sécurité qui soutiennent les obligations du GC en matière de protection des données et de la confidentialité. Des rôles et des responsabilités clairs doivent également être définis au sein du CG afin de garantir une utilisation rentable et gérée des risques de l’informatique en nuage pour soutenir la prestation des programmes et des services.

## Objectif du document

Le présent document décrit les rôles et les responsabilités des divers acteurs du GC qui participeront à la gouvernance, à la planification, à l’orchestration, à la mise en œuvre, à l’exploitation et à la maintenance des services du système d’informatique en nuage du GC pour soutenir la prestation des programmes et des services.

Ce document appuie également l’avis de mise en œuvre de la politique de sécurité (AMPS) pour l’utilisation sécuritaire des services infonuagiques commerciaux [1] qui aide les ministères et organismes à comprendre les exigences de la politique de sécurité du Conseil du Trésor (CT) dans le contexte de l’informatique en nuage.

## Destinataires

Ce document est destiné aux chefs d’entreprise, aux gestionnaires de TI, aux praticiens de l’IT et de la sécurité informatique, ainsi qu’aux autres intervenants de l’informatique en nuage du GC qui cherchent à tirer parti des services infonuagiques.

## Définitions des termes clés

Vous trouverez ci-dessous les définitions des termes clés utilisés dans le document. Tous les autres termes sont définis dans les références énumérées à la section 5.

|  |  |
| --- | --- |
| Service infonuagique | Tout service de système d’information fourni par un FSI. Une offre de service infonuagique peut être une infrastructure comme service (IaaS), une plateforme en tant que service (PaaS) ou un modèle SaaS. |
| Service dans le nuage | Un service de système d’information du GC qui est mis en œuvre dans un service infonuagique. La composition d’un service dans le nuage varie en fonction du modèle du service infonuagique sous-jacent : pour l’IaaS, une plateforme et une application; pour la PaaS, une application, et pour le modèle SaaS, la personnalisation et la configuration de l’application SaaS. |
| Fournisseur de services infonuagiques (FSI) | Un fournisseur commercial d’un service infonuagique. |

# Contexte

Les rôles et responsabilités du GC en matière d’informatique en nuage sont structurés autour du modèle de responsabilité partagée inhérent à l’informatique en nuage. Le document du Conseil du Trésor du Canada (SCT), [Approche et procédures de gestion des risques liés à la sécurité de l’informatique en nuage du GC](http://www.gcpedia.gc.ca/gcwiki/images/c/c7/GC_Cloud_Security_Risk_Management_Approach_and_Procedures_-_EN.pdf) [2], qui est basé sur le [cadre de gestion des risques de sécurité des TI](https://www.cse-cst.gc.ca/en/publication/itsg-33) d’ITSG-33 du Centre de la sécurité des télécommunications (CST) [: Une approche fondée sur le cycle de vie](https://www.cse-cst.gc.ca/en/publication/itsg-33) [3] souligne la responsabilité partagée dans la mise en œuvre des contrôles de sécurité avec la rigueur appropriée pour permettre l’hébergement des services du GC et des informations connexes sur des services infonuagiques fournis par des FSI commerciaux. Elle décrit également les autorités, l’approche et les procédures de gestion des risques de sécurité informatique lors de l’utilisation de services infonuagiques. Le FSI assume une certaine responsabilité en ce qui concerne l’atténuation des risques, mais les ministères et les organismes portent la responsabilité des risques. Ce modèle de responsabilité partagée est décrit dans le contexte du GC dans les sous-sections qui suivent.

## Responsabilité partagée

Les ministères doivent gérer en permanence leurs informations et leurs actifs informatiques pendant toute la durée de vie de leurs programmes et services. Dans le contexte de l’informatique en nuage, la gestion des actifs informatiques repose sur un modèle de responsabilité partagée. Le FSI assume certaines responsabilités en matière d’informatique et de sécurité informatique, mais les ministères conservent la responsabilité globale.

Figure 2— 1 une vue simplifiée des couches architecturales de l’informatique en nuage. Décrit le champ de responsabilité des consommateurs et des fournisseurs de services tel qu’il s’applique aux modèles de services infonuagiques définis dans les documents NIST 500-292 (architecture de référence infonuagique) [4] et NIST 500-299 (architecture de référence pour la sécurité de l’informatique en nuage) [5].



Figure 2‑1 Champ de responsabilité

## Profils de l’informatique en nuage du GC

La Direction du dirigeant principal de l’information (DDPI) du SCT a élaboré des profils de contrôle de la sécurité pour l’informatique en nuage. Un profil de contrôle de sécurité de base est un ensemble de contrôles de sécurité des TI qu’une organisation établit comme exigences minimales obligatoires pour ses systèmes d’information. En adhérant à un ensemble normalisé de contrôles de sécurité, les ministères peuvent cibler et évaluer les risques, et élaborer des stratégies pour les atténuer de manière appropriée.

La responsabilité de la mise en œuvre et du maintien de ces contrôles de sécurité dans ces profils est partagée entre le GC et les FSI. En fonction du modèle de service choisi, le GC, en tant que consommateur de services infonuagiques, sera responsable de la mise en œuvre de contrôles de sécurité supplémentaires, soit entièrement, soit partiellement, dans le cadre de sa part du modèle de responsabilité partagée. Figure 2‑2 donne un aperçu de la répartition de la responsabilité de la mise en œuvre des contrôles de sécurité entre le FSI et l’organisme de défense du consommateur du GC.



Figure 2‑2 Portée des profils d’informatique en nuage du GC

La nature des contrôles de sécurité qu’une organisation du GC doit mettre en œuvre dans le service infonuagique est dictée par le modèle de service sur lequel le service du système d’information est déployé. Par exemple, si le modèle de service est IaaS, l’organisation du GC doit mettre en œuvre les contrôles de sécurité plate-forme et les couches d’application de la technologique infonuagique. Il s’agit notamment des contrôles de sécurité relatifs au contrôle d’accès, à la vérification et à la responsabilité, à l’identification et à l’authentification, à la protection des systèmes et des communications, à la gestion de la configuration, aux plans d’urgence, à la réponse aux incidents, à la maintenance et à l’intégrité des systèmes et des informations. Même dans le cadre du modèle de service SaaS, l’organisation du GC doit mettre en place certains contrôles de sécurité pour gérer l’accès des utilisateurs, effectuer des vérifications et répondre aux incidents.

Le document [Profil des mesures de sécurité pour les services du GC fondés sur l’informatique en nuage](https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/cloud-computing/government-canada-security-control-profile-cloud-based-it-services.html) [6] cible les contrôles de sécurité de base dont la mise en œuvre est recommandée par les FSI et les ministères et organismes du GC, afin de protéger de façon appropriée les services infonuagiques ayant une catégorie de sécurité Protégé B, une intégrité moyenne et une disponibilité moyenne. Il documente également le contexte dans lequel ces contrôles de sécurité devraient être mis en œuvre.

## Mise en œuvre de services infonuagiques

Lors de la mise en œuvre d’un service infonuagique, l’organisation du GC responsable et le FSI de soutien sont chacun responsables de la mise en œuvre et des opérations de leur partie du service du système d’information. Cette responsabilité partagée est illustrée dans la Figure 2‑3. Cette figure met également en évidence les principaux apports. Pour le processus de cycle de vie du système, il s’agit des procédures et outils du cycle de vie du développement du système, des procédures et outils de l’ingénierie du système/de la sécurité du système, et des artefacts applicables de l’architecture intégrée/de l’architecture de sécurité intégrée. Pour le processus d’approvisionnement, les données clés comprennent des éléments tels que l’énoncé des travaux pour tout service infonuagique requis, les clauses contractuelles standard et une liste de contrôle des exigences de sécurité.



Figure 2‑3 Modèle théorique de partage de la responsabilité de la mise en œuvre et des opérations

# Intervenants de l’informatique en nuage

## Portée du GC

Cette section détermine et décrit les intervenants du GC qui ont un rôle à jouer dans le contexte de l’informatique en nuage. Les intervenants sont regroupés en fonction de l’étendue de leurs responsabilités, qui sont soit à l’échelle du GC, soit à l’échelle du ministère.

Tableau 3‑1 Intervenant de l’informatique en nuage - Portée du GC

| Intervenant | Description |
| --- | --- |
| Dirigeant principal de l’information (DPI) du GC  | Le DPI du GC a la responsabilité générale de fournir une orientation stratégique pour l’informatique en nuage afin de soutenir la prestation des programmes et des services du GC. |
| Comité d’examen de l’architecture intégrée du gouvernement du Canada (CEAI) du GC | Le CEAI du GC fournit une orientation pour les TI d’entreprise dans l’ensemble du gouvernement. Cela inclut la gestion des risques liés à l’adoption de l’informatique en nuage. Le CEAI du GC examine tous les projets d’informatique dématérialisée du point de vue de l’architecture et des risques afin de s’assurer que les risques potentiels sont correctement atténués. |
| Équipe de l’architecture intégrée (AI)/de l’architecture de sécurité intégrée (ASI) du GC | L’équipe AI/ASI du GC est responsable de l’établissement et du maintien d’un cadre d’adoption de l’informatique en nuage à l’échelle du GC. Ce cadre se compose d’artefacts architecturaux ainsi que de stratégies et d’outils spécifiques à l’informatique infonuagique pour orchestrer, simplifier et guider l’adoption de services infonuagique par les ministères et les agences.  |
| Groupe de travail sur l’informatique en nuage du GC | Le groupe de travail sur l’informatique en nuage du GC est chargé de fournir aux ministères et aux organismes des conseils et des orientations à l’échelle du GC sur l’adoption de l’informatique en nuage. Il s’agit notamment de contribuer à l’établissement du cadre d’adoption de l’informatique en à l’échelle du GC. Le groupe de travail sur l’informatique en nuage du GC est composé de représentants de diverses organisations, dont la DDPI du SCT, le CST, le SPC et le SPAC, et comprendra des experts en la matière de l’industrie et du ministère, notamment :* *Analystes de l’automatisation de l’informatique en nuage* — fournir des outils d’automatisation de l’informatique en nuage
* *Conseillers en transition vers les services* infonuagiques — fournir des conseils et une orientation en matière de migration et de transition vers l’informatique en nuage
* *Conseillers en sécurité de l’informatique en nuage* - fournir des conseils et des orientations en matière d’architecture et d’ingénierie de la sécurité de l’informatique en nuage
 |
| Services de courtage en informatique en nuage du GC,  | Le SPC, dans son rôle de courtier en informatique en nuage du GC, agira comme intermédiaire entre les FSI et les ministères et organismes qui consomment des services infonuagiques en fournissant divers types de services de courtage comme l’administration d’un marché de services infonuagiques, l’établissement de véhicules d’approvisionnement en services infonuagiques et la vérification de l’utilisation des services infonuagiques conformément aux politiques, directives et normes applicables. |
| Analystes de la chaîne d’approvisionnement et de l’assurance des produits | Les analystes de la chaîne d’approvisionnement/de l’assurance des produits sont responsables de la gestion de la chaîne d’approvisionnement et du processus d’assurance des produits pour l’acquisition de services infonuagique pour le GC. |
| Propriétaire du service de gestion de l’identité, des justificatifs d’identité et de l’accès (GIJIA) | Les propriétaires de services de GIJIA d’entreprise. Il s’agit notamment du service d’annuaire, de maCLÉ et de CléGC.  |
| Services techniques du réseau, Réseaux et utilisateurs Finaux (RUF) | Les services techniques du réseau sont responsables de la définition, de la conception et de la maintenance des interconnexions entre le GC et les environnements de services infonuagiques commerciaux afin d’assurer une accessibilité optimale des services infonuagiques par les communications internes et externes des utilisateurs finaux.  |
| Centre d’exploitation du réseau (CER) | Le CER du SPC est responsable de la surveillance centralisée du réseau pour les services dans le nuage. Le CER du SPC surveille et gère les réseaux du GC et les interconnexions des services infonuagiques et réagit aux événements. |
| Centre des activités en matière de sécurité (CAMS) : | Le CAMS du SPC est responsable des opérations de sécurité centralisées pour les services dans le nuage. Le CAMS du SPC surveille les journaux de sécurité et répond aux incidents de sécurité. Le CAMS du SPC fait office de point de contact central pour la coordination, la production de rapports et l’analyse des tendances des événements de sécurité qui ont eu ou peuvent avoir un impact sur le GC.  |
| Opérations de cyber défense | Le CST est chargé de fournir des services de surveillance et de défense contre les menaces pour le GC. |
| Évaluateurs de sécurité du GC | Les évaluateurs de sécurité sont chargés de mener des évaluations des FSI et des services infonuagiques à l’appui de l’autorisation et du maintien de l’autorisation, et dans le cadre du processus de validation de l’assurance par un tiers. |
| Direction générale des approvisionnements | La Direction générale des approvisionnements de Services publics et Approvisionnements Canada (SPAC) offre des conseils et du soutien pour aider les ministères et organismes du gouvernement fédéral à atteindre leurs objectifs en matière d’approvisionnement. |
| Programme de sécurité industrielle | Le programme de sécurité industrielle de SPAC est responsable de la validation de la conformité des entrepreneurs aux exigences de sécurité du contrat. La validation couvre la sécurité physique, la sécurité du personnel et la sécurité des systèmes d’information. |
| Conseillers en sécurité physique | Les conseillers en sécurité physique contribuent à l’établissement et à la maintenance du cadre d’adoption de l’informatique en nuage à l’échelle du GC en fournissant des conseils et des orientations sur la sécurité physique des installations infonuagiques. |

## Portée ministérielle

La section suivante détermine et décrit les intervenants ministériels qui ont un rôle à jouer dans le contexte de l’informatique en nuage. Toutefois, si l’étendue des responsabilités décrites concerne les ministères, les mêmes responsabilités pourraient être appliquées pour une organisation fournissant une entreprise ou un service commun.

Tableau 3‑2 Intervenant de l’informatique en nuage - Portée ministérielle

| Intervenant | Description du rôle dans le contexte de l’informatique en nuage |
| --- | --- |
| Administrateur général | L’administrateur général a la responsabilité globale de l’utilisation rentable et gérée par les risques des services infonuagiques pour soutenir la prestation des programmes et des services du ministère. |
| DPI | Le DPI est responsable de l’établissement et du maintien d’une structure de gouvernance ministérielle et d’un cadre d’adoption de l’informatique en nuage pour la mise en œuvre de services dans le nuage afin de soutenir la prestation de programmes et de services ministériels.  |
| Coordinateur de la sécurité des TI | Le coordinateur de la sécurité des TI est responsable de la coordination générale des activités de sécurité dans l’ensemble du ministère afin de garantir une mise en œuvre et une maintenance des services dans le nuage axées sur les risques. Le coordinateur de la sécurité de TI est également responsable de l’évaluation de la sécurité et des activités de surveillance continue. |
| Propriétaires d’entreprise (gestionnaires de programmes et de prestation de services) | Les propriétaires d’entreprises s’appuieront sur des services dans le nuage pour fournir leurs programmes et services. En collaboration avec les propriétaires des données, ils sont chargés de fournir leurs besoins et leurs exigences commerciales, y compris en matière de sécurité, aux concepteurs de services infonuagiques. Parce qu’ils sont responsables des risques qui y sont liés, les propriétaires d’entreprises sont tenus d’autoriser l’exploitation des services infonuagiques qui soutiennent leurs programmes et services. |
| Responsables de la protection de la confidentialité | Les responsables ministériels de la protection de la confidentialité sont chargés de conseiller les propriétaires d’entreprises et les concepteurs de services infonuagiques afin de garantir la conformité des services infonuagiques avec les règles de protection de la confidentialité. |
| Architecte d’entreprise | Les architectes d’entreprise (y compris les architectes de l’informatique en nuage et les architectes de la sécurité d’entreprise) sont responsables de l’établissement et de la maintenance d’un cadre d’adoption de l’informatique en nuage à l’échelle du ministère, conformément au cadre d’adoption de l’informatique en nuage à l’échelle du gouvernement. Les architectes d’entreprise collaborent également avec les concepteurs de services infonuagiques pour garantir la conformité de ces services aux artefacts architecturaux.  |
| Concepteurs et développeurs de services infonuagiques | Les concepteurs et développeurs de services infonuagiques sont responsables de la conception, du développement, de l’intégration, des tests, du déploiement et de la maintenance des services infonuagiques. Les concepteurs et les développeurs de services infonuagiques prennent en compte les besoins et les exigences de l’entreprise et travaillent avec des architectes d’entreprise, des conseillers en confidentialité, des analystes de sécurité et des évaluateurs de sécurité pour mettre en œuvre des services infonuagiques fiables.  |
| Analyste de l’automatisation de l’informatique infonuagique | Les analystes de l’automatisation de l’informatique infonuagique sont des experts en la matière qui sont responsables du développement et de la maintenance de l’automatisation de l’informatique infonuagique traitée pour être utilisée dans les services dans nuage dans le cadre d’un ministère.  |
| Analystes de sécurité | Les analystes de sécurité sont chargés de fournir un soutien en matière d’ingénierie de la sécurité des systèmes aux concepteurs et développeurs de services infonuagiques et d’assurer la liaison avec les évaluateurs de sécurité.  |
| Évaluateurs de sécurité | Les évaluateurs de sécurité sont chargés de mener des évaluations de sécurité des services basés sur l’informatique en nuage afin de soutenir l’autorisation et la surveillance et l’évaluation continues de la sécurité. |
| Propriétaires de services dans le nuage | Les propriétaires de services dans le nuage ont la responsabilité globale de la mise en œuvre, de l’exploitation et de la maintenance des services dans le nuage. |
| Opérateurs et administrateurs de services infonuagiques | Les opérateurs et administrateurs de services infonuagiques sont responsables des opérations et de l’administration quotidiennes des services dans le nuage.  |
| Opérations en matière de sécurité | Les opérations en matière de sécurité sont responsables des opérations de sécurité centralisées pour les services dans le nuage. Les opérations de sécurité surveillent les journaux de sécurité et répondent aux incidents de sécurité. |
| Bureau des services de TI | Le Bureau des services de TI est chargé de fournir une assistance de première ligne pour les services dans le nuage. |
| Auditeurs de services dans le nuage | Les auditeurs des services dans le nuage sont chargés de vérifier les activités d’utilisation des services dans le nuage conformément aux politiques, directives et normes applicables.  |

# Matrice des responsabilités de l’informatique en nuage du GC

Les responsabilités des intervenants de l’informatique en nuage du GC sont décrites dans une matrice RACI détaillée, qui peut être consultée en cliquant sur le lien suivant :

[Dépôt de fichiers du groupe de travail GC Connex de l’informatique en nuage du GC](https://gcconnex.gc.ca/file/view/37162556/gc-public-cloud-raci-matrix-v1?language=en)

Le tableau ci-dessous résume la matrice RACI par domaine de responsabilité et par les différentes entités du GC, y compris les ministères et les organismes.

Tableau 4‑1 Matrice RACI de l’informatique en nuage du GC - Vue d’ensemble

R = Responsable, A = Approbateur, C = Consulté, I = Informé

| **Sect.** | Rôles**Résumé des responsabilités de haut niveau** |  **DDPI du SCT** |  **SPC** |  **CST** |  **SPAC** |  **GRC** |  **Ministères et agences**  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Établir une gouvernance de l’informatique en nuage à l’échelle du GC | **A,R** | **C** | **C** | **C** | **C** | **C** |
| 2 | Établir un cadre d’adoption de l’informatique en nuage à l’échelle du GC | **A,R** | **C** | **C** | **C** | **C** | **C** |
| 3 | Établir une garantie de sécurité par un tiers | **C** | **C** | **A,R** | **C** | **C** | **C** |
| 4 | Acquérir des services infonuagiques commerciaux | **C** | **A,R** | **C** | **A,R** | **C** | **C** |
| 5 | Fournir des services de courtage en informatique en nuage du GC | **C** | **A,R** | **C** | **C** | **C** | **C** |
| 6 | Fournir des services d’intégration de réseaux aux services infonuagiques | **C** | **A,R** | **C** |  |   | **C** |
| 7 | Fournir la GIJIA aux services dans le nuage | **C** | **A,R** | **C** |  |   | **C** |
| 8 | Fournir un soutien à la mise en œuvre et au fonctionnement aux ministères | **C** | **A,R** | **R** |  |  | **C** |
| 9 | Surveiller l’exploitation de l’informatique en nuage à l’échelle du GC | **C** | **A,R** | **C** |  |   | **C** |
| 10 | Établir une gouvernance ministérielle pour les services dans le nuage | **C** | **C** | **C** |  |  | **A,R** |
| 11 | Établir un cadre ministériel d’adoption de l’informatique en nuage | **C** | **C** | **C** |  |  | **A,R** |
| 12 | Mettre en œuvre des services dans le nuage | **C** | **C** | **C** |  |  | **A,R** |
| 13 | Exploitation et maintenance des services dans le nuage | **I** | **C** | **C** |  |   | **A,R** |
| 14 | Surveiller les opérations d’exploitation de l’informatique en nuage des ministères | **I** | **C** | **C** |  |   | **A,R** |
| 15 | Effectuer une surveillance continue des services dans le nuage | **I** | **C** | **C** |  |   | **A,R** |

# Références

|  |  |
| --- | --- |
| [1]  | Treasury Board of Canada Secretariat, “Security Policy Implementation Notice (SPIN) for the Secure Use of Commercial Cloud Services,” October 2017. |
| [2]  | Treasury Board of Canada Secretariat, “Cloud Security Risk Management Approach and Procedures,” Version 1.0, 20 July 2017. |
| [3]  | Communications Security Establishment (CSE), “IT Security Risk Management: A Lifecycle Approach (ITSG-33),” November 2012. |
| [4]  | National Institute of Standards and Technology, “NIST Cloud Computing Reference Architecture (SP 500-292),” September 2011. |
| [5]  | National Institute for Standards and Technology, “NIST Cloud Computing Security Reference Architecture [SP 500-299],” Draft, 2013. |
| [6]  | Treasury Board of Canada Secretariat, “GC Security Control Profile for Cloud-based IT Services—PBMM,” November 2016. |
| [7]  | Treasury Board of Canada Secretariat, “GC Cloud Adoption Strategy,” DRAFT, December 2015. |
| [8]  | Treasury Board of Canada Secretariat, “Government of Canada Cyber Security Event Management Plan (GC CSEMP),” August 2015. [Online]. Available: https://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/atip-aiprp/sim-gsi/msi-gis/csemp-pgec-eng.asp. |
| [9]  | National Institute of Standards and Technology (NIST), “[SP800-53, Rev4] Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4,” April 2013. |
| [10]  | National Institute of Standards and Technology, “NIST Special Publications, SP800s—Computer Security,” [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html#SP 800. |
| [11]  | National Institute of Standards and Technology, “Guide for Applying the Risk Management Framework to Federal Information Systems [SP800-37],” February 2010. |
| [12]  | National Institute of Standards and Technology, NIST Cloud Computing Reference Architecture (Special Publication 500-292),” September 2011. |
| [13]  | National Institute of Standards and Technology, “NIST Cloud Computing Security Reference Architecture (Special Publication 500-299),” DRAFT. |
| [14]  | National Institute of Standards and Technology, “Assessing Security and Privacy Controls in Federal Information (Special Publication 800-53A Revision 4),” December 2014. |
| [15]  | US Government, “Federal Risk and Authorization Program (FedRAMP)”. |
| [16]  | Treasury Board of Canada Secretariat, “Government of Canada Strategic Reference Model,” [Online]. Available: https://tbs-sct.gc.ca/it-ti/itr-rti/srm-mrs-eng.asp. |
| [17]  | National Institute of Standards and Technology, “[SP 800-137] Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,” September 2011. |
| [18]  | T. B. o. C. Secretariat, “Directive on Privacy Impact Assesssment,” April 2010. |
| [19]  | Communications Security Establishment, “Security Considerations for the Contracting of Public Cloud Computing Services (ITSB-105),” December 2014. |