



Secrétariat du Conseil du Trésor  
du Canada

Treasury Board of Canada  
Secretariat

Canada

# Plan stratégique de la GI/TI du gouvernement du Canada de 2017 à 2021 et Stratégie d'adoption de l'informatique en nuage mise à jour

Présentation au Conseil de dirigeants principaux de  
l'information du secteur public (CDPISP)

Le 5 octobre 2017, Charlottetown, Île-du-Prince-Édouard

Denise Gomes

Directrice principale, Priorités et planification de la TI



CANADA 150  
1867-2017

# Contexte

---

- Le premier Plan stratégique de la TI du GC a été publié en juin 2016
  - Il présentait l'orientation de toute l'organisation en matière de TI.
  - Il a créé des liens entre les priorités et les stratégies du GC et les plans ministériels de la TI.
  - Il s'engageait à la présentation d'un compte rendu annuel et à un rapport d'étape à la secrétaire à l'automne de 2017.

# But

- Une version à jour du Plan stratégique de la GI/TI du GC de 2017 à 2021 sera publiée en octobre.
  - Il s'agit d'une étape intérimaire à une politique et une stratégie sur le numérique qui sont en cours d'élaboration pour 2018-2019.
  - Elle décrit les mesures stratégiques visant à renforcer le fondement de la GI/TI et à positionner le GC en vue de changer sa perspective pour le numérique.
  - Réalise l'orientation présentée dans la lettre de décision du Conseil du Trésor à Services partagés Canada (SPC) en date de mai 2017 :
    - [Traduction] « Que le SCT présente un Plan stratégique de la TI du gouvernement du Canada tous les mois d'octobre dans lequel il décrit les priorités du gouvernement et qui sert de fondement à la planification de SPC, notamment à son Plan d'investissement annuel. »
- Fixe l'orientation de la GI/TI pour le GC et détermine les priorités organisationnelles et les principales activités des ministères, des organismes et des fournisseurs de services.
  - Des données d'entrée principales à notre processus de planification de la TI ministérielle en tant qu'élément du Cadre d'établissement des priorités utilisé pour déterminer l'ensemble des investissements en matière de GI/TI ainsi que les priorités de travail lié à la GI/TI pour le GC.
- Les ministères et organismes devraient utiliser ce document pour établir les priorités internes en matière d'investissements et des initiatives en matière de GI/TI, et démontrer l'harmonisation avec l'orientation organisationnelle.
- Pour les organisations qui fournissent des services, il cerne les priorités et les activités de base qui sont nécessaires pour moderniser la prestation de services et améliorer la durabilité.

# Changements et ajouts depuis juin 2016

- Perspective sur l'orientation numérique établie par le GC.
- Répond à la rétroaction fournie dans le cadre des consultations auprès :
  - Du public au cours de l'été et de l'automne 2016.
  - Les collectivités des dirigeants principaux de l'information (DPI) et des cadres supérieurs responsables de la gestion de l'information (CSGI) du GC en février 2017.
- Principaux changements :
  - Élimine les écarts relevés dans le cadre des consultations publiques dans les domaines de l'accessibilité, des sources ouvertes et de l'approvisionnement.
  - Renforce les énoncés de problème et approfondit l'argument en faveur du changement.
  - Répond aux messages clés de la collectivité de la GI/TI du GC que la TI appuie la GI, qui doit à son tour appuyer les activités.
  - Intègre les orientations de la lettre de décision du Conseil du Trésor.

Cette version rassemble les facteurs habilitants de base de l'information, des données, de la technologie et de la sécurité qui sont nécessaires pour réaliser un gouvernement ouvert et transparent et offrir des services améliorés aux Canadiens.

# Vision et facteurs déterminants

## Vision

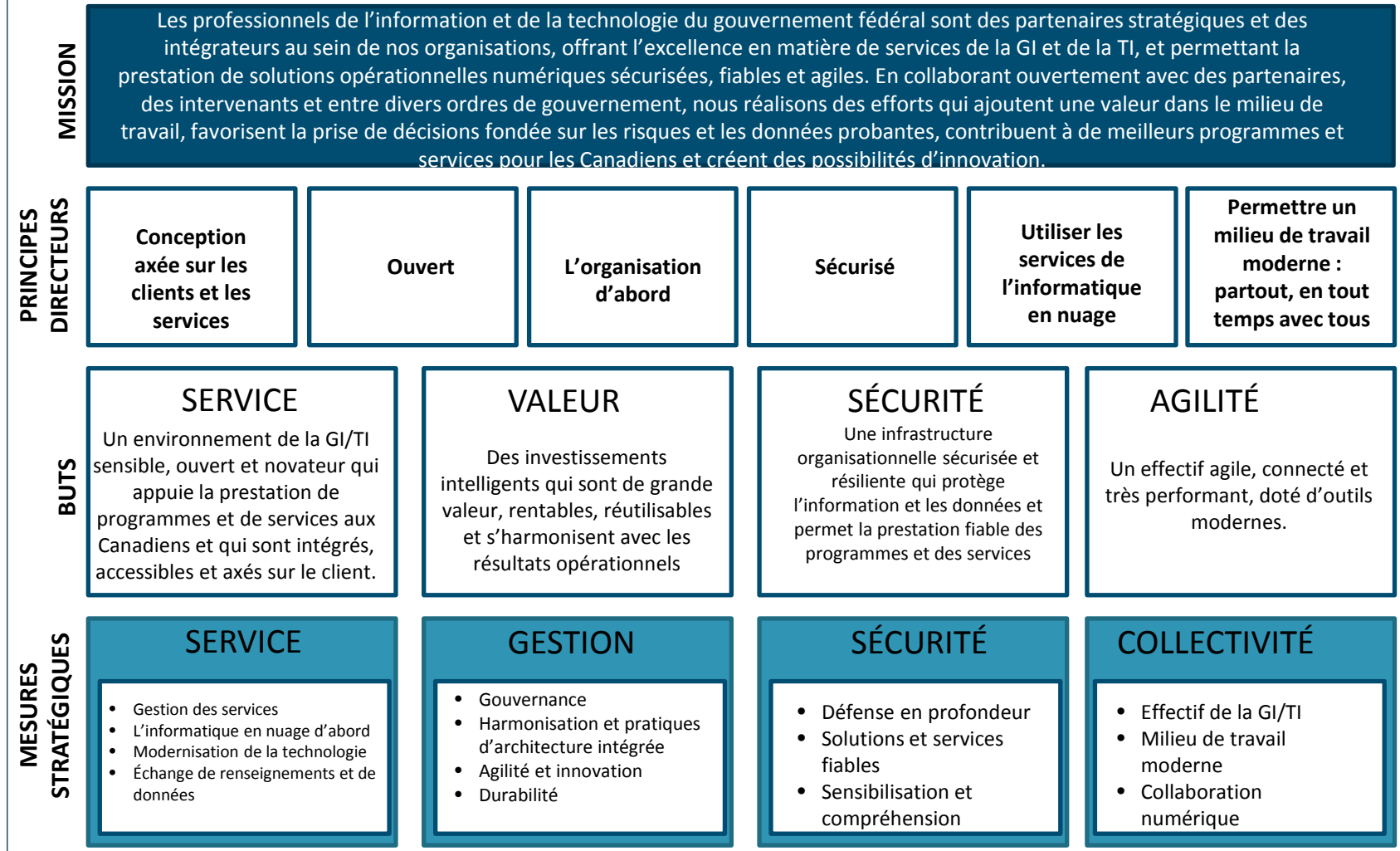
**Le gouvernement du Canada est une organisation ouverte et axée sur le service qui offre des programmes et des services aux citoyens et aux entreprises de manière simple, moderne et efficace optimisée pour le numérique – disponibles en tout temps, n'importe où et à partir de n'importe quel appareil.**

## Facteurs déterminants

- Attentes des citoyens
- Évolution du milieu de travail et de l'effectif
- Vie privée et sécurité
- Approche organisationnelle
- Durabilité de la GI/TI et IT vieillissante

# Cadre général

## CADRE GÉNÉRAL – PLAN STRATÉGIQUE EN MATIÈRE DE GI/TI



# Principes directeurs

Les principes guident la prise de décisions et la mise en œuvre

1

## Conception axée sur le client et les services

- Les solutions et les services du gouvernement du Canada sont conçus d'un point de vue de la prestation de services numérique axée sur les clients et de bout en bout afin d'accroître la valeur qu'ils offrent aux clients.

2

## Ouvert

- Les renseignements et les données du gouvernement du Canada sont ouverts par défaut.

3

## L'organisation d'abord

- Les ministères et organismes suivront des normes, des approches et une orientation communes et utiliseront les actifs existants de l'organisation (processus, données, contrats, solutions etc.) comme accélérateurs.

4

## Sécurisé

- L'information du gouvernement du Canada est sécurisée pour assurer la sécurité, la protection des renseignements personnels, la confidentialité, contrôlée pour empêcher les fuites et protégée pour les générations futures.

5

## Utiliser les services de l'informatique en nuage

- Les ministères et organismes étudieront les services informatiques en nuage Anything as a Service (XaaS) avant de développer des solutions internes

6

## Permettre un milieu de travail moderne : partout, en tout temps, avec tous

- Le gouvernement du Canada cherche à être une organisation novatrice.

# Buts stratégiques

Les buts présentent des secteurs d'intérêts et décrivent des résultats de niveau élevé

- Un environnement de la GI/TI sensible, ouvert et novateur qui appuie la prestation de programmes et de services aux Canadiens et qui sont intégrés, accessibles et axés sur le client.

Service



- Des investissements intelligents qui sont de grande valeur, rentables, réutilisables et s'harmonisent avec les résultats opérationnels.

Valeur



- Une infrastructure organisationnelle sécurisée et résiliente qui protège l'information et les données et permet la prestation fiable des programmes et des services.

Sécurité



- Un effectif agile, connecté et très performant, doté d'outils modernes.

Agilité





# Mesures stratégiques

- Les priorités pour 2018-2019 sont des éléments clés qui permettent de passer à la prestation de services numériques.

Priorité (Responsable)	Mesures stratégiques	Aperçu
Stabiliser les systèmes existants (SSC)	6, 35	Les activités requises pour rendre l'infrastructure évolutive et réduire les risques liés à la TI vieillissante, y compris la transformation des services de courriel.
La stratégie ministérielle sur les applications et le plan pour le regroupement des centres de données et l'adoption de l'informatique en nuage (ministères et SPC).	4, 7	Pour appuyer le regroupement des centres de données et l'adoption de l'informatique en nuage, les ministères ont besoin d'une stratégie et d'un plan qui facilitera la transition des applications opérationnelles des centres de données existants vers de nouveaux environnements.
Gestion des services (SPC, Services publics et Approvisionnement Canada (SPAC)	1, 2, 3	Mise en œuvre des processus de gestion des services et des jeux d'outils pour assurer l'uniformité entre les ministères et améliorer la prestation de services de bout en bout.
Interopérabilité au sein du GC (SCT-Direction du dirigeant principal de l'information [DDPI])	11	Parmi les résultats attendus tirés de l'interopérabilité améliorée, notons : un flux d'information ininterrompu entre les administrations; une optimisation des coûts grâce à la réutilisation; une sensibilité et une agilité accrues; et une présentation de rapports améliorée.
Migration au service de gestion de l'identité et des justificatifs en matière d'accès (GIJA) du GC (SCT-DDPI, SPC)	22	Offre une solution pangouvernementale qui réduira les coûts, améliorera l'expérience et l'efficacité des utilisateurs finaux, améliorera la posture de sécurité générale des réseaux, des systèmes et des applications du GC, et offrira un meilleur contrôle de la protection des renseignements personnels. La GIJA du GC sera mise en œuvre au moyen d'une approche par étapes, étalée sur plusieurs années.
Gouvernement ouvert (SCT-DDPI)	63, 73	La Politique sur le gouvernement ouvert vise à rendre le gouvernement plus accessible à tous. Cela signifie que le public canadien et le milieu des affaires auront la possibilité d'accéder plus facilement aux données et à

# Prochaines étapes

- Publier la version mise à jour à partir du site Canada.ca en octobre.
- Mener des discussions sur le passage au numérique
  - L'ébauche du Plan stratégique sera communiquée aux DPI, aux cadres supérieurs de la gestion de l'information (CSGI) et aux chefs de la TI par l'entremise de GCconnex :  
<https://gcconnex.gc.ca/groups/profile/20866369/gc-it-strategic-plan-plan-strategique-de-la-ti-du-gc>
  - Atelier d'une journée – le mercredi 18 octobre 2017
    - Faire évoluer le Plan stratégique pour appuyer et activer le numérique
- Nouvelle conception et mise à jour du Plan stratégique pour 2018-2019
  - Inclure la rétroaction de l'atelier
  - Faire évoluer la nouvelle Stratégie du numérique et l'harmoniser avec la nouvelle Politique sur le numérique
  - Mobiliser des intervenants à une plus large échelle
- Rédiger un rapport à l'intention de la secrétaire sur le Plan stratégique de la TI de 2016

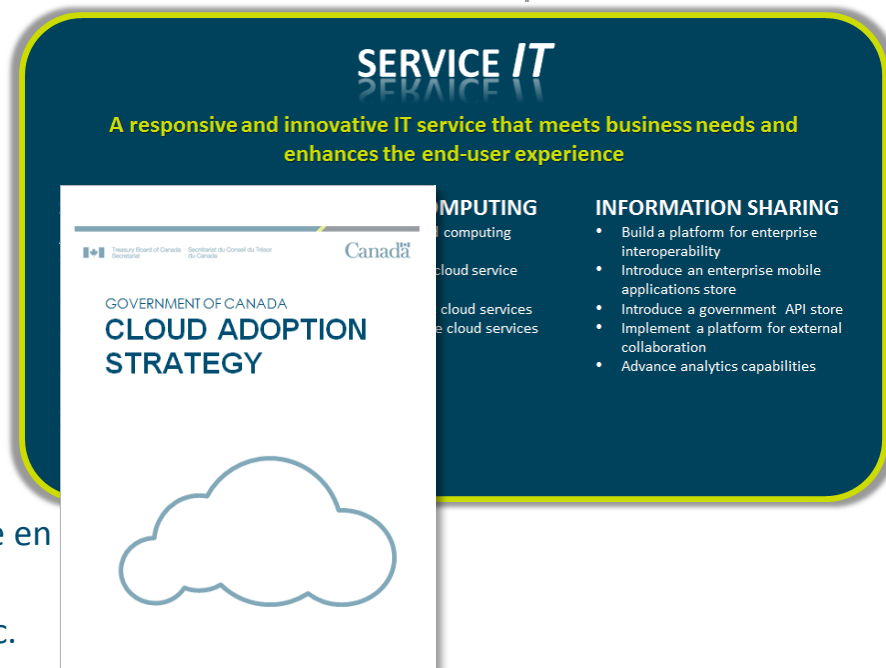


# Stratégie d'adoption de l'informatique en nuage du GC

# Une sous-composante du Plan stratégique de la TI du GC

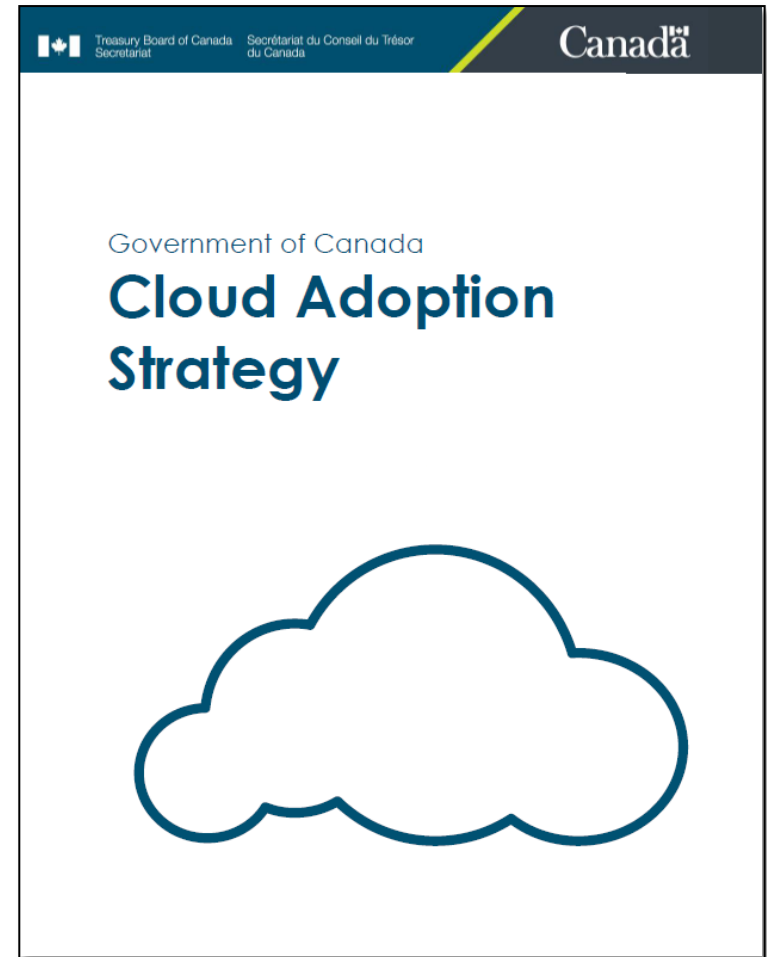
## *Le Plan stratégique de la technologie de l'information du gouvernement du Canada 2016-2020*

- Décrit les mesures stratégiques pour positionner le gouvernement afin de gérer et d'utiliser la TI comme actif organisationnel stratégique, de façon agile et novatrice, afin d'offrir une meilleure valeur aux programmes et services gouvernementaux.
- **Principe directeur n° 3 :**
  - Utilisation accrue des services d'informatique en nuage
- **Actions du plan stratégique concernant l'informatique en nuage**
  - Tous les ministères
    - Adopter les services d'informatique en nuage.
  - SPC
    - Établir un service de courtage pour l'informatique en nuage.
    - Offrir des services d'informatique en nuage public.
    - Offrir des services d'informatique en nuage privé.

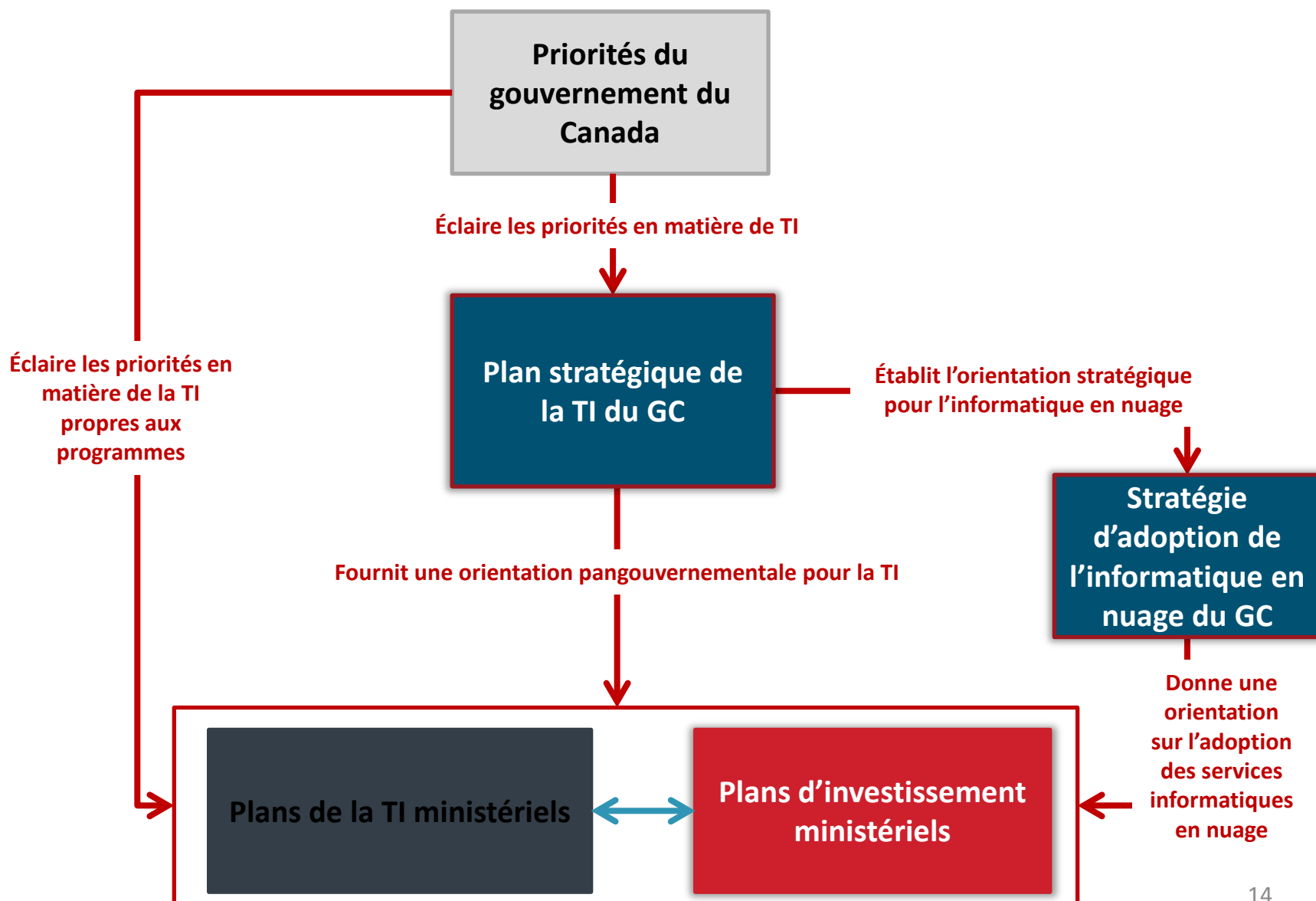


# Stratégie d'adoption de l'informatique en nuage de 2017\*

- Ajout de l'informatique en nuage hybride et de l'informatique en nuage communautaire.
- Ajout d'un énoncé d'orientation pour l'informatique en nuage d'abord.
- Approfondissement des exigences de résidence des données pour le stockage de renseignements de nature délicate.
- Ajout d'une stratégie de sortie comme principe directeur avant d'utiliser les services d'informatique en nuage.
- Précision des rôles et responsabilités entre le SCT, SPC, SPAC et les ministères
- Autres mises à jour et clarifications diverses



# Relations entre le *Plan stratégique de la TI du GC*, le Plan d'investissement de SPC et la *Stratégie d'adoption de l'informatique en nuage du GC*



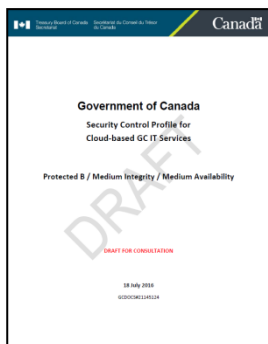
# Comment le GC s'est préparé à l'informatique en nuage

*Le SCT a publié des documents d'orientation et met sa politique à jour :*



**Stratégie d'adoption de l'informatique en nuage du Gouvernement du Canada** : Découvrez comment le gouvernement du Canada maximisera les avantages découlant de l'adoption de l'informatique en nuage tout en assurant la confidentialité des données des Canadiens et des Canadiennes, et la protection de leurs renseignements personnels.

**Guide de sélection du nuage approprié du gouvernement du Canada pour les services de la TI en nuage** : Déterminer les charges de travail appropriées pour l'informatique en nuage et la façon de considérer les modèles de déploiement



**Profil de contrôle de la sécurité de l'informatique en nuage du gouvernement du Canada** : Une approche de gestion du risque robuste qui garantira que les contrôles de sécurité appropriés du gouvernement du Canada sont en place.

# Qu'est-ce que l'avenir nous réserve?

**Orientation relative à la résidence des données électroniques (Avis de mise en œuvre de la Politique sur la technologie de l'information [AMPTI])**

**Direction for Secure-Use of Commercial-Cloud-Services<sup>¶</sup>**  
**Security-Policy-Implementation-Notice (SPIN)<sup>¶</sup>**

SPIN No. 2017-2005  
 Date: **March 20, 2017**

1. Purpose	1/5
2. Scope	1/5
3. Effective Date	1/5
4. Application	1/5
5. Context	1/5
6. Direction	1/5
6.1 → Risk Management	1/5
6.2 → Information Management Asset Protection	1/5
6.3 → Security Operations, Management and Organization	1/5
6.4 → Security Operations	1/5
6.5 → Continuous Monitoring	1/5
7. Enquiries	1/5
8. References	1/5
8.1 → Legislation	1/5
8.2 → Non-legislative instruments	1/5
8.3 → Additional references	1/5
9. Additional Guidance	1/5
9.1 → GC References	1/5
9.2 → Other References	1/5
10. Definitions	1/5
11. Appendix: Roles and Responsibilities	1/5
Page Break	1/5

**Livre blanc sur la résidence et le contrôle des données**

**Orientation pour l'utilisation sécuritaire des services d'informatique en nuage commerciaux (avis de mise en œuvre de la Politique sur la sécurité [AMOPS])**

## **Direction for Electronic Data Residency<sup>¶</sup>** **IT Policy Implementation Notice (ITPIN)<sup>¶</sup>**

ITPIN No. 2017-016  
 Date: **August 14, 2017**

The purpose of this ITPIN is to direct departments and agencies on the control, access and ownership of Government of Canada (GC) electronic data.

This ITPIN is effective as of **August 14, 2017**, and all initiatives, procurement, projects and services that require the storage or transmission of Protected B, Protected C and classified GC electronic data must be in full compliance with this ITPIN as of the effective date. All existing initiatives, procurement, projects and services requiring the storage or transmission of Protected B, Protected C and classified GC electronic data must be in full compliance with this ITPIN as of the effective date. Full compliance with this ITPIN is required for all electronic data that is stored or transmitted by the Government of Canada, including data that is stored or transmitted by the Government of Canada in the cloud.

This ITPIN applies to departments as defined in section 2 of the Financial Administration Act unless otherwise excluded by other acts, regulations or orders in council.

The heads of the following organizations are solely responsible for monitoring and ensuring compliance with this ITPIN within their organizations:

- Office of the Auditor General
- Office of the Chief Electoral Officer
- Office of the Commissioner of Labour of Canada
- Office of the Commissioner of Official Languages
- Office of the Public Sector Integrity Commissioner of Canada
- Office of the Information and Privacy Commissioner of Canada

**Background**

The GC stores and moves its electronic data through distributed computing networks and GC-approved computing facilities located both within Canada and internationally. The location and movement of the data is subject to various international, national and local laws and regulations.

Data residency refers to the physical or geographic location of the data while stored and to access it.

Based on the *Government of Canada Cloud Adoption Strategy*, the provision of the GC of cloud computing services has and will continue to amplify the use of data residency.

In recognition of this, the Government of Canada is providing this ITPIN to clarify the data residency requirements for the operations of the GC and must be enforced to maintain the security and integrity of the GC's information. The ITPIN is intended to provide guidance to the GC on the requirements for the storage and movement of its electronic data, particularly through departments with an information security or privacy mandate or a government or contractual obligation with commercial suppliers. Failure to fully implement GC data residency obligations could result in security and privacy breaches, impairment of GC

## **Data sovereignty and data residency White Paper**

**Background**

Cloud computing is a model that supports the delivery of computing services over the internet ("the cloud"). Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations, including applications (e.g. email, customer relationship management, and accounting software), platforms (e.g. website architecture) and infrastructure (e.g. servers). These IT functions are offered as a service to organizations either independently or as a package, using a shared pool of configurable computing resources.

The nature of cloud computing has raised concerns with data protection and potential privacy risks should the data "hosted" in the cloud be disclosed to foreign law enforcement agencies without appropriate disclosure or oversight. These concerns are often associated with the concepts of data sovereignty and data residency. While issues relating to these concepts do not only arise in the context of cloud computing solutions, these solutions have indeed heightened them.

In the cloud computing context, all information could be stored and processed in facilities in Canada, the US or elsewhere, when information is stored or accessible outside of Canada, the concern is that it can be subject to not just Canadian law, but also the law of the country in which it will reside. These concerns have raised questions about the impacts on the government's plan to move the government's cloud computing services outlined in the *Government of Canada's IT Policy, 2016-2020*, and the potential risks to the confidentiality, integrity and availability of GC information.

**Definitions**

While there are no universally accepted definitions for data sovereignty and data residency, a review of online sources indicates there is general agreement on their conceptual underpinnings. Based on this general agreement, the following definitions are offered in order to facilitate understanding of data sovereignty and data residency.

- **Data residency** - Data residency refers to the physical or geographic location of an organization's digital information.
- **Data sovereignty** - Data sovereignty refers to the fact that digital information is subject to the laws of the country in which it is stored.

**Issues and Advice**

There are a number of potential risks associated with processing and storage of GC information in facilities managed by non-GC service providers, and the associated transfer of data flow that are involved. In particular, the following definitions are offered in order to facilitate understanding of data sovereignty and data residency.

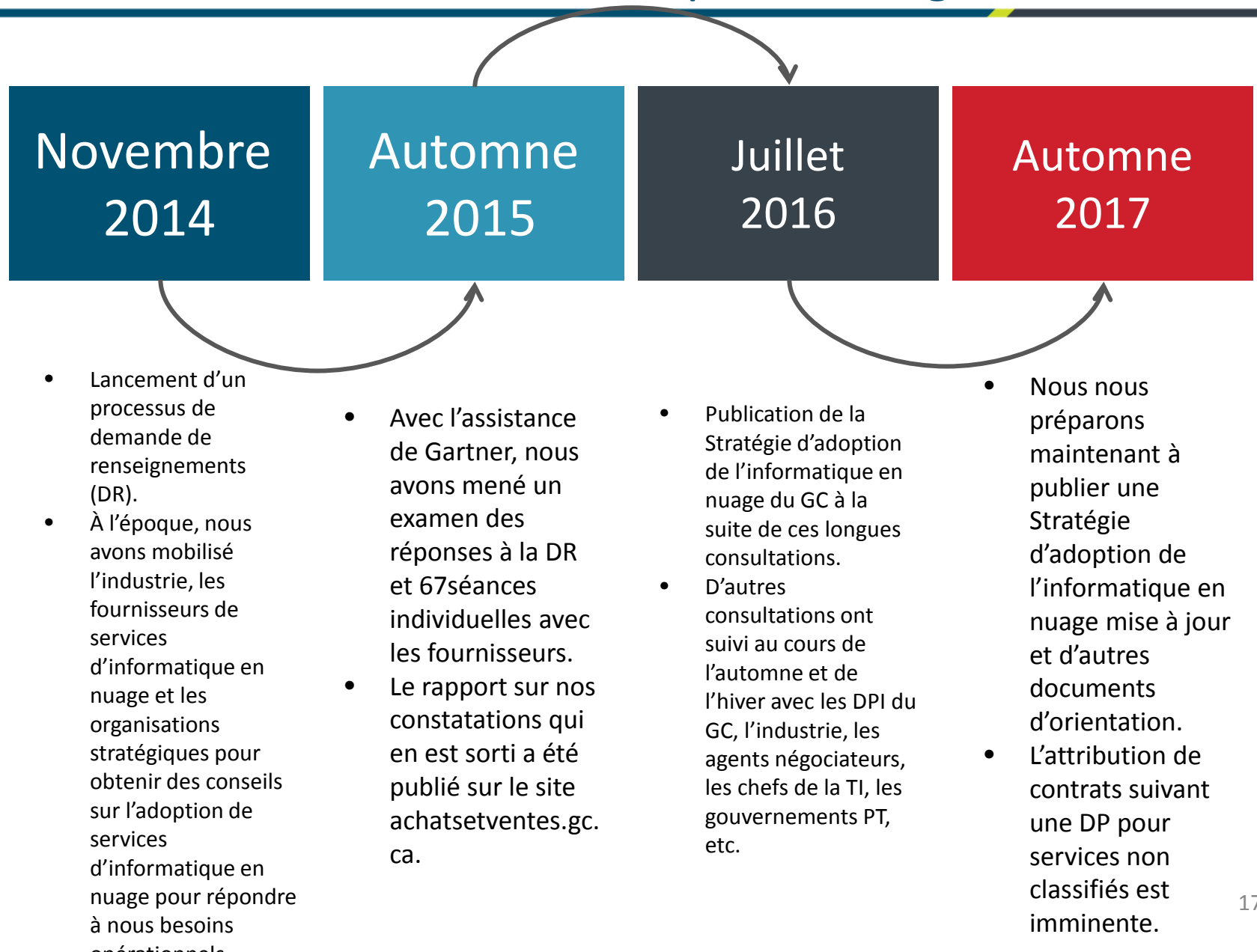
- **Unauthorized access to the information by a foreign organization**

Example: A cloud service provider's servers are located in a foreign country, and the provider's servers are subject to the laws of that country. This could result in unauthorized access to the information by a foreign organization.

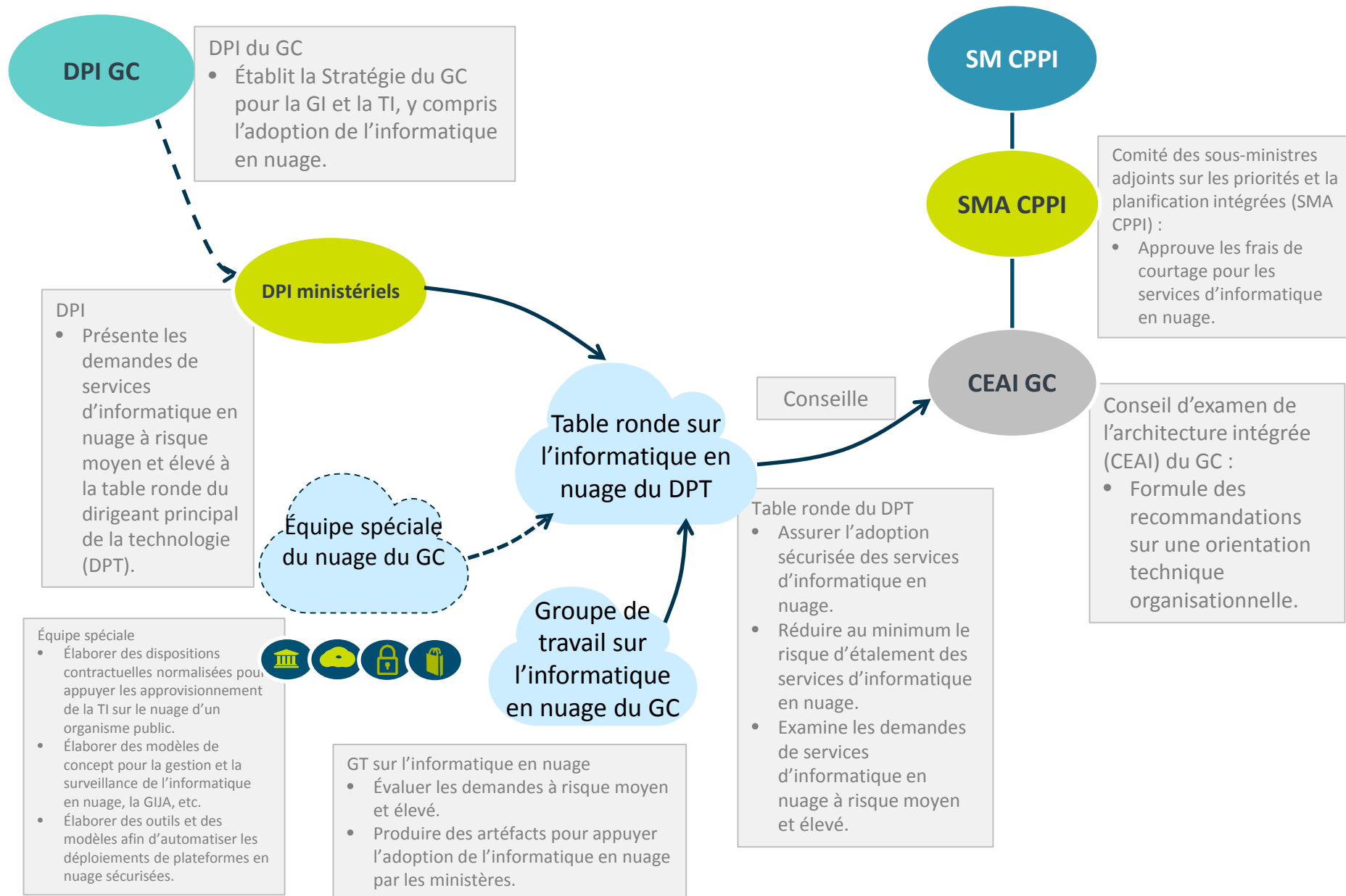



# Comment nous y sommes-nous parvenu?

## Cheminement de l'informatique en nuage au GC



# Modèle de gouvernance de l'informatique en nuage

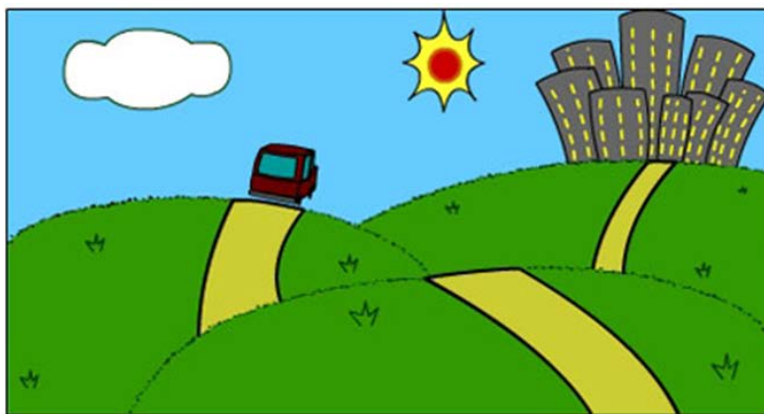




# Approvisionnement de services d'informatique en nuage non classifiés

# Demande d'approvisionnement de services d'informatique en nuage non classifiés

- ✓ Août 2016 – Lancement d'une invitation à se qualifier (ISQ)
- ✓ Date 16 2016 – Envoi d'une DP aux répondants à l'ISQ retenus
- ✓ 16 juin 2017 – Clôture de la DP
- ✓ 27 juillet 2017 – Évaluations techniques achevées
- ✓ En cours – Diligence raisonnable juridiques effectuée sur les soumissions (modalités)
- ✓ En cours – Examen de la documentation SOC2 des soumissionnaires
- ✓ septembre 2017 (à confirmer) – Début de l'attribution de contrats

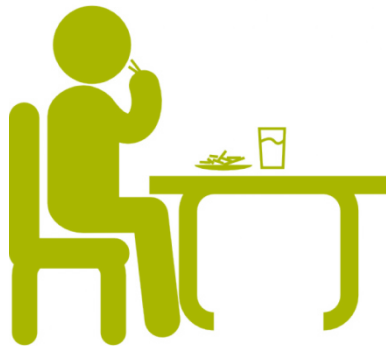


*Le chemin a été long et  
plein d'obstacles, mais  
notre destination est  
en vue!*

# Qui choisit?



**Gouvernance (Comité sur les plans et les priorités intégrés et CEAI du GC) :** Surveille le rendement du processus. Offre une orientation sur les points qui ont été acheminés à un échelon supérieur.



**DPI ministériels :**  
Sélectionnent l'option appropriée pour leur contexte opérationnel. L'évaluation des choix repose ici.

Sélection du nuage approprié



**Courtier des services d'informatique en nuage (SPC) :**  
Offre aux DPI des options d'approvisionnement dont ils peuvent se prévaloir.

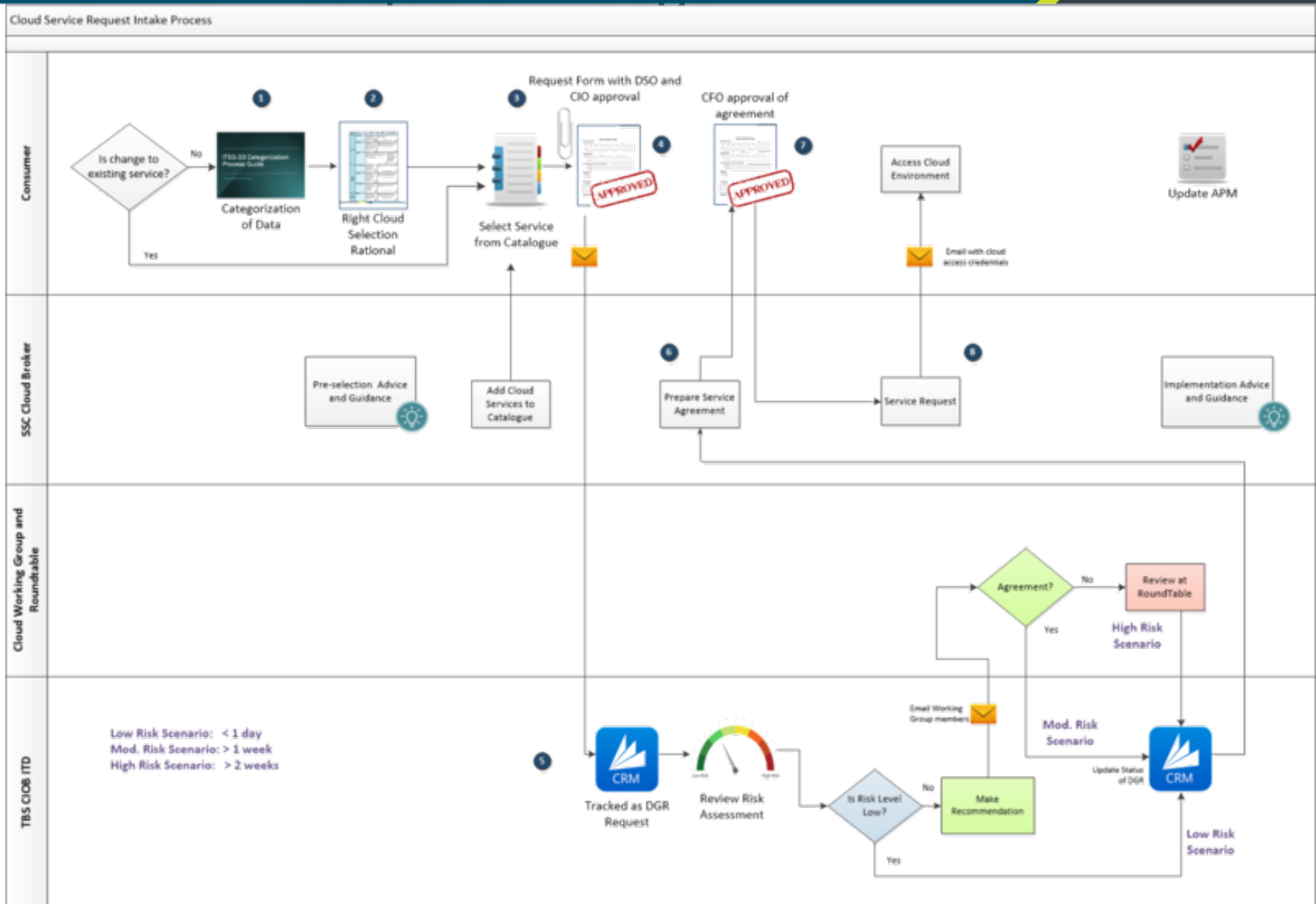


Nuage public



Nuage privé (à déterminer)

# Processus de réception des services d'informatique en nuage



# Foire aux questions (FAQ) sur l'informatique en nuage

# Répondre aux questions

Notre compréhension de la multitude de services d'informatique en nuage offerts évolue, tout comme nos fausses conceptions et notre mauvaise compréhension entre tous les niveaux

Le GC peut-il éviter d'utiliser l'informatique en nuage?

Comment puis-je veiller à ce que mes données soient protégées?

Maintenant que mes données sont dans le nuage, l'ASM est responsable de toute la sécurité, n'est-ce pas?



D'autres pays ont-ils adopté « l'informatique en nuage d'abord »?

L'informatique en nuage éliminera-t-elle le besoin d'avoir recours à des centres de données du GC?

Le nuage public est-il moins cher?



# FAQ sur l'informatique en nuage au GC

*Les prochaines diapositives souligneront les défis et répondront aux questions les plus fréquentes liées au déplacement des services protégés du GC au nuage :*

## L'INFORMATIQUE EN NUAGE D'ABORD

### Définition

- Un énoncé de politique pour orienter tous les nouveaux projets de la TI pour tirer parti des services d'informatique en nuage (avec une analyse de rentabilisation suffisante pour justifier le fait de ne pas utiliser l'informatique en nuage).

### FAQ

- D'autres gouvernements ont-ils adopté une politique sur l'informatique en nuage d'abord?

## RÉSIDENCE DES DONNÉES

- Référence à l'emplacement physique ou géographique des données d'une organisation (c'est-à-dire, toutes les données du GC supérieures au niveau non classifié doivent être stockées dans le territoire canadien).

- Est-il nécessaire que les renseignements sensibles et protégés résident au Canada?

## CONTRÔLE DES DONNÉES

- Concept que tous les actifs numériques peuvent être assujettis aux lois du pays où se trouve le siège des fournisseurs de services, ou même là où ils font des affaires.

- Les gouvernements étrangers ont-ils un accès sans obstacle aux données du GC stockées dans des centres de données étrangers hébergés en territoire canadien?

## APPROVISIONNEMENT

- Capacité d'acheter des services liés au nuage à l'aide des méthodes d'approvisionnement traditionnelles.

- Les politiques du Conseil du Trésor créent-elles des défis pour l'approvisionnement en services informatiques en nuage?

## VISIBILITÉ

- Capacité de surveiller le trafic du réseau sortant ou entrant des environnements du nuage.

- Le recours aux services informatiques en nuage aura-t-il une incidence sur la visibilité du GC à l'égard des activités de réseau et des données?

## RESPONSABILITÉS

- Précisions sur la nature partagée des responsabilités de sécurité et d'entretien.

- Les ministères ont-ils des responsabilités pour protéger et maintenir des services de la TI en nuage?



# L'informatique en nuage d'abord

Question : D'autres gouvernements ont-ils adopté une politique sur l'informatique en nuage d'abord?

Réponse : Le Canada est le seul membre des pays du groupe Five Eyes (Royaume-Uni, États-Unis, Australie, Nouvelle-Zélande) à ne pas avoir mis en œuvre une politique sur l'informatique en nuage d'abord.

## Enjeux/Points à considérer

- Le GC n'a pas de politique sur l'informatique en nuage d'abord qui soit obligatoire (seulement une recommandation dans la Stratégie d'adoption de l'informatique en nuage).
- Il se peut que l'ÉBAUCHE de la Politique sur la gestion de la TI comprend des exigences d'informatique en nuage d'abord obligatoires (à déterminer).

## Approche proposée

- Mettre à jour la Stratégie d'adoption de l'informatique en nuage du GC afin de refléter une position plus solide sur l'informatique en nuage d'abord.
- Approuver les exigences d'informatique en nuage d'abord obligatoires de la Réinitialisation des politiques de la TI – à déterminer

*\*Voir l'annexe A pour le Sommaire des approches d'autres gouvernements à l'informatique en nuage d'abord.*



# Résidence des données

Question : Est-il nécessaire que les renseignements sensibles et protégés résident au Canada?

Réponse : Oui, car la capacité d'appliquer la législation canadienne (comme la *Loi sur la protection des renseignements personnels*) est limitée à l'étranger.

## Enjeux/Points à considérer

- **La Stratégie d'adoption de l'informatique en nuage du GC** affirme que *toutes les données de nature délicate ou protégées sous le contrôle du gouvernement seront stockées sur des serveurs qui résident au Canada*.
  - Il n'existe toutefois pas encore d'énoncé de politique pour renforcer cette exigence.
- L'ÉBAUCHE de la **Réinitialisation des politiques de la TI** inclura une exigence obligatoire sur la résidence des données.

## Approche proposée

- Publier un Avis de mise en œuvre de la Politique sur la TI (AMPTI) pour renforcer l'exigence de résidence des données au Canada pour l'information de nature délicate en attendant que l'ensemble des politiques soient approuvé – *septembre 2017*
- Approuver l'exigence de résidence de données obligatoire dans la Réinitialisation des politiques de la TI – *automne 2017*



# Contrôle des données

**Question :** Les gouvernements étrangers ont-ils un accès sans obstacle aux données du GC stockés dans des centres de données étrangers hébergés en territoire canadien?

**Réponse :** Tous les pays ont des lois pour obtenir l'accès à des données, mais le GC peut appliquer des mesures pour respecter les règlements canadiens sur la sécurité et la protection des renseignements personnels.

## Enjeux/Points à considérer

- On craint que le fait de placer des données du GC dans des centres de données qui appartiennent à des pays étrangers permette aux gouvernements étrangers d'avoir un accès sans obstacle aux renseignements sur le GC, même si les centres de données résident au Canada.
- Les fournisseurs de service d'informatique en nuage ont de l'expérience à traiter les demandes de renseignements et à demeurer dans les limites du processus juridique (p. ex., Amazon - <https://aws.amazon.com/compliance/amazon-information-requests/>).
- Des contrôles peuvent être mis en œuvre pour atténuer le risque d'accès aux données, mais il y aura toujours des risques résiduels liés à l'adoption de services informatiques en nuage.

## Approche proposée

- Obtenir une attestation des fournisseurs de services informatiques en nuage concernant leur processus et la réponse aux demandes d'information – *août 2017*
- Obtenir des avis juridiques canadiens et américains sur le contrôle des données relativement à l'informatique en nuage – *août 2017*
- Élaborer des stratégies et une orientation sur le chiffrement des données afin de fournir des mesures de protection supplémentaires pour les données du GC (p. ex., utiliser des clés de chiffrement détenues par le GC) pour atténuer les risques – *août 2017*



# Approvisionnement

Question : Les politiques du Conseil du Trésor créent-elles des défis pour l'approvisionnement en services informatiques en nuage?

Réponse : L'approche actuelle en matière d'approvisionnement crée des défis pour l'approvisionnement en services d'informatique en nuage.

## Enjeux/Points à considérer

- À l'heure actuelle, le GC acquiert des services informatiques en nuage au moyen des clauses contractuelles actuelles conçues pour les déploiements sur place et les groupes de produits de consommation pour les biens et les services professionnels, et non des services d'informatique en nuage.
- La validation de sécurité liée au filtrage de sécurité du personnel, aux autorisations de sécurité des sites (installations) et de l'intégrité de la chaîne d'approvisionnement est aussi fondée sur des approches traditionnelles. Le GC a besoin d'un processus d'approvisionnement uniforme et simplifié qui appuie la prestation de services d'informatique en nuage en temps utile tout en maintenant la posture de sécurité du GC.

## Approche proposée

- Approbation de l'Avis de mise en œuvre des politiques de sécurité (AMOPS) pour préciser l'orientation relative aux exigences de sécurité des installations et du personnel pour les services d'informatique en nuage (tirer parti des normes de l'industrie si possible) – *septembre 2017*
- Faire évoluer le processus d'approvisionnement afin d'établir des groupes de produits de consommation pour les services d'informatique en nuage et établir des clauses contractuelles favorables à l'informatique en nuage qui s'harmonisent avec les approches de l'industrie (p. ex., ISO27001, ISO27017, ISO27018, etc.) – *octobre 2017*

Question : Le recours aux services informatiques en nuage aura-t-il une incidence sur la visibilité du GC à l'égard des activités de réseau et des données?

Réponse : Avec la bonne architecture en place, la visibilité du GC ne sera pas différente de celle d'aujourd'hui.

## Enjeux/Points à considérer

- Aujourd'hui, le GC a la visibilité de la majorité du trafic sur le réseau du GC par l'intermédiaire de SPC et du CSTC. On craint que le GC perde sa visibilité à mesure que les services passent à l'informatique en nuage.
- Les fournisseurs de services d'informatique en nuage ont mis en place des mécanismes qui permettent au GC d'examiner et de consommer les registres de la partie des services d'informatique en nuage du GC qui permettront s'appuyer les capacités d'inspection des données et le soutien pour la surveillance de la sécurité et la gestion des incidents du GC.
- L'architecture intégrée du GC doit évoluer pour mettre en œuvre des services défensifs en nuage dans le cadre d'une solution holistique et intégrée qui assurer le maintien de la visibilité du GC.

## Approche proposée

- Développer une architecture d'informatique en nuage protégée (approuvée par le Conseil d'examen de l'architecture intégrée du GC) qui permet la visibilité du trafic du réseau à destination et en provenance des services d'informatique en nuage du GC et appuie la surveillance de la sécurité et la gestion des incidents du GC – *octobre 2017*



# Responsabilités dans le nuage

Question : Les ministères ont-ils des responsabilités pour protéger et maintenir des services de la TI en nuage?

Réponse : La sécurité en nuage est une responsabilité partagée entre les fournisseurs de service en nuage et les ministères.

## Enjeux/Points à considérer

- Les ministères sont responsables de sécuriser et de tenir à jour les services **DANS** le nuage, **VERS** le nuage et en **PROVENANCE** du nuage, alors que les fournisseurs de service sont responsables de la sécurité **DU** nuage. Les ministères peuvent satisfaire à certaines des exigences en ayant recours aux services offerts par le GC (p. ex., COS de SPC).
- L'équipe spéciale du nuage\* a été établie avec les principaux intervenants à SPC, au SCT, au CSTC afin d'élaborer le document d'orientation (c.-à-d., « Directive sur le nuage protégé ») pour permettre aux ministères de mettre en œuvre en toute sécurité les charges de travail en nuage classées comme Protégé B.
- Le courtier de l'informatique en nuage du GC a un rôle à jouer pour établir les contrats de service d'informatique en nuage qui comptent les bonnes clauses de sécurité, notamment le fait de tirer parti des audits de tiers et des normes et attestations de l'industrie.

## Approche proposée

- Élaborer la Directive sur l'informatique en nuage Protégé B pour orienter les ministères dans le déploiement de services d'informatique en nuage sécurisés – *En cours (cible pour la mise au point : automne 2017)*
- Valider la Directive avec les projets de pionniers du nuage – *En cours*
- Continuer de faire évoluer le rôle de courtier de l'informatique en nuage du GC pour s'assurer de tenir compte de la sécurité dans les processus – *En cours*

\*Voir l'annexe B pour la liste de tous les membres de l'équipe spéciale du nuage

# Extrait d'une ébauche d'AMOPS

## 6.1.1 Security Categorization

Before using cloud services to support departmental programs, services and activities, or to hold departmental information, departments must ensure that information is identified and categorized based on the degree of injury that could be expected to result from a compromise of its confidentiality, availability or integrity. A [security categorization tool](#) is available to support departments in performing this activity.

## 6.2 Information Assurance and Asset Protection

Departments that use cloud services must safeguard their information and assets from unauthorized access, use, disclosure, modification, disposal, transmission, or destruction throughout their lifecycle. These safeguards must be commensurate with the security categorization of the information and assets, and must include an assurance that appropriate physical and personnel security controls are implemented.

### 6.2.2 Identity, Credential, and Access Management

Departments are responsible for ensuring that individuals and devices are uniquely identified and authenticated to an appropriate level of assurance before being granted access to information and information systems hosted in a CSP environment, in accordance with the [Standard on Identity and Credential Assurance](#), and in alignment with GC enterprise identity and authentication services.

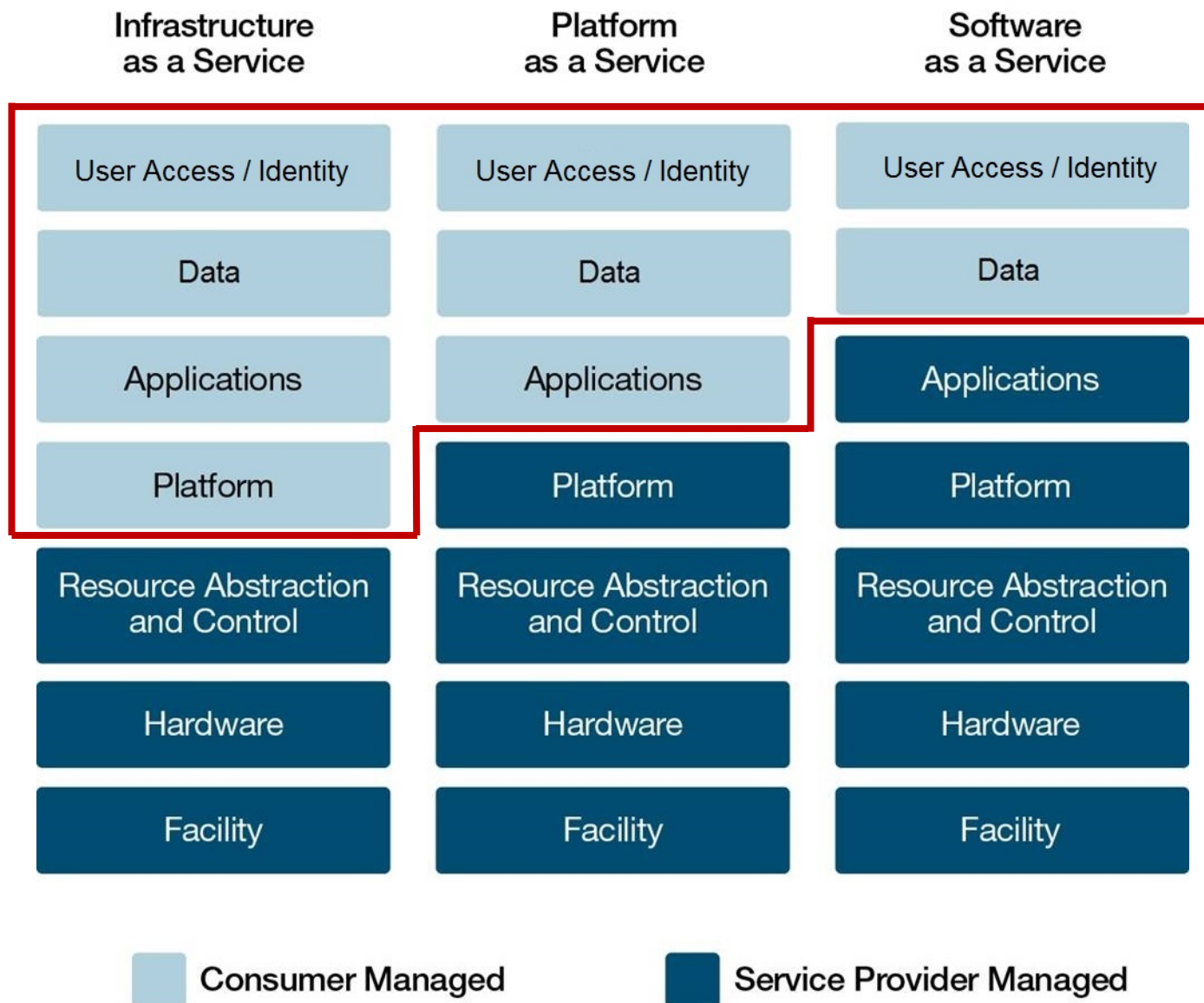




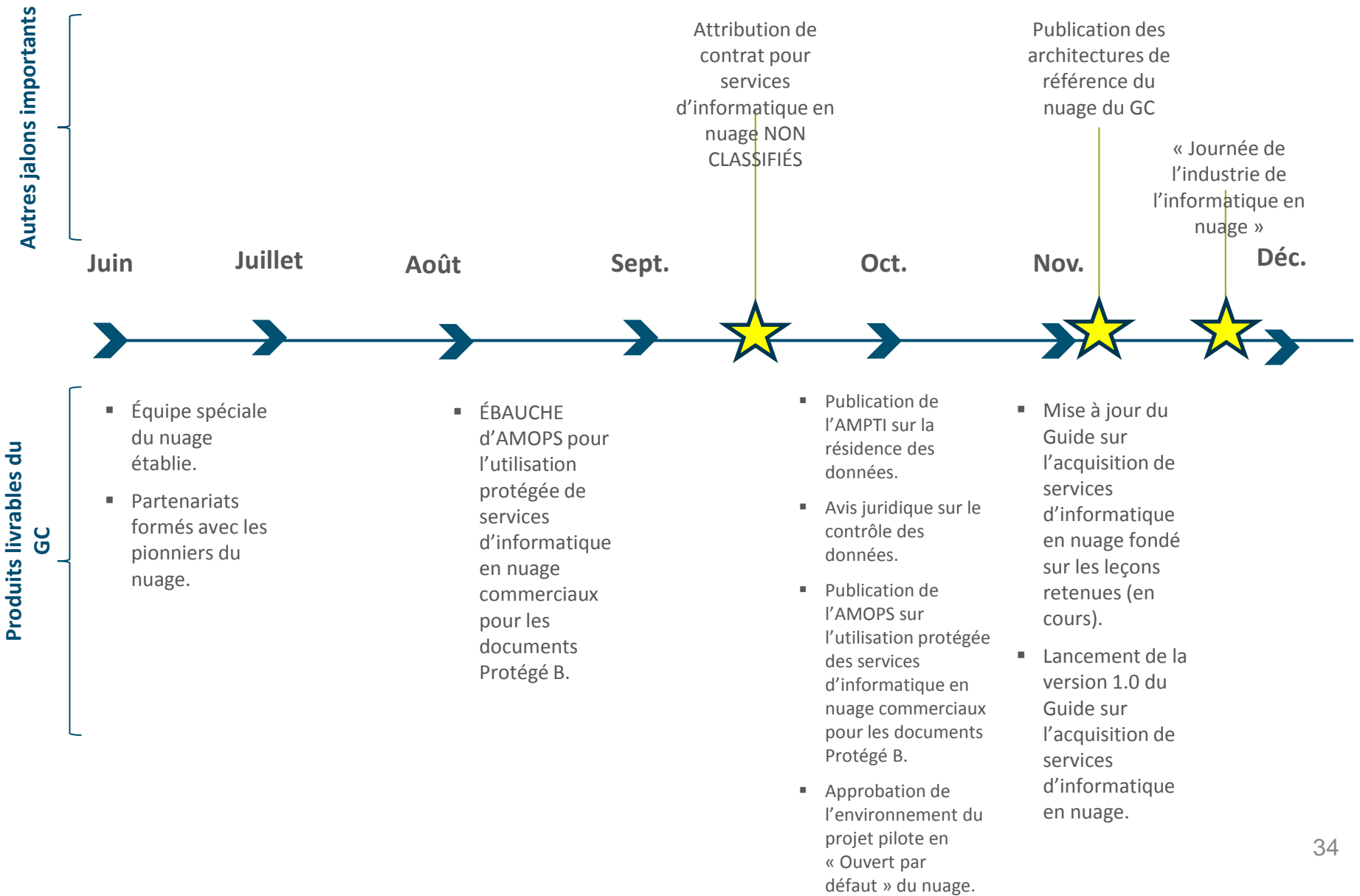
# Responsabilité partagée entre le GC et les fournisseurs de services en nuage



Les ministères sont responsables de sécuriser et de tenir à jour les services **DANS** le nuage, **VERS** le nuage et en **PROVENANCE** du nuage



# Calendrier





# Documents supplémentaires

## Plan stratégique de la GI/TI du GC

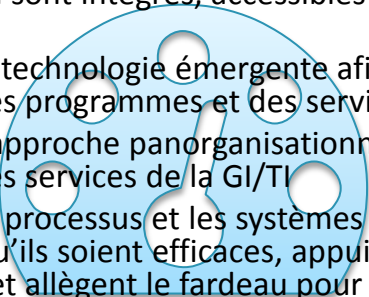
# Buts stratégiques

Les buts présentent des secteurs d'intérêts et décrivent des résultats de niveau plus élevé

## But stratégique n° 1 : Service

Un environnement de la GI/TI sensible, ouvert et novateur qui appuie la prestation de programmes et de services aux Canadiens et qui sont intégrés, accessibles et axés sur le client.

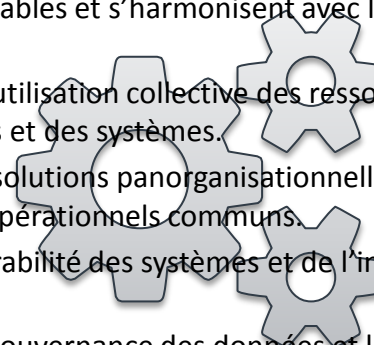
- Adopter une technologie émergente afin d'améliorer la prestation des programmes et des services.
- Poursuivre l'approche panorganisationnelle à la prestation des services de la GI/TI.
- Simplifier les processus et les systèmes de la GI pour veiller à ce qu'ils soient efficaces, appuient les objectifs d'ouverture et allègent le fardeau pour les travailleurs du GC.



## But stratégique n° 2 : Valeur

Des investissements intelligents qui sont de grande valeur, rentables, réutilisables et s'harmonisent avec les résultats opérationnels.

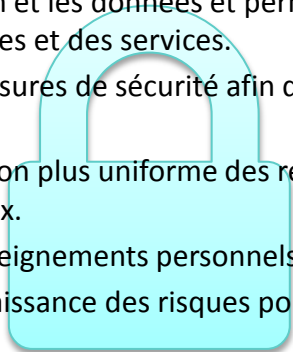
- Encourager l'utilisation collective des ressources, des outils, des processus et des systèmes.
- Élaborer des solutions panorganisationnelles pour répondre aux besoins opérationnels communs.
- Assurer la durabilité des systèmes et de l'infrastructure de la GI/TI.
- Renforcer la gouvernance des données et la reddition de compte.



## But stratégique n° 3 : Sécurité

Une infrastructure organisationnelle sécurisée et résiliente qui protège l'information et les données et permet la prestation fiable des programmes et des services.

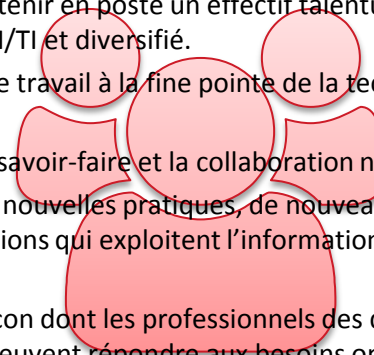
- Améliorer les mesures de sécurité afin de réduire le risque au minimum.
- Fournir une gestion plus uniforme des réseaux gouvernementaux.
- Protéger les renseignements personnels et sensibles.
- Élaborer la connaissance des risques pour la cybersécurité.



## But stratégique n° 4 : Agilité

Un effectif agile, connecté et très performant, doté d'outils modernes.

- Attirer et maintenir en poste un effectif talentueux hautement spécialisé en GI/TI et diversifié.
- Offrir un lieu de travail à la fine pointe de la technologie qui appuie la mobilité.
- Promouvoir le savoir-faire et la collaboration numériques.
- Faire l'essai de nouvelles pratiques, de nouveaux processus et de nouvelles solutions qui exploitent l'information comme un bien stratégique.
- Repenser la façon dont les professionnels des données et de l'information peuvent répondre aux besoins opérationnels actuels et futurs.



# Éléments du Plan stratégique de la GI/TI du GC

## Plan stratégique de la GI/TI du GC

Version mise  
à jour en  
octobre 2017

Mise en œuvre

En cours

### Vision

État cible de la GI/TI (ce que nous espérons atteindre)

### Mission

Les activités de la GI/TI (ce que nous faisons)

### Principes directeurs

Principes fondamentaux visant à orienter la prise de décisions et la mise en œuvre

### Domaines des résultats clés et résultats

Domaines à cibler et résultats escomptés connexes (avantages à l'état final)

### Mesures stratégiques

Stratégiques visant à obtenir des résultats (dans chacun des quatre domaines clés)

### Cadre de gouvernance

Prise de décisions stratégiques et surveillance simplifiées

### Feuille de route de la mise en œuvre

Produits livrables quantifiables et échéanciers

Plans de la TI  
ministériels

Cadre de  
rendement

Plan de  
communication



## Gestion de services

- 1 – Élaborer des portefeuilles et de répertoires des services de la TI.
- 2 – Rendre compte des principaux domaines de rendement de la santé des systèmes de la TI.
- 3 – Mise en œuvre des outils de gestion des services de la TI de l'organisation.
- 48 – Élaborer la Politique sur le numérique.
- 49 – Identifier et prioriser les services essentiels de SPC.
- 50 – Établir un répertoire et une base de référence des actifs de SPC.

## L'informatique en nuage d'abord

- 7 – Adopter les services d'informatique en nuage.
- 8 – Établir un courtier de services d'informatique en nuage.
- 9 – Offrir des services de nuage public.
- 10 – Offrir des services de nuage privé.

## Modernisation de la technologie

- 4 – Achever le regroupement et la modernisation des centres de données.
- 5 – Achever le regroupement des réseaux.
- 6 – Achever le regroupement des messages courriel du gouvernement.

## Échange de renseignements et de données

- 11 – Bâtir une plateforme pour l'interopérabilité organisationnelle.
- 51 – Lancer une stratégie à utiliser pour les logiciels de source ouverte et les normes ouvertes.
- 12 – Introduire une stratégie et un cadre pour les applications mobiles.
- 52 – Élaborer une stratégie d'API.
- 13 – Lancer un magasin d'API du gouvernement.
- 53 – Améliorer l'infrastructure en ligne afin de permettre aux ministères de libérer leurs données et leurs renseignements.
- 54 – Développer un programme de gestion des données-maître.
- 15 – Promouvoir l'analyse.
- 14 – Mettre en œuvre une plateforme pour la collaboration externe.
- 55 – Mettre en œuvre GCDocs.
- 56 – Migrer les sites Web vers Canada.ca.



# Mesures stratégiques - Gestion

## Gouvernance

- 27 – Établir une gouvernance de la GI/TI organisationnelle.
- 28 – Élaborer des méthodes pour établir la priorité des investissements dans les initiatives visant les systèmes existants et la transformation.
- 29 – Documenter les rôles et les responsabilités pour la TI et la sécurité de la TI.
- 57 – Établir la gouvernance des données.

## Harmonisation et pratiques d'architecture intégrée

- 30 – Faire évoluer les pratiques, les processus et les outils de gestion pour la GI/TI.
- 31 – Élaborer des architectures organisationnelles pour les activités, l'information, les applications et la technologie.
- 32 – Adopter des approches souples pour la mise en œuvre de solutions opérationnelles.
- 58 – Normaliser les métadonnées.
- 59 – Élaborer des cadre d'évaluation de l'information et des données.
- 60 – Élaborer un cadre de rendement pour la gestion de l'information.

## Agilité et innovation

- 33 – Diriger l'innovation.
- 34 – Adopter des modèles opérationnels modernes et souples.
- 61 – Créer un moteur de l'innovation pour l'information et les données.
- 62 – Fournir des outils et des ressources afin d'utiliser l'information et les données de façon innovatrices.
- 63 – Changer la culture et les processus vers l'ouverture par défaut.
- 64 – Établir un Conseil consultatif sur le numérique.
- 65 – Promouvoir la transformation de la gestion financière.

## Durabilité

- 35 – Assurer la durabilité de l'infrastructure de la TI.
- 36 – Rationaliser les investissements.
- 66 – Élaborer un processus visant à équilibrer l'offre et la demande en matière d'infrastructure.



# Mesures stratégiques - Sécurité

## Défense en profondeur

- 16 – Protéger le périmètre du réseau du gouvernement.
- 17 – Mettre en œuvre des profils de sécurité de point terminal.
- 18 – Mettre en œuvre une approche organisationnelle pour la gestion des vulnérabilités et des rustines.
- 19 – Gérer et contrôler les privilèges administratifs.

## Solutions et services fiables

- 20 – Protéger les opérations Web vers les sites externes et en provenance de ceux-ci.
- 21 – Mettre en œuvre un service d'authentification électronique amélioré.
- 22 – Mettre en œuvre une identité numérique fiable pour les personnes qui accèdent aux réseaux et aux systèmes internes du gouvernement.
- 23 – Mettre en œuvre un service de communication protégé pour l'information classifiée.
- 24 – Mettre en œuvre la prévention des pertes de données organisationnelles.

## Sensibilisation et compréhension

- 25 – Permettre la compréhension approfondie des appareils de point terminal.
- 26 – Accroître la sensibilisation aux menaces de cybersécurité et à l'environnement du risque.





# Mesures stratégiques – Collectivité

## Effectif de la GI/TI

- 39 – Faciliter le perfectionnement professionnel.
- 40 – Améliorer la diversité.
- 67 – Renforcer le recrutement.
- 68 – Moderniser la profession de gestion de l'information et des données.
- 69 – Élaborer une formation en gestion de l'information et des données.
- 70 – Renforcer le perfectionnement en leadership.
- 71 – Diriger des initiatives ciblées.

## Milieu de travail moderne

- 41 – Moderniser les appareils technologiques du milieu de travail.
- 42 – Appuyer un effectif mobile.
- 43 – Fournir un accès Wi-Fi.
- 44 – Fournir la vidéoconférence sur ordinateur de bureau pour les employés.
- 45 – Mettre en œuvre des services d'impression gérés.
- 72 – Améliorer l'accessibilité à la GI/TI.

## Collaboration numérique

- 46 – Favoriser l'alphabétisation et la collaboration.
- 47 – Promouvoir la collaboration numérique.
- 73 – Élaborer la formation et la sensibilisation sur le gouvernement ouvert.