FINAL v1.0 GC EARB endorsement 2018-03-22

Government of Canada

Cloud Roles and Responsibilities

27 September 2022

Executive Summary

Cloud computing has the potential to provide a flexible means of delivering information system services and provides an alternate service delivery model enabling the GC to support its digital transformation agenda. Cloud adoption can support the GC’s ability to continue to sustain information system service excellence during a period of increased demand by Canadians for online services and timely access to accurate information. This developing shift will affect how we procure, secure, and work with information systems that support GC and departmental programs and services.

Care must be taken to mitigate risks associated with using cloud services. Adopting this model will require due diligence and prudence on the part of the GC in the selection of appropriate cloud service provider (CSP), as well as a clear delineation of the roles and responsibilities between the GC and the CSP for implementing, operating, and maintaining security controls which support GC obligations for data protection and privacy. Clear roles and responsibilities must also be defined within the GC to help ensure a cost-effective and risk-managed use of cloud computing to support program and service delivery.

To help ensure a cost-effective and risk-managed use of cloud computing to support program and service delivery, this document describes the roles and responsibilities of the various GC actors who will be involved in the governance, planning, orchestration, implementation, operations, and maintenance of cloud-based information system services.

Revision History

|  |  |  |
| --- | --- | --- |
| Document Version No. | Changes | Date |
| 0.1 | Initial draft prepared by TBS-CIOB, Cyber Security. | 29 September 2017 |
| 0.2 | Updated based on comments received from cloud ninja team and GC cloud working group consultation | 27 November 2017 |
| 0.3 | Hand-over from TBS CIOB Cyber to TBS CIOB ITD | 10 December 2017 |
| 0.4 | Updated to reflect GC Cloud CoE as GC Cloud Working Group and associated description | 19 December 2017 |
| 0.5 | Endorsed by GC EARB | 22 March 2018 |
| 2.0 | Translated and guardrail responsibilities added to matrix | 27 September 2022 |

Table of Contents

[1. Introduction 1](#_Toc499819833)

[1.1 Background 1](#_Toc499819834)

[1.2 Document Purpose 1](#_Toc499819835)

[1.3 Audience 1](#_Toc499819836)

[1.4 Definitions of Key Terms 1](#_Toc499819837)

[2. Context 3](#_Toc499819838)

[2.1 Shared Responsibility 3](#_Toc499819839)

[2.2 GC Cloud Profiles 4](#_Toc499819840)

[2.3 Cloud-based Service Implementation 6](#_Toc499819841)

[3. Cloud Actors 7](#_Toc499819842)

[3.1 GC Scope 7](#_Toc499819843)

[3.2 Departmental Scope 9](#_Toc499819844)

[4. GC Cloud Responsibility Matrix 11](#_Toc499819845)

[5. References 13](#_Toc499819846)

List of Tables

[Table 3‑1 Cloud Actors – GC Scope 7](#_Toc499819847)

[Table 3‑2 Cloud Actors – Departmental Scope 9](#_Toc499819848)

[Table 4‑1 GC Cloud RACI Matrix – Summary View 11](#_Toc499819849)

List of Figures

[Figure 2‑1 Scope of Responsibility 4](#_Toc499819850)

[Figure 2‑2 Scope of GC Cloud Profiles 5](#_Toc499819851)

[Figure 2‑3 Notional Model of Shared Implementation and Operations Responsibility 6](#_Toc499819852)

List of Abbreviations and Acronyms

|  |  |
| --- | --- |
| CIO | Chief Information Officer |
| CIOB | Chief Information Officer Branch |
| CISD | Canada Industrial Security Directorate |
| CSE | Communications Security Establishment |
| CSP | Cloud Service Provider |
| DSB | Departmental Security Branch |
| EA | Enterprise Architecture |
| ESA | Enterprise Security Architecture |
| GC | Government of Canada |
| IaaS | Infrastructure as a Service |
| ICAM | Identity, Credential, and Access Management |
| IT | Information Technology |
| NEUB | Network and End User Branch |
| NIST  | National Institute of Standard and Technology |
| NOC | Network Operations Centre |
| PaaS | Platform as a Service |
| PIA | Privacy Impact Assessment |
| PSPC | Public Services and Procurement Canada |
| RACI | Responsible, Accountable, Consulted, Informed |
| RCMP | Royal Canadian Mounted Police |
| SaaS | Software as a Service |
| SDLC | System Development Lifecycle |
| SE | Systems Engineering |
| SOC | Security Operations Centre |
| SOW | Statement of Work |
| SRCL | Security Requirements Checklist |
| SSC | Shared Services Canada |
| SSE | System Security Engineering |
| TA | Threat Assessment |
| TBS  | Treasury Board of Canada Secretariat |

# Introduction

## Background

Cloud computing has the potential to provide a flexible means of delivering information system services and provides an alternate service delivery model enabling the Government of Canada (GC) to support its digital transformation agenda. This alternative service delivery model allows individuals and organizations (or “tenants”) to use software, hardware, and services, hosted external to the GC’s facilities, and managed by private sector organizations, including software (e.g. customer relationship management, etc.), platforms (e.g. operating system, database) and infrastructure (e.g. servers, storage, and networks).

Cloud adoption can support the GC’s ability to continue to sustain information system service excellence during a period of increased demand by Canadians for online services and timely access to accurate information. This developing shift will affect how we procure, secure, and work with information systems that support GC and departmental programs and services. Adopting this model will require due diligence and prudence on the part of the GC in the selection of appropriate cloud service provider (CSP), as well as a clear delineation of the roles and responsibilities between the GC and the CSP for implementing, operating, and maintaining security controls which support GC obligations for data protection and privacy. Clear roles and responsibilities must also be defined within the GC to help ensure a cost-effective and risk-managed use of cloud computing to support program and service delivery.

## Document Purpose

This document describes the roles and responsibilities of the various actors within the GC who will be involved in the governance, planning, orchestration, implementation, operations, and maintenance of GC cloud-based information system services to support program and service delivery.

This document also supports the Security Policy Implementation Notice (SPIN) for the Secure Use of Commercial Cloud Services [1] which helps departments and agencies in understanding existing Treasury Board (TB) security policy requirements in the context of cloud computing.

## Audience

This document is to be used by business owners, IT project managers, IT and IT security practitioners, and other GC cloud actors seeking to leverage cloud services.

## Definitions of Key Terms

Below are the definitions of key terms used in the document. All other terms are defined in the references listed in Section 5.

|  |  |
| --- | --- |
| cloud service | Any information system service provided by a CSP. A cloud service offering can be infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS). |
| cloud-based service | A GC information system service that is implemented over a cloud service. The composition of a cloud-based service will vary depending on the model of the underlying cloud service: for IaaS, a platform and an application; for PaaS, an application, and for SaaS, the customization and configuration of the SaaS application. |
| cloud service provider (CSP) | A commercial provider of a cloud service. |

# Context

The GC cloud roles and responsibilities are structured around the shared responsibility model inherent to cloud computing. The Treasury Board of Canada (TBS) [GC Cloud Security Risk Management Approach and Procedures](http://www.gcpedia.gc.ca/gcwiki/images/c/c7/GC_Cloud_Security_Risk_Management_Approach_and_Procedures_-_EN.pdf) [2] document, which is based on Communication Security Establishment (CSE)’s ITSG-33 [IT Security Risk Management Framework: A Lifecycle Approach](https://www.cse-cst.gc.ca/en/publication/itsg-33)[3], highlights the shared responsibility in implementing the security controls with the appropriate rigour to allow the hosting of GC services and related information on cloud services provided by commercial CSPs. It also describes the authorities, approach, and procedures for managing IT security risks when using cloud services. The CSP fulfils some responsibility with respect to risk mitigation, but departments and agencies are ultimately accountable for the risks. This shared responsibility model is described in the context of the GC in the subsections that follow.

## Shared Responsibility

Departments must continuously manage their information and IT assets throughout the life of their programs and services. In the cloud context, IT asset management is based on a shared responsibility model. The CSP fulfils some responsibilities with respect to IT and IT security, but departments maintain overall accountability.

Figure 2‑1 is a simplified view of the architectural layers of cloud computing. It depicts the scope of responsibility of consumers and service providers as it applies to the cloud service models defined in NIST 500-292 (Cloud Computing Reference Architecture) [4] and NIST 500-299 (Cloud Computing Security Reference Architecture) [5].



Figure ‑ Scope of Responsibility

## GC Cloud Profiles

The Chief Information Officer Branch (CIOB) within TBS has developed security control profiles for cloud computing. A baseline security control profile is a set of IT security controls an organization establishes as minimum mandatory requirements for their information systems. By adhering to a standardized set of security controls, departments can identify and assess risks, and develop strategies to appropriately mitigate them.

The responsibility for implementing and maintaining these security controls in these profiles is shared between the GC and CSPs. Depending on the service model selected, the GC, as a consumer of cloud services, will be responsible for implementing additional security controls either fully or partially as part of their portion of the shared responsibility model. Figure 2‑2 provides a view of the division of responsibility for security control implementation between the CSP and the GC consumer organization.



Figure ‑ Scope of GC Cloud Profiles

The nature of security controls that a GC organization needs to implement in the cloud service is dictated by the service model upon which the information system service is being deployed. For example, if the service model is IaaS, the GC organization must implement the security controls of the platform and application layers of the cloud technology stack. These include security controls for access control, audit and accountability, identification and authentication, system and communications protection, configuration management, contingency planning, incident response, maintenance, and system and information integrity. Even under the SaaS service model, the GC organization needs to implement some security controls to manage user access, conduct audits, and respond to incidents.

The [GC Security Control Profile for Cloud-based Services](https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/cloud-computing/government-canada-security-control-profile-cloud-based-it-services.html) [6] document identifies the baseline security controls recommended for implementation by CSPs and GC departments and agencies, in order to appropriately protect cloud-based services having a security category of Protected B, medium integrity, and medium availability. It also documents the context in which these security controls are expected to be implemented.

## Cloud-based Service Implementation

When implementing a cloud-based service, the responsible GC organization and the supporting CSP are each responsible for the implementation and operations of their portion of the information system service. This shared responsibility is illustrated in Figure 2‑3. This figure also highlights key inputs. For the system lifecycle process, these include system development life cycle procedures and tools, system engineering/system security engineering procedures and tools, and applicable enterprise architecture/enterprise security architecture artifacts. For the procurement process, key inputs include items such as the statement of work for any required cloud service, standard contractual clauses, and a security requirements checklist.



Figure ‑ Notional Model of Shared Implementation and Operations Responsibility

# Cloud Actors

## GC Scope

This section identifies and describes the GC actors who have a role to play within the cloud computing context. The actors are grouped based on the scope of their responsibilities, which are either GC-wide or departmental.

Table ‑ Cloud Actors – GC Scope

| Actor | Description |
| --- | --- |
| GC Chief Information Officer (CIO)  | The GC CIO has the overall responsibility for providing strategic direction for cloud computing to support GC program and service delivery. |
| GC Enterprise Architecture Review Board (EARB) | The GC EARB provides direction for enterprise IT across government. This includes managing risks related to the adoption of cloud computing. The GC EARB reviews all cloud projects from both an architecture and a risk perspective in order to ensure that potential risks are properly mitigated. |
| GC Enterprise Architecture(EA)/ Enterprise Security Architecture (ESA) Team | The GC EA/ESA team is responsible for the establishment and maintenance of a GC-wide cloud adoption framework. This framework consists of architectural artifacts and cloud-specific strategies and tools to orchestrate, simplify, and guide cloud service adoption by departments and agencies.  |
| GC Cloud Working Group | The GC Cloud Working Group is responsible to provide GC-wide advice and guidance to departments and agencies on cloud adoption. This includes contributing to the establishment of the GC-wide cloud adoption framework. The GC Cloud Working Group is composed of representatives from various organizations including as TBS-CIOB, CSE, SSC, PSPC and will include industry and departmental subject matter experts such as:* *Cloud automation analysts* - providing cloud computing automation tools
* *Cloud service transition advisors* - providing cloud migration and transition advice and guidance
* *Cloud security advisors* - providing cloud security architecture and engineering advice and guidance
 |
| GC Cloud Service Broker[[1]](#footnote-1),  | SSC, in its role as the GC cloud service broker, will act as the intermediary between CSPs and departments and agencies that consume cloud services by providing various types of brokerage services such as the administration of a cloud service marketplace, establishment of cloud service procurement vehicles, and auditing of cloud service usage in accordance with applicable policies, directives, and standards. |
| Supply Chain and Product Assurance Analysts | Supply chain / product assurance analysts are responsible for the supply chain management and product assurance process for the procurement of cloud services for GC consumption. |
| Identity, Credential, and Access Management (ICAM) Service Owner | The owners of enterprise ICAM services. These include Directory Services, MyKey, and GCKey.  |
| Network Engineering, Network and End User Branch (NEUB) | Network Engineering is responsible for defining, designing, and maintaining interconnections between the GC and commercial cloud service environments to ensuring optimal accessibility of cloud-based services by internal and external end user communications.  |
| Network Operations Centre (NOC) | The SSC NOC is responsible for the centralized network monitoring for cloud-based services. The SSC NOC monitors and manages GC networks and cloud service interconnections and responds to events. |
| Security Operations Centre (SOC) | The SSC SOC is responsible for the centralized security operations for cloud-based services. The SSC SOC monitors security logs and responds to security incidents. The SSC SOC acts as the central point of contact for the coordination, reporting, and trending analysis of security events that may have impacted or may impact the GC.  |
| Cyber Defence Operations | CSE is responsible for providing threat monitoring and defensive services for the GC. |
| GC Security Assessors | Security assessors are responsible to conduct assessments of CSPs and cloud services in support of authorization and authorization maintenance, and as part of the third-party assurance validation process. |
| Acquisitions Branch | Public Services and Procurement Canada (PSPC)’s Acquisitions Branch provides advice and support to help federal government departments and agencies achieve their procurement objectives. |
| Industrial Security Program | PSPC’s Industrial Security Program is responsible for validating compliance of contractors to the contract security requirements. Validation covers physical, personnel, and information system security. |
| Physical Security Advisors | Physical security advisors contribute to the establishment and maintenance of the GC-wide cloud adoption framework by providing advice and guidance on the physical security of cloud facilities. |

## Departmental Scope

The following section identifies and describes the departmental actors who have a role to play within the cloud computing context. However, while the scope of the responsibilities outlined are for departments, the same responsibilities could be applied for an organization providing an enterprise or common service.

Table ‑ Cloud Actors – Departmental Scope

| Actor | Description of Role in the Context of Cloud Computing |
| --- | --- |
| Deputy Head | The deputy head has the overall responsibility for the cost-effective, risk-managed use of cloud services to support departmental program and service delivery. |
| CIO | The CIO is responsible for establishing and maintaining a departmental governance structure and cloud adoption framework for the implementation of cloud-based services to support departmental program and service delivery.  |
| IT Security Coordinator[[2]](#footnote-2) | The IT security coordinator is responsible for the overall coordination of security activities across the department to ensure a risk-based implementation and maintenance of cloud-based services. The IT security coordinator is also responsible for the security assessment and ongoing monitoring activities. |
| Business Owners (Program and Service Delivery Managers) | Business owners will rely on cloud-based services to deliver their programs and services. Working with data owners, they are responsible to provide their business needs and requirements, including business needs for security, to cloud service designers. Because they are accountable for related risks, business owners are responsible for authorizing the operation of the cloud-based services that support their programs and services. |
| Privacy Officers | Departmental privacy officers are responsible to provide advice to business owners and cloud service designers to assure privacy compliance of cloud-based services. |
| Enterprise Architect | Enterprise architects (to include cloud architects and enterprise security architects) are responsible for the establishment and maintenance of a departmental cloud adoption framework in alignment with the GC-wide cloud adoption framework. Enterprise architects also work with cloud service designers to assure compliance of cloud-based services to architectural artifacts.  |
| Cloud Service Designers and Developers | Cloud service designers and developers are responsible for designing, developing, integrating, testing, deploying, and maintaining cloud-based services. Cloud service designers and developers take business needs and requirements and work with enterprise architects, privacy advisors, security analysts, and security assessors to implement dependable cloud-based services.  |
| Cloud Automation Analyst | Cloud automation analysts are subject matter experts who are responsible for the development and maintenance of cloud automation processed to be used in cloud-based services within a departmental scope.  |
| Security Analysts | Security analysts are responsible for providing system security engineering support to cloud service designers and developers and liaise with security assessors.  |
| Security Assessors | Security assessors are responsible for conducting security assessments of cloud-based services to support authorization and continuous security monitoring and assessment. |
| Cloud-based Service Owners[[3]](#footnote-3) | Cloud-based service owners have the overall responsibility for the implementation, operation, and maintenance of cloud-based services. |
| Cloud Service Operators and Administrators | Cloud service operators and administrators are responsible for the day-to-day operations and administration of cloud-based services.  |
| Security Operations | Security operations are responsible for the centralized security operations for cloud-based services. Security operations monitor security logs and respond to security incidents. |
| IT Service Desk | The IT service desk is responsible for providing first line support for cloud-based services. |
| Cloud-based Service Auditors | Cloud-based service auditors are responsible for auditing cloud-based service usage activities in accordance with applicable policies, directives, and standards.  |

# GC Cloud Responsibility Matrix

The responsibilities of the GC cloud actors are described in a detailed RACI matrix, which can be viewed by clicking on the following link:

[GC Connex GC Cloud Working Group File Repository](https://gcconnex.gc.ca/file/view/37162556/gc-public-cloud-raci-matrix-v1?language=en)

The table below summarizes the RACI matrix by responsibility area and the various GC entities including departments and agencies.

Table ‑ GC Cloud RACI Matrix – Summary View

R = Responsible, A = Accountable, C = Consulted, I = Informed

| **Sect.** | Roles**High-level Summary of Responsibilities** |  **TBS CIOB** |  **SSC** |  **CSE** |  **PSPC** |  **RCMP** |  **Departments and Agencies**  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Establish GC-wide governance for cloud | **A,R** | **C** | **C** | **C** | **C** | **C** |
| 2 | Establish GC-wide cloud adoption framework | **A,R** | **C** | **C** | **C** | **C** | **C** |
| 3 | Establish third-party security assurance | **C** | **C** | **A,R** | **C** | **C** | **C** |
| 4 | Acquire commercial cloud services[[4]](#footnote-4) | **C** | **A,R** | **C** | **A,R** | **C** | **C** |
| 5 | Provide GC cloud brokering services | **C** | **A,R** | **C** | **C** | **C** | **C** |
| 6 | Provide network integration services to cloud-based services | **C** | **A,R** | **C** |  |   | **C** |
| 7 | Provide ICAM to cloud-based services | **C** | **A,R** | **C** |  |   | **C** |
| 8 | Provide implementation and operation support to departments | **C** | **A,R** | **R** |  |  | **C** |
| 9 | Monitor GC-wide cloud operations | **C** | **A,R** | **C** |  |   | **C** |
| 10 | Establish departmental governance for cloud-based services | **C** | **C** | **C** |  |  | **A,R** |
| 11 | Establish departmental cloud adoption framework | **C** | **C** | **C** |  |  | **A,R** |
| 12 | Implement cloud-based services | **C** | **C** | **C** |  |  | **A,R** |
| 13 | Operate and maintain cloud-based services | **I** | **C** | **C** |  |   | **A,R** |
| 14 | Monitor departmental cloud operations | **I** | **C** | **C** |  |   | **A,R** |
| 15 | Perform continuous monitoring of cloud-based services | **I** | **C** | **C** |  |   | **A,R** |

# References

|  |  |
| --- | --- |
| [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. |

1. More information about the GC Cloud Service Broker function is available in the GC Cloud Broker Concept of Operations document available on GCpedia - <http://www.gcpedia.gc.ca/gcwiki/images/a/ad/Cloud_Service_Broker_ConOps_%28draft%29.pdf> [↑](#footnote-ref-1)
2. The departmental IT Security Coordinator has responsibility for security of workloads hosted in the Cloud. On the other hand, the ITSC for the GC department managing the cloud management environment has responsibility for the security of the management environment. [↑](#footnote-ref-2)
3. The responsibilities of the cloud-based service owner could also be applied for services that are delivered on a GC-wide basis. [↑](#footnote-ref-3)
4. As per the GC Cloud Adoption Strategy, both PSPC and SSC have a role in acquiring cloud services. [↑](#footnote-ref-4)