Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Application Modernization Guidance

Cloud-based Managed Services

Version 6.0

Overview

As much as the Government of Canada has moved to a cloud first policy, so too has the private industry that supplies the GC with services and goods. When procuring services, whether technology services or business services, departments should expect that providers will deliver a portion of those services using cloud services. Departments should set clear requirements in any request for proposal where a managed service provider may process or store GC information as requirement of the contract. Setting these requirements later in the contracting process will complicate the process and may lead to failure.

The Government of Canada has provided clear policy and guidance as to how it should procure and manage its relationship with cloud service providers. For cases where the GC does not have a direct contractual relationship with the cloud service provider, where a managed service provider may own that relationship, the GC's policy and guidance still applies. In those cases, the consumer portions of the shared responsibility model become further shared between the GC and the managed service provider.

This guidance document aims to provide an understanding of key concepts related to Managed Services that include cloud services and key areas that departments and agencies should factor in their decision-making process should you wish to leverage the use of Cloud-based Managed Services.

This document does not explore the merits of managed services or contracting models.

When multiple providers are involved in delivering a technology service, it is critical that the GC, as the contract holder and service owner, understand the roles and responsibilities of each contractor and sub-contractor.

Key Concepts

This section provides terminology that will be used through-out this guidance document.

Managed Service:

A managed service can be either business process or technical. With a managed business process an entire business process is being managed by a provider. Examples include health care, internal services, administration, amongst others. Managed business process providers typically use technology to automate the delivery of its services. Contracts with managed business process providers may not directly specify technology as part of the requirements.

Technology managed service providers manage a scope of technology such as an application or platform. Contracts for managed services specify the information technology service management requirements a provider must meet in the delivery of that technology.

Managed Services are carried out by a Managed Service Provider on behalf of the Service Owner.

Managed Service Provider (MSP):

A Managed Service Provider is a vendor that manages a cloud service on behalf of the service owner. Typically, the provider helps build or deliver an IT solution that is tailored to the requirements specified by the GC.

Cloud Service Provider (CSP):

A Cloud Service Provider is a company that offers some component of cloud computing -- typically

Infrastructure as a service (IaaS), Software as a Service (SaaS) or platform as a service (PaaS) -- to other businesses.

Service Owner:

The Service Owner is responsible for the delivery of particular service. The service owner owns the overall accountability for the cloud service delivery. GC in this case is the service owner.

Types of GC Cloud Managed Service Relationships

How contractual relationships are structured is critical to understand roles and responsibilities of each provider. Broadly, two models exist:

1. **The GC as the integrator:**

   In this model, the GC contracts with both the Cloud Service Provider and the Managed Service Provider. The Managed Service Provider is directed to deploy its service on top of the service offered by the Cloud Service Provider. As an example, the Managed Service Provider may be directed to deploy its services onto the service the GC acquired through the SSC Public Cloud Framework Agreement. The GC must coordinate issues between both parties.

2. **The Managed Service Provider as the integrator:**

   In this model, the GC acquires the services of a Managed Service Provider. The Managed Service Provider has a contractual agreement with the GC, therefore will be responsible for some or all of the consumer responsibilities in the Shared Responsibility Model. The Managed Service Provider then contracts some aspects of the service directly with the Cloud Service Provider. The Managed Service Provider is responsible for the performance of the Cloud Service Provider and resolution of any issues.

These relationship scenarios are illustrated below:

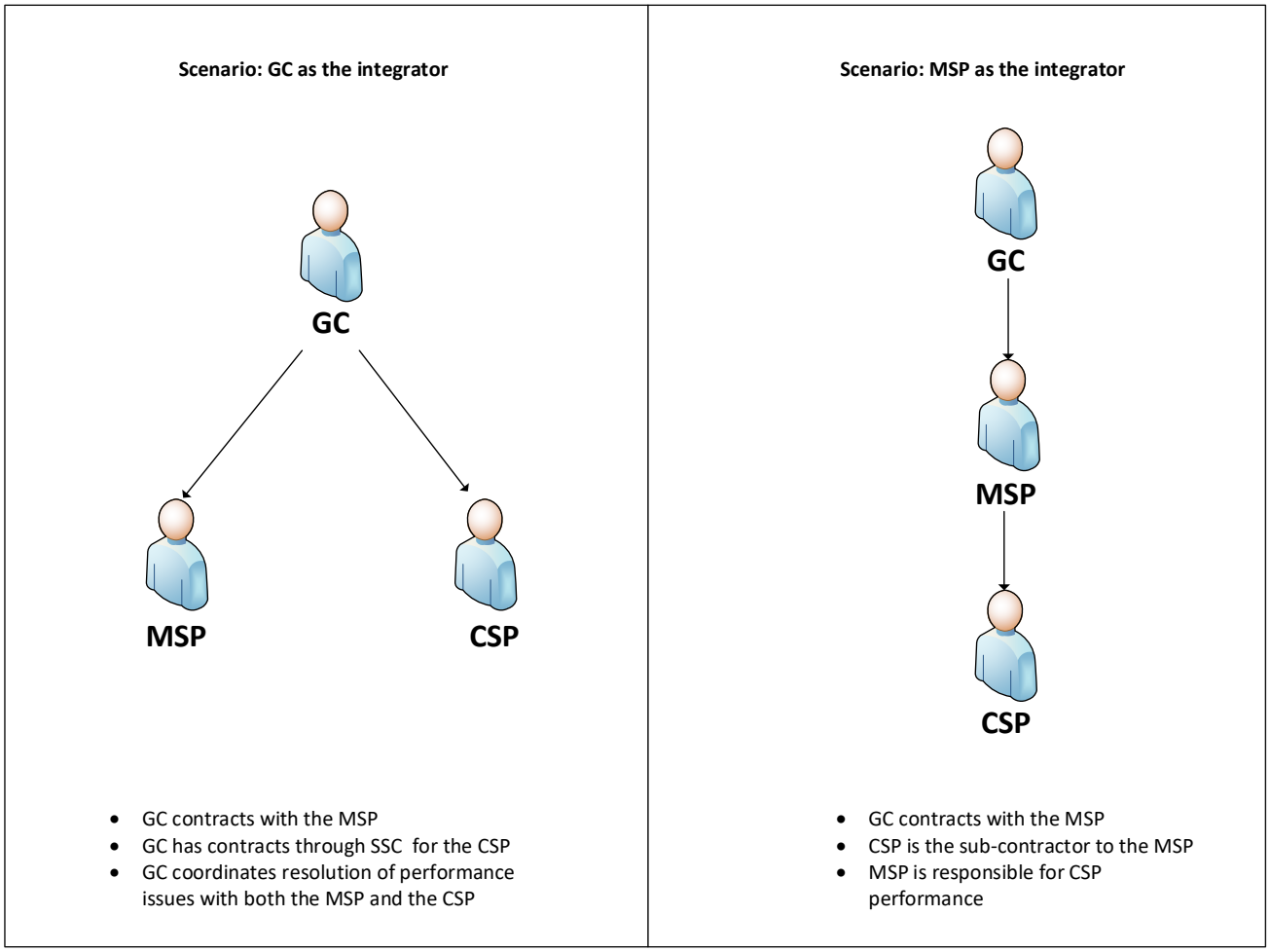

Figure 1 GC Cloud Managed Service Relationships

Note: This segment of the market is still growing, other types of relations and Cloud-based Managed Services will evolve over time.

Shared Responsibility Model

When consuming cloud services, the shared responsibility model governs the provider's scope of responsibility versus that of the consumer. When other providers are added to those relationships, the simple two-party shared responsibility model becomes more complex. Below is illustrated how the shared responsibility model changes with the cloud service model being used.

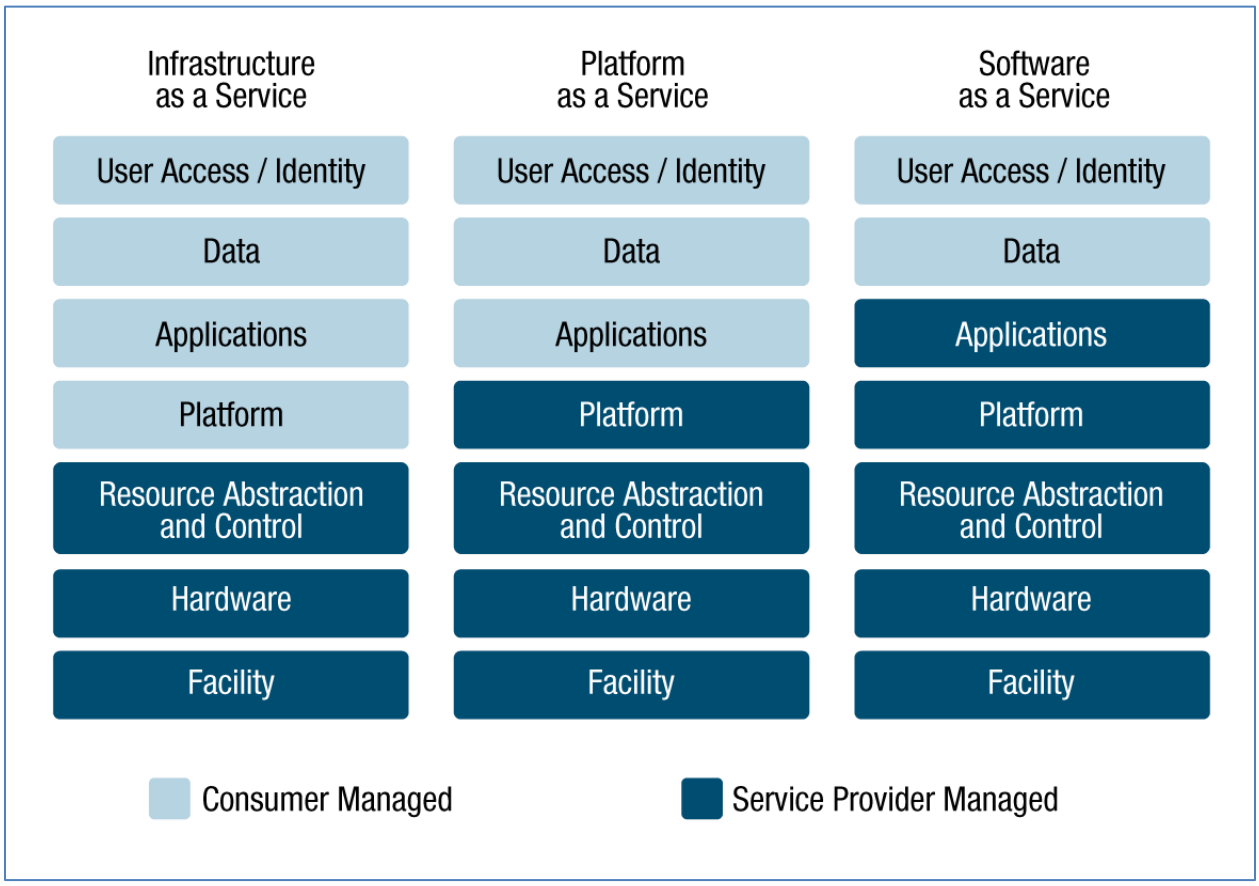

Figure 2 Shared Responsibility Model

When one or more managed services providers are added to the shared responsibility model, it is important to understand how the shared responsibility model changes and the scope of responsibility each assumes. This will be important not only for accountability of performance, but also security assessment activities.

The roles and responsibilities of the consumer (the GC), the managed service provider(s), and the cloud service provider will differ depending upon the requirements of the request for proposal.

For example, consider an application services provider, a type of managed service provider, who uses the services of a public cloud Infrastructure-as-a-Service provider (IaaS) to host software and platforms. In this type of arrangement, the responsibility for user access and data quality may rest with the GC. Management of the hosted software as well as service management, may rest with the managed service provider. If there is an issue with the security or performance of the CSP, the MSP would have contractual responsibility for those issues. This does not mean; however, the GC abdicates accountability for compliance and oversight of all suppliers' activities and services.

	Responsibility
User Access/Identity	**GC**
Data	**GC**
Applications	**MSP**
Platform (Middleware, OS, Resources)	**MSP**
Resource Abstraction And Control	**CSP**
Hardware (Compute, Storage, Network)	**CSP**
Facility	**CSP**

Table 1 Distribution of Cloud-based Managed Service Responsibilities Example

The GC holds the MSP responsible for the performance and security of the service through contractual terms. The MSP must demonstrate compliance to the GC's security requirements through a security assessment process.

As the CSP is a sub-contractor of the MSP, the CSP must also be compliant to the GC's security requirements for its scope of services in accordance with the Direction on Secure Use of Commercial Cloud Services. The MSP will leverage the security assessment artefacts of the CSP, combined with the security assessment artefacts of its own services, to demonstrate compliance to the GC's security requirements.

Common Misconceptions

1. Managed Services are not the same as Software-as-a-Service

   A common misconception that exists is hosting commercial off-the-shelf software on a public cloud Infrastructure-as-a-Service (IaaS) managed by a private or public sector managed services vendor is Software-as-a-Service.

   Public Cloud IaaS + Managed Services + Software**! =** Software-as-a-Service

   This misconception, however, can lead to a misunderstanding of roles and responsibilities and capabilities. It is important to understand that a SaaS is a multi-tenant service meant for consumption by organizations other than just the Government of Canada. Service Level Agreements, and the solution itself is provided to many consumers equally. SaaS offerings are highly commoditized and resist tailoring for the GC. In a managed service, the GC is consuming a solution built and operated for the GC. It can be tailored specifically for the GC.

   The key is to under the scope of responsibility of each provider.

2. Cloud Security Certifications Extends to the Managed Service Provider

   A common misconception that exists is when a managed service or SaaS provider hosts its services on a public cloud IaaS provider whose services have been assessed for the GC, that certification and assessment extend to the managed service or SaaS provider. In fact, the managed service provider or SaaS provider inherits the security controls of the IaaS provider, but the scope of the service provided by the other providers must still be assessed.

Guidance

1. **Assume all procured services include cloud services in their supply chain**

   - Assume any procurement process will attract responses from a managed services provider that will use technology to deliver their services, even if the procurement is limited to business process delivery.
   - Assume all procurements that may include technology will deliver that technology using cloud services.

2. **Include contract clauses in the event suppliers include cloud services**

   - Clauses should be included in all managed services contracts where the provider is processing or storing GC information. Cloud service providers should demonstrate compliance to the Direction on Secure Use of Commercial Cloud Services

3. **Look past the marketing terms**

   - Terms such as cloud service provider, managed service provider, SaaS and others are broadly applied business terms. Do not rely on product and service labeling alone to determine the type

of service agreement you are choosing.

4. **Understand each providers' security responsibilities in the relationship**

   - Understand your roles and responsibilities with respect to the shared responsibility model.
   - Identify and know the different stakeholders' security policies, practices, certification and they how align with GC security policies. A Security Assessment and Authorization of each provider's personnel, operations, policies, and services is required.

Acronyms

CCCS	Canadian Centre for Cyber Security
CSP	Cloud Service Provider
GC	Government of Canada
IaaS	Infrastructure as a Service
ISO	International Organization for Standardization
IT	Information Technology
MSP	Managed Service Provider
OS	Operating System
PaaS	Platform as a Service
SaaS	Software as a Service
SLA	Service Level Agreement
SOC2	Service Organization Control 2
SSC	Shared Services Canada