Shared Services Canada

Cloud Product Management and Services

Connectivity Readiness Process

Version 1.5

GCDOCS <# 68861147>

2020-12-01

Revision History

| Version Number | Description | Date Modified | Author |
| --- | --- | --- | --- |
| 1.0 | Original Version (taken from TBS draft – Scott Levac) | 2020-02-17 | TBS OCIO |
| 1.1 | Edits by Cloud Operations | 2020-02-28 | SSC Cloud |
| 1.2 | Edits by TBS OCIO | 2020-02-28 | TBS OCIO |
| 1.3 | Changes/Edits suggested by CBSA Cloud Team | 2020-03-06 | SSC Cloud with CBSA |
| 1.4 | Changed CSP field to be free-form text (formerly check box) | 2020-10-23 | SSC Cloud |
| 1.5 | Added ITAM and UTM firewall requirement. | 2020-11-30 | SSC Cloud |
|  |  |  |  |

Table of Contents

[1 Purpose 1](#_Toc34985505)

[2 Process Overview 1](#_Toc34985506)

[2.1 Obtain Cloud Account 1](#_Toc34985507)

[2.2 Apply Guardrails 2](#_Toc34985508)

[2.3 Obtain Cloud Infrastructure ATO 2](#_Toc34985509)

[2.4 Connectivity Readiness 3](#_Toc34985510)

[2.4.1 Connection Agreement 3](#_Toc34985511)

[2.4.2 Cloud Connectivity Readiness Checklist 3](#_Toc34985512)

[2.5 Deploy Hybrid Cloud Solutions 3](#_Toc34985513)

[2.6 Operate and Maintain 3](#_Toc34985514)

[3 Frequently Asked Questions: 5](#_Toc34985515)

[Appendix A – Cloud Connectivity Readiness Checklist 8](#_Toc34985516)

[Appendix B – Cloud Connectivity Readiness Checklist (Example) 10](#_Toc34985517)

[Appendix C – Acronyms and Glossary 13](#_Toc34985518)

[List of Acronyms 13](#_Toc34985519)

# Purpose

Departments have a requirement to establish a Hybrid IT model. On January 31st, 2020, the GC Enterprise Architecture Review Board (EARB) endorsed a recommendation to have departments demonstrate cloud connection readiness prior to establishing an interconnection between a departmental cloud environment and GC data centers. Departments who have completed the cloud readiness activities will be prioritized for onboarding. The readiness process is an extension of the activities that already exist as part of the Cloud PB Operationalization Framework, including implementing and validating the mandatory cloud [guardrails](https://github.com/canada-ca/cloud-guardrails).

Departments will be able to view the results of their Cloud Connectivity Readiness Assessments on the TBS OCIO [Cloud Information Centre](https://wiki.gccollab.ca/cloud).

# Process Overview

To avoid departments being on-boarded to the Cloud eXchange Provider (CXP) and not fully exploiting its capability, departments will demonstrate readiness to consume the CXP service.

The Cloud and Computing Network of Expertise (CCNE) was engaged to review a proposed readiness process. In this section, we will elaborate on the responsibilities of the department as illustrated in Figure 1, below.

**Figure 1: Departmental Role in Cloud Operationalization Framework**



Figure 1 is an extract of Slide 5 of the GC EARB [Readiness and Prioritization for CXP Connectivity](https://gcconnex.gc.ca/file/download/59833196).

## Obtain Cloud Account

The department submits a request to obtain a cloud account for IaaS/PaaS cloud services with a GC-approved Cloud Service Provider (CSP) via the [GC Cloud Broker](https://cloud-broker.canada.ca/). Each client has been assigned two “designated users”, appointed by the departmental CIO, who has access to the request portal and can make requests on behalf of that client.

Departments can request a range of IP addresses to be assigned to them, as per SSC [Cloud IPAM Strategy](https://gccollab.ca/file/view/3690502/encloud-internet-protocol-address-management-cloud-ipamfrgestion-des-adresses-de-protocole-internet-dans-le-cloud-cloud-ipam). It is critical that departments integrate the IP Addresses provided into their future designs as this will facilitate network routing between their cloud environment and GC networks.

## Apply Guardrails

As per the Cloud PB Operationalization Framework, departments and agencies who are in-scope of the [Policy on Service and Digital](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603), must implement the enterprise-wide mandatory, minimum, initial 30-day [GC Cloud Guardrails](https://github.com/canada-ca/cloud-guardrails).

The guardrails are a subset of the recommended baseline controls for cloud, in accordance with the [Direction on the Secure Use of Commercial Cloud Services: SPIN 2017-02](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-secure-use-commercial-cloud-services-spin.html) and the [GC Security Control Profile for Cloud-based GC Solutions for Protected B, Medium Integrity, Medium Availability (PBMM)](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/government-canada-security-control-profile-cloud-based-it-services.html).

The guardrails should be applied based on [cloud usage profiles](https://www.gcpedia.gc.ca/gcwiki/images/8/84/GC_Cloud_Guardrails.pdf). Where possible, GC approved templates (i.e. GC Accelerators) should be leveraged. Using the GC Accelerators will aid in deploying Infrastructure as Code (IaC) which incorporates required technical guardrails.

The GC Accelerators can be found here:

AWS: <https://github.com/canada-ca/cloud-guardrails-aws>

Azure: <https://github.com/canada-ca/cloud-guardrails-azure>

Verification that the guardrails have been implemented is conducted by SSC Cloud Operations. Tools to support automated compliance checks are available in the github repositories referenced above.

Specifically for Guardrail 8, [*Segment and Separate*](https://github.com/canada-ca/cloud-guardrails/blob/master/EN/08_Segmentation.md), a firewall must be selected that has Virtual Private Network (VPN) capabilities including encryption algorithms compliant with the [*GC Encryption Standards*](https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111). Having a firewall or Unified Threat Management (UTM) device with this capability is a prerequisite for connectivity to the SSC Secure Cloud-to-Ground Service (GC TIP and GC CAP). Several offerings which satisfy this requirement can be found in the GC Cloud Marketplace.

## Obtain Cloud Infrastructure ATO

Departments are expected to continue to apply graduated safeguards that are commensurate with the risks to their information and IT assets, with more rigorous safeguards as asset values, service delivery requirements, and threats to confidentiality, availability or integrity increase.

An initial starting point for the security controls for the cloud platform layer (your cloud environment), as a subset of the GC Cloud PBMM profile, will be made available to departments:

* For Azure, the starting point is made available via the [Canada PBMM Blueprint](https://azure.microsoft.com/en-ca/updates/new-canada-federal-pbmm-azure-blueprint-is-now-available/).
* For AWS, the ***Landing Zone*** is pre-configured by the vendor for all GC clients.

An iterative approach to designing, building, and assessing your cloud environment is expected. As part of this systems engineering activities, evidence will be generated to provide assurance for the implementation of the controls.

The use of the draft [Naming and Tagging Strategy](https://gccollab.ca/file/view/3634499/ennaming-and-tagging-standardsfr) will also help to ensure that the various cloud usage profiles that may exist within a cloud tenant is appropriately labelled and the guardrails and controls applied.

Performing a Security Assessment and Authorization (SA&A) of the cloud infrastructure will facilitate a security inheritance model that can be leveraged by future information system deployments. This assessment must be signed-off by the appropriate authorities within the organization.

Departments are expected to provide evidence such as a signed authorization letter to demonstrate that the organization has approved the use of the cloud infrastructure at the time of signing the [Interconnectivity Security Agreement](https://wiki.gccollab.ca/File:Interconnection_Security_Agreement_for_Cloud_Connectivity_v1.2.docx).

Treasury Board Secretariat has made some of their Azure [security assessment documentation](https://gccode.ssc-spc.gc.ca/GCCloudEnablement/Microsoft/tree/master/TBS%20Cloud%20Environment) available for other departments to leverage.

## Connectivity Readiness

This activity requires that the appropriate agreements are signed and network flow details are provided.

### Connection Agreement

An Interconnection Security Agreement (ISA) specifies the technical and security requirements of the interconnection. It also includes the responsibilities of the organizations and defines the service levels and system availability. The ISA document is published at the [Cloud Information Centre](https://wiki.gccollab.ca/GC_Cloud_Infocentre).

**\* The** [**Interconnection Security Agreement**](https://gccollab.ca/file/view/3741474/endraft-interconnection-security-agreement-for-cloud-connectivityfr) **must be completed, signed, and returned to** [**ssc.cloud-infonuagique.spc@canada.ca**](mailto:ssc.cloud-infonuagique.spc@canada.ca) **with the subject line: “Interconnection Security Agreement”.**

### Cloud Connectivity Readiness Checklist

Department must be able to describe the application and network flows using the template in Appendix A. Details should be sufficient to allow SSC to define network traffic flows from a cloud environment to applications and services inside legacy or enterprise data centre(s). This should include IP addresses, ports and protocols. Don’t forget to include any traffic flows for supporting services such as identity stores.

**\* The Cloud Connectivity Readiness Checklist must be completed, encrypted, and returned to** [**ssc.cloud-infonuagique.spc@canada.ca**](mailto:ssc.cloud-infonuagique.spc@canada.ca) **with the subject line: “Cloud Connectivity Readiness Checklist”.**

Once the Cloud PB Operationalization Framework, signing of the agreement, and Cloud Connectivity Readiness Checklist are completed, you will have provided SSC all the required artefacts to demonstrate completion of the readiness process.

Please note: Departments can request a range of IP addresses to be assigned to them, as per SSC [Cloud IPAM Strategy](https://gccollab.ca/file/view/3690502/encloud-internet-protocol-address-management-cloud-ipamfrgestion-des-adresses-de-protocole-internet-dans-le-cloud-cloud-ipam).

## Deploy Hybrid Cloud Solutions

At this point connectivity activities will start, or if there is insufficient capacity to perform capacity, you will be prioritized and scheduled for connectivity.

## Operate and Maintain

Departments must continuously manage the security risks to their information and IT assets including continuously monitoring cloud-based services as an essential component on effective IT security strategy. Continuous monitoring encompasses activities such as:

* monitoring threats and vulnerabilities,
* reviewing the results of system monitoring,
* self-assessment and internal audits, and,
* developing corrective action plans where necessary to remediate deficiencies.

# Frequently Asked Questions:

Q1: Why is a readiness process needed?

The demand to onboard to the Cloud eXchange Provider (CXP) is higher than resources available to onboard departments. For this reason, the readiness process was created to ensure those departments who are onboarding to the CXP are ready to fully exploit its capabilities from the start.

Q2: What do you mean by connectivity?

In the content of this document, connectivity being discussed is connecting to P/IaaS cloud environments. This is not about SaaS connectivity which has a different plan. Connectivity is meant to address one or more of the following challenges for departments:

1. A hybrid architecture is required where applications in the cloud communicate with applications in an SSC-managed data centre.
2. Current internet gateways have insufficient bandwidth available to support a department’s bandwidth needs for cloud activities.
3. The network latency of the connection between the cloud and the ground is of acceptable levels.

Most organizations are not yet experiencing the second issue. While internet gateways experience significant stress, most departments’ cloud usage is not sufficient scale to fully saturate the internet gateways. The focus, is typically the first scenario. These are usage profiles 5 and 6.

Q3. What is a CXP?

The Cloud eXchange Provider (CXP) is a service that connects the edge of the GC’s network to cloud service provider’s network. The GC will leverage a CXP which aggregates many cloud provider’s networks in one location, thus simplifying efforts. Departments are expected to complete the configuration for the dedicated connection by establishing the CSP services such as ExpressRoute or DirectConnect.

Q4. What if I want to connect multiple cloud environments across multiple providers?

Each environment is going to have its own unique IP ranges, security assessment, etc… While you could proceed through the readiness process with two environments in parallel, you are doubling the work. Ask yourself if you’re ready to fully operate both environments and if you’re ready to fully exploit the CXP’s capabilities across both environments. It may be preferred to tackle your highest priority environment first.

Q5. Will you review my security assessment?

No. Security assessments are a departmental responsibility to manage. It is your organization who decides its own risk tolerance.

Q6. Does my security assessment include all my applications?

No. what is expected here is your cloud environment is being assessed prior to migrating or building applications.

Q7. Why do I need to be prioritized?

If a number of departments complete the readiness process and there is a backlog of demand, prioritization will be applied.

Q8. What is the Operationalization Framework?

The Operationalization Framework was endorsed by GC EARB on September 19th, 2019. Prior to opening up the Cloud Services Framework to departments, the GC implemented a set of minimum, mandatory guardrails that all departments must apply to their environments to ensure minimum protections are in place.

Q9. Will this help me adopt Office 365?

No. A different network architecture solution called an Internet eXchange Provider (IXP) is being deployed for SaaS and large internet content providers.

Q10. Will the readiness process disappear?

Possibly, one day. Looking back at Question 1, the readiness process is a way of making sure those being on-boarded to the CXP are ready to use the CXP’s capabilities. As demand to onboard is higher than the supply available to onboard organizations, the readiness process was created. If demand drops or onboarding capacity increases or becomes more automated, the need for the readiness process is greatly reduced.

Q11. How will SSC know I’m ready to onboard?

By signing the required agreements and completing the Operationalization Framework with Shared Services Canada, you have completed all the required activities. One of two things will happen:

1. You will be prioritized
2. Connectivity activities will start

Q12. What if I need a service level higher than that stated in the service agreement?

Then, you need a different service. The service level agreement is meant to articulate what level you can expect and build your services on.

Q13. How long does is take from demonstrating readiness to having connectivity up and running?

Assuming there is no onboarding backlog, past experience has shown that connectivity takes about two months to complete.

# Appendix A – Cloud Connectivity Readiness Checklist

**Evaluation column to be filled out by assessor only.**

|  |  |
| --- | --- |
| **Project, Initiative or Application Overview** | **Evaluation** |
| Name of Department: \_\_\_\_\_\_\_\_\_\_\_\_\_  GC IT Project/Activity Name (TBS Clarity): \_\_\_\_\_\_\_\_\_\_\_\_\_  GC IT Project/Activity ID# (TBS Clarity): \_\_\_\_\_\_\_\_\_\_\_\_\_  Description of Project, Initiative or Application: (2-3 paragraphs) | Pass:  Fail: |
| **Obtain Cloud Account** | **Evaluation** |
| Have the two designated users received their GC Cloud Broker Portal accounts?  Please provide your cloud supply CRM Request #: \_CRXXXXX\_\_\_\_\_\_\_\_\_\_\_\_  Cloud Service Provider (select one): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Cloud Service Model: IaaS  PaaS  SaaS  IPAM Reservation Completed: Yes ☐ No ☐ | Pass:  Fail: |
| **Apply Guardrails** | **Evaluation** |
| Have you submitted the evidence package for the 30-day Cloud Guardrails?  Submission Date: \_\_\_\_\_\_\_\_\_\_\_\_\_  Firewall/UTM with VPN-Capabilities Deployed: Yes ☐ No ☐ | Pass:  Fail: |
| **Complete Cloud Infrastructure ATO** | **Evaluation** |
| Have you completed your Cloud ATO? | Pass:  Fail: |
| **Connectivity Readiness** | **Evaluation** |
| Have you signed and submitted the Interconnection Security Agreement? | Pass:  Fail: |
| **Connectivity Patterns (**[**reference**](https://www.gcpedia.gc.ca/gcwiki/images/7/75/GC_Cloud_Connection_Patterns.pdf)**)** | **Evaluation** |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | A1 | A2 | A3 | A4 | A5 | A6 | | B1 | B2 | B3 | B4 | B5 | B6 | | C1 | C2 | C3 | C4 | C5 | C6 | | D1 | D2 | D3 | D4 | D5 | D6 | | E1 | E2 | E3 | E4 | E5 | E6 | | Pass:  Fail: |
| **Network Flow Table** | **Evaluation** |
| |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **Flow #** | **Application Flow Description** | **Source Zone** | **Source Server Name** | **Source IP** | **Load Balancers, Proxy Required?** | **Destination Zone** | **Destination Server Name** | **Destination IP** | **Port(s)** | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | | Pass:  Fail: |
| **Data Flow Diagram** | **Evaluation** |
| [Insert diagram here] | Pass:  Fail: |
| **Administration Section Only** | **Evaluation** |
| Overall results | Pass:  Fail: |

# Appendix B – Cloud Connectivity Readiness Checklist (Example)

This annex provides an example of the checklist based on a fictitious scenario, for illustration purposes.

|  |  |
| --- | --- |
| **Project, Initiative or Application Overview** | **Evaluation** |
| Name of Department: \_\_\_SSC\_\_\_\_\_\_\_  GC IT Project/Activity Name (TBS Clarity): \_\_GC Reviews\_\_\_\_\_\_\_\_\_  GC IT Project/Activity ID# (TBS Clarity): \_\_\_30887\_\_\_\_\_\_\_\_  Description of Project, Initiative or Application:  The new application will enable Canadians to submit reviews on GC products and services from anywhere in Canada. Citizens will also be able to browse/search the review database by product name, category, or rating. The application was developed by the department in Q2 2019. The user-trial was completed in September in an unclassified cloud tenant with favourable results. The department is now seeking approval to proceed with advancing the application to Production.  The application will be leverage IaaS services in the public cloud. The cloud platform will be Windows-based (IIS, .NET, MS SQL) and will exchange data with Apache/J2EE applications on the ground. This will allow for a smooth transition of functionality from the Legacy Data Centre to the Cloud. When all functionality has been transitioned (Q3 next fiscal), the Legacy systems will be retired.  Once in production, all new reviews submitted will be stored in the cloud platform. Database searches will query records from the cloud database and the legacy database (on the ground). As records are retrieved from the ground (via searches), they will be stored (cached) in the cloud database and marked for deletion in the legacy database. This mechanism will result in the migration of data from the ground to the cloud based on frequency and demand. | Pass:  Fail: |
| **Obtain Cloud Account** | **Evaluation** |
| Have the two designated users received their GC Cloud Broker Portal accounts?  Please provide your cloud supply CRM Request #: \_CR7883457\_\_\_\_\_\_\_\_\_\_\_\_  Cloud Service Provider (select one): \_\_\_\_\_\_Microsoft Azure\_\_\_\_\_\_\_\_\_  Cloud Service Model: IaaS  PaaS  SaaS | Pass:  Fail: |
| **Apply Guardrails** | **Evaluation** |
| Have you submitted the evidence package for the 30-day Cloud Guardrails?  Submission Date: \_\_2020-02-26\_\_\_\_\_\_\_\_\_\_\_ | Pass:  Fail: |
| **Complete Cloud Infrastructure ATO** | **Evaluation** |
| Have you completed your Cloud ATO? | Pass:  Fail: |
| **Connectivity Readiness** | **Evaluation** |
| Have you signed and submitted the Interconnection Security Agreement? | Pass:  Fail: |
| **Connectivity Patterns (**[**reference**](https://www.gcpedia.gc.ca/gcwiki/images/7/75/GC_Cloud_Connection_Patterns.pdf)**)** | **Evaluation** |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | A1 | A2 | A3 | A4 | A5 | A6 | | B1 | B2 | B3 | B4 | B5 | B6 | | C1 | C2 | C3 | C4 | C5 | C6 | | D1 | D2 | D3 | D4 | D5 | D6 | | E1 | E2 | E3 | E4 | E5 | E6 | | Pass:  Fail: |
| **Network Flow Table** | **Evaluation** |
| |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **Flow#** | **Application Flow Description** | **Source Zone** | **Source Server Name** | **Source IP** | **Load Balancers, Proxy Required?** | **Destination Zone** | **Destination Server Name** | **Destination IP** | **Port(s)** | | 1 | Internet to cloud web traffic (outside) | Public Zone (PZ) | Any | Any | Yes, VIP | Core Network Services (Cloud) | LB1 | 201.141.10.10 | 443/tcp | | 2 | Internet to cloud web traffic (inside) | Core Network Services (Cloud) | LB1 | 172.16.0.1 | Yes | Cloud PAZ | www1 – www5 | 172.16.1.3-172.16.1.8  (scale set) | 80/tcp | | 3 | IIS to .NET App Pool | Cloud PAZ | www1 – www5 | 172.16.1.3-172.16.1.8 | No | Cloud App-RZ | App1-App7 | 172.16.2.3 – 172.16.2.10  (scale set) | 80/tcp | | 4 | .NET to SQL | Cloud App-RZ | App1-App7 | 172.16.2.3– 172.16.2.10 | No | Cloud DB-RZ | SQL1 | 172.16.3.5 | 1433/tcp | | 5 | .NET post to LB1 | Cloud App-RZ | App1-App7 | 172.16.2.3– 172.16.2.10 | Yes | Core Network Services (Cloud) | LB1 | 172.16.0.1 | 443/tcp | | 6 | LB1 post to REV Proxy | Core Network Services (Cloud) | LB1 | 172.16.0.1 | Yes, SNAT | Ground PAZ | Apache1 | 142.22.41.3 | 443/tcp | | 7 | Apache1 to JavaApp2 Post | Ground PAZ | Apache1 | 142.22.41.3 | No | Ground App-RZ | JavaApp2 | 142.22.44.3 | 443/tcp | | Pass:  Fail: |
| **Data Flow Diagram** | **Evaluation** |
|  | Pass:  Fail: |
| **Administration Section Only** | **Evaluation** |
| Overall results | Pass:  Fail: |

# Appendix C – Acronyms and Glossary

**Glossary**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| CXP | Cloud eXchange Providers are 3rd-party WAN-hosting companies that provide cost-effective, dedicated, low latency, high-bandwidth connectivity to multiple/simultaneous Cloud Service Providers (CSPs). |
| IaaS | Infrastructure as a Service: cloud-based services such as storage, networking, and virtualization. |
| PaaS | Platform as a Service: hardware and software tools available over the internet allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app. |
| Private Cloud | The private cloud is defined as computing services offered either over the Internet or a private internal network and only to select users instead of the general public. Private cloud can be deployed “on premise” in a data centre behind a firewall. |
| Public Cloud | The public cloud is defined as computing services offered by third-party providers over the public Internet, making them available to anyone who wants to use or purchase them. |
| SaaS | Software as a Service is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. SaaS applications are also known as “Web-based” software, “on-demand” software and “hosted” software. |

## List of Acronyms

| Acronym | Full Name |
| --- | --- |
| CCNE | Cloud and Computing Network of Expertise |
| CSP | Cloud Service Provider |
| CXP | Cloud eXchange Provider |
| GC EARB | Government of Canada Enterprise Architecture Review Board |
| IaC | Infrastructure as Code |
| PaaS | Platform as a Service |
| IaaS | Infrastructure as a Service |
| SaaS | Software as a Service |
| SA&A | Security Assessment and Authorization |