

**Government of Canada**

**Cloud Guardrails**

**December 9, 2019**

GCdocs 36578005

**Contents**

1. Introduction ............................................................................................................................. 1

1.1 Purpose ........................................................................................................................ 1

1.2 Scope............................................................................................................................ 1

2. Cloud Guardrails ...................................................................................................................... 3

2.1 Initial 30 Days............................................................................................................... 3

2.2 Post 30 Days............................................................................................................... 10

3. Cloud Usage Profiles .............................................................................................................. 12

3.1 Overview of Cloud Usage Profiles ............................................................................. 12

3.2 Guardrails Mapping to Cloud Usage Profiles............................................................. 12

4. References ............................................................................................................................. 14

4.1 Related policy instruments ........................................................................................ 14

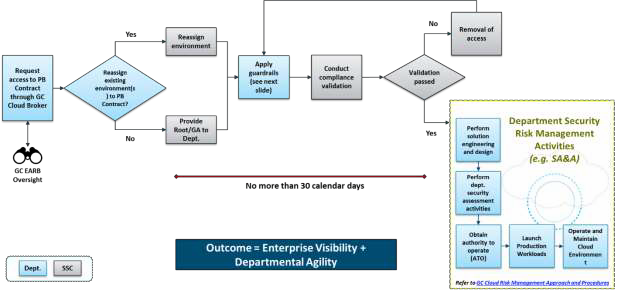
4.2 Additional references ................................................................................................ 14

**1. Introduction**

**1.1 Purpose**

In August 2019, the Government of Canada (GC) established supply contracts for Protected B Cloud Services with AWS Canada and Microsoft Azure. In order for the GC to consume this supply in secure and responsible fashion, the Chief Technology Officer of the GC deemed that an underlying operationalization framework was required. An operationalization framework was established and

endorsed by [GC EARB](https://gcconnex.gc.ca/file/view/53195105/enabling-secure-access-to-protected-b-cloud-services-gcearb-sept-19-2019?language=en) in September 2019 establishing a set of minimal security controls and architecture prior to departments consuming PB supply. The following figure provides an overview of the framework.



**1.2 Scope**

This document focuses on a preliminary set of baseline security controls to ensure that the cloud service environment has a minimum set of configurations for the cloud environment.

It provides a starting point for project teams and was selected to achieve the following objectives:

 comply with the applicable mandatory procedures in the  *[Directive on Security Management](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611)*

 meet the requirements of the [Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-secure-use-commercial-cloud-services-spin.html)

 address the Communications Security Establishment’s (CSE’s) [Top 10 Security Actions](https://www.cse-cst.gc.ca/en/top10)

 align with [*Government of Canada Security Control Profile for Cloud-Based GC Services*](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/government-canada-security-control-profile-cloud-based-it-services.html)

 focus on the selection of security controls to those implemented in software components of information system solutions

• achieve threat protection objectives specified in the [ITSG-33 generic PBMM profile](https://cyber.gc.ca/en/guidance/annex-4a-profile-1-protected-b-medium-integrity-medium-availability-itsg-33) and the

[*Government of Canada Security Control Profile for Cloud-Based GC Services*](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/government-canada-security-control-profile-cloud-based-it-services.html)

**2. Cloud Guardrails**

**2.1 Initial 30 Days**

This section describes a set of minimum guardrails that are part of the GC’s operationalization framework. The following table outlines the key guardrails that need to be enabled within the GC- specified initial period (e.g. 30 days).

Departments are responsible for implementing the key considerations identified in the table below. Validation of the guardrails will be performed by SSC Cloud Services Directorate. The [Standard Operating Procedure (SOP) on Validating Cloud Guardrails](https://www.gcpedia.gc.ca/gcwiki/images/1/19/SOP_for_Validating_Cloud_Guardrails.pdf) has been developed to support this activity.

|  |  |
| --- | --- |
| **Guardrail** | **Description** |
| **1. Protect Root / Global**  **Admins Account** | **Objective**  Protect root or master account used to establish the cloud service. |
| **Key Considerations**  Implement multi-factor authentication (MFA) mechanism for root/master account.  Ref: [Evidence document](http://gcdocs2/otcsdav/nodes/389973749/IRCC%20Asylum%20Application%20-%20Control%20Evidence%20Report.docx) **(2.19 Conditional Access Policies, Page 103)**  Document a break glass emergency account management procedure.  Including names of users with root or master account access.  Ref: [Evidence document](http://gcdocs2/otcsdav/nodes/389973749/IRCC%20Asylum%20Application%20-%20Control%20Evidence%20Report.docx) **(2.1.2 AC-2, Page 11)**  Obtain signature from Departmental Chief Information Officer (CIO) and Chief Security Officer (CSO) to confirm acknowledgement and approval of the break glass emergency account management procedures. **(Not Found in Evidence Document)**  Implement a mechanism for enforcing access authorizations. [Evidence document](http://gcdocs2/otcsdav/nodes/389973749/IRCC%20Asylum%20Application%20-%20Control%20Evidence%20Report.docx) **(1.1 Background, Page 1)**  Configure appropriate alerts on root/master accounts to detect a potential compromise, in accordance with the [GC Event Logging Guidance.](https://www.gcpedia.gc.ca/gcwiki/images/e/e3/GC_Event_Logging_Strategy.pdf) |
| **Validation**  Confirm policy for MFA is enabled through screenshots and compliance reports. [Evidence document](http://gcdocs2/otcsdav/nodes/389973749/IRCC%20Asylum%20Application%20-%20Control%20Evidence%20Report.docx) **(2.19 Conditional Access Policies, Page 103)**  Confirm that an attestation letter of the emergency break glass procedure has been signed by the Departmental CIO and CSO. **(Not Found in Evidence Document)** |
| **Additional Considerations**  Leverage enterprise services such as Administrative Access Control System (AACS) for Privileged Access Management (PAM), Attribute-based access control (ABAC). (**Not Met, Asylum Environment SRTM SAAS Document, MA-5 Control)** |
| **References**  1) [SPIN 2017-01,](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html) subsection 6.2.3  2) CSE Top 10 #3 |

|  |  |
| --- | --- |
|  | 3) Refer to the [Recommendations for Two-Factor User Authentication Within](https://intranet.canada.ca/wg-tg/rtua-rafu-eng.asp)  [the Government of Canada Enterprise Domain](https://intranet.canada.ca/wg-tg/rtua-rafu-eng.asp)  4) Refer to the [template](https://gcconnex.gc.ca/file/view/55010566/break-glass-emergency-account-procedure-departments-can-use-to-develop-their-emergency-access-management-controls-for-cloud?language=en) for a break glass emergency account management procedure.  5) Refer to the [GC Event Logging Guidance.](https://www.gcpedia.gc.ca/gcwiki/images/e/e3/GC_Event_Logging_Strategy.pdf)  6) Related security controls: AC-2, AC-2(1), AC-3, AC-5, AC-6, AC-6(5),  AC-6(10), AC-7, AC-9, AC-19, AC-20(3), IA-2, IA-2(1), IA-2(2), IA-2(11), IA-4, IA-5, IA-5(1), IA-5(6), IA-5(7), IA-5(13), IA-6, IA-8 |
| **2. Management of**  **Administrative Privileges** | **Objective**  Establish access control policies and procedures for management of administrative privileges. |
| **Key Considerations**  Document a process for managing accounts, access privileges, and access credentials for organizational users, non-organizational users (if required), and processes based on the principles of separation of duties and least privilege (for example, operational procedures and active directory). **(2.1 Account Management (AC), 2.7 Identity & Authentication (IA))**  Implement a mechanism for enforcing access authorizations.  Implement a mechanism for uniquely identifying and authenticating organizational users, non-organizational users (if applicable), and processes (for example, username and password).  Implement a multi-factor authentication mechanism for privileged accounts (for example, username, password and one-time password) and for external facing interfaces.  Change default passwords.  Ensure that no custom subscription owner roles are created.  Configure password policy in accordance with [GC Password Guidance.](https://www.canada.ca/en/government/system/digital-government/password-guidance.html)  Minimize number of guest users; add only if needed.  Determine access restrictions and configuration requirements for GC- issued endpoint devices, including those of non-privileged and privileged users, and configure access restrictions for endpoint devices accordingly.  **Note:** Some service providers may offer configuration options to restrict endpoint device access. Alternatively, organizational policy and procedural instruments can be implemented to restrict access. |
| **Validation**  Confirm policy for MFA is enabled through screenshots and compliance reports.  Confirm that a privileged account management plan and process has been documented.  Confirm password policy aligns with [GC Password Guidance](https://www.canada.ca/en/government/system/digital-government/password-guidance.html) as appropriate. |

|  |  |
| --- | --- |
|  | **Additional Considerations**  Leverage enterprise services such as Administrative Access Control System (AACS) for Privileged Access Management (PAM), Attribute-based access control (ABAC). |
| **References**  1) [SPIN 2017-01,](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html) subsection 6.2.3  2) CSE Top 10 #3  3) Refer to [CCCS ITSP.30.031 V2 User Authentication Guidance for](https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3)  [Information Technology Systems](https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3)  4) Refer to the [Guidance on Cloud Authentication for the Government of](https://intranet.canada.ca/wg-tg/cagc-angc-eng.asp)  [Canada](https://intranet.canada.ca/wg-tg/cagc-angc-eng.asp)  5) Refer to the [Recommendations for Two-Factor User Authentication Within the Government of Canada Enterprise Domain](https://intranet.canada.ca/wg-tg/rtua-rafu-eng.asp)  6) Related security controls: AC-2, AC-2(1), AC-3, AC-5, AC-6, AC-6(5),  AC-6(10), AC-7, AC-9, AC-19, AC-20(3), IA-2, IA-2(1), IA-2(2), IA-2(11), IA-4, IA-5, IA-5(1), IA-5(6), IA-5(7), IA-5(13), IA-6, IA-8 |
| **3. Cloud Console Access** | **Objective**  Limit access to GC-approved IP addresses and authorized users (e.g. developers, application owners, etc.) |
| **Key Considerations**  Implement multi-factor authentication mechanism for privileged accounts and remote network (cloud) access.  Determine access restrictions and configuration requirements for GC- issued endpoint devices, including those of non-privileged and privileged users, and configure access restrictions for endpoint devices accordingly.  **Note:** Some service providers may offer configuration options to restrict endpoint device access. Alternatively, organizational policy and procedural instruments can be implemented to restrict access.  Implement a mechanism for enforcing access authorizations.  Implement password protection mechanisms to protect against password brute force attacks. |
| **Validation**  Confirm policy for MFA is enabled through screenshots and compliance reports. |
| **Additional Considerations**  Leverage enterprise services such as Administrative Access Control System (AACS) for Privileged Access Management (PAM), Attributed-based access control (ABAC). |
| **References** |

|  |  |
| --- | --- |
|  | 1) [SPIN 2017-01,](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html) subsection 6.2.3  2) CSE Top 10 #2  3) Refer to the [Recommendations for Two-Factor User Authentication Within the Government of Canada Enterprise Domain](https://intranet.canada.ca/wg-tg/rtua-rafu-eng.asp)  4) Related security controls: AC-2, AC-2(1), AC-3, AC-5, AC-6, AC-6(5),  AC-6(10), AC-7, AC-9, AC-19, AC-20(3), IA-2, IA-2(1), IA-2(2), IA-2(11), IA-4, IA-5, IA-5(1), IA-5(6), IA-5(7), IA-5(13), IA-6, IA-8 |
| **4. Enterprise Monitoring**  **Accounts** | **Objective**  Create role-based account to enable enterprise monitoring and visibility |
| **Key Considerations**  Assign roles to approved GC stakeholders to enable enterprise visibility.  Roles include billing reader, policy contributor/reader, security reader, and  global reader.  Ensure that multi-factor authentication mechanism for enterprise monitoring accounts is enabled. |
| **Validation**  Confirm presence of GC enterprise role-based accounts created by  Department for GC approved stakeholders.  Confirm that accounts have appropriate read access to Departmental tenant environment. |
| **References**  1) [SPIN 2017-01,](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html) subsection 6.2.3  2) CSE Top 10 #2  3) Related security controls: AC-2, AC-2(1), AC-3, AC-5, AC-6, AC-6(5),  AC-6(10), AC-7, AC-9, AC-19, AC-20(3), IA-2, IA-2(1), IA-2(2), IA-2(11), IA-4, IA-5, IA-5(1), IA-5(6), IA-5(7), IA-5(13), IA-6, IA-8 |
| **5. Data Location** | **Objective**  Establish policies to restrict GC sensitive workloads to approved geographic locations |
| **Key Considerations**  As per the Direction on Electronic Data Residency (ITPIN 2017-02), “All sensitive electronic data under government control, that has been categorized as Protected B, Protected C or is Classified, will be stored in a GC-approved computing facility located within the geographic boundaries of Canada or within the premises of a GC department located abroad, such as a diplomatic or consular mission.” |
| **Validation**  Confirm policy and tagging for data location. |
| **References** |

|  |  |
| --- | --- |
|  | 1) [SPIN 2017-01,](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html) subsection 6.2.3  2) [ITPIN 2017-02](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-electronic-data-residency.html) |
| **6. Protection of Data-at-**  **rest** | **Objective**  Protect data at rest by default (e.g. storage) for cloud-based workloads |
| **Key Considerations**  Seek guidance from privacy and access to information officials within institutions before storing personal information in cloud-based environments.  Implement an encryption mechanism to protect the confidentiality and  integrity of data when data are at rest in your solution’s storage.  Use CSE-approved cryptographic algorithms and protocols.  Implement key management procedures. |
| **Validation**  Confirm policy for encryption (e.g. storage and/or VM based on risk-based assessment). |
| **References**  1) [SPIN 2017-01,](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html) subsection 6.2.4  2) Refer to the cryptography guidance in [ITSP.40.111](https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111) and [ITSP.40.062.](https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.40.062-eng.pdf)  3) Refer to the guidance in [Considerations for Cryptography in Commercial](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/government-canada-consideration-use-cryptography-in-cloud.html)  [Cloud Services.](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/government-canada-consideration-use-cryptography-in-cloud.html)  4) Related security controls: SC-12, SC-13, SC-17, SC-28, SC-28(1) |
| **7. Protection of Data-in-**  **transit** | **Objective**  Protect data transiting networks through the use of appropriate encryption and network safeguards |
| **Key Considerations**  Implement an encryption mechanism to protect the confidentiality and integrity of data when data are in transit to and from your solution.  Use CSE-approved cryptographic algorithms and protocols.  Encryption of data in transit by default (e.g. TLS v1.2, etc.) for all publicly accessible sites and external communications as per the direction on [Implementing HTTPS for Secure Web Connections](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/policy-implementation-notices/implementing-https-secure-web-connections-itpin.html) (ITPIN 2018-01).  Encryption for all access to cloud services (e.g. Cloud storage, Key  Management systems, etc.).  Consider encryption for internal zone communication in the cloud based on risk profile and as per the direction in CCCS network security zoning guidance in [ITSG-22](https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22) and [ITSG-38.](https://cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38)  Implement key management procedures. |
| **Validation** |

|  |  |
| --- | --- |
|  | Confirm policy for secure network transmission. |
| **References**  1) [SPIN 2017-01,](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html) subsection 6.2.4  2) [ITPIN 2018-01](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/policy-implementation-notices/implementing-https-secure-web-connections-itpin.html)  3) Refer to the cryptography guidance in [ITSP.40.111](https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111) and [ITSP.40.062.](https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.40.062-eng.pdf)  4) Refer to the network security zoning guidance in [ITSG-22](https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22) and [ITSG-38.](https://cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38)  5) Refer to the guidance in [Considerations for Cryptography in Commercial](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/government-canada-consideration-use-cryptography-in-cloud.html)  [Cloud Services.](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/government-canada-consideration-use-cryptography-in-cloud.html)  6) Related security controls: SC-8, SC-8(1), SC-12, SC-13, SC-17 |
| **8. Segment and Separate**  **(Doesn't apply for SaaS)** | **Objective**  Segment and separate information based on sensitivity of information |
| **Key Considerations**  Develop a target network security design that considers segmentation via network security zones, in alignment with [ITSG-22](https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22) and [ITSG-38. .](https://cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38) Implement increased levels of protection for management interfaces. |
| **Validation**  Confirm that department has a target network architecture diagram with appropriate segmentation between network zones. |
| **References**  1) [SPIN 2017-01,](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html) subsection 6.2.4  2) CSE Top 10 #5  3) Refer to the network security zoning guidance in [ITSG-22](https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22) and [ITSG-38.](https://cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38)  4) Related security controls: AC-4, SC-7, SC-7(5) |
| **9. Network Security**  **Services** | **Objective**  Establish external and internal network perimeters and monitor network traffic. |
| **Key Considerations**  Ensure that egress/ingress points to and from GC cloud-based environments are managed and monitored. Use centrally provisioned network security services where available.  Implement network boundary protection mechanisms for all external facing interfaces that enforce a deny-all or allow-by-exception policy.  Perimeter security services such as boundary protection, intrusion prevention services, proxy services, TLS traffic inspection, etc. must be enabled based on risk profile, in alignment with GC Secure Connectivity Requirements and [ITSG-22](https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22) and ITSG-38.  Access to Cloud storage shall be limited to authorized source IP addresses only (generally GC only). |

|  |  |
| --- | --- |
|  | **Validation**  Confirm policy for network boundary protection.  Confirm policy for limiting number of public IPs.  Confirm policy for limiting to authorized source IP addresses (e.g. GC IP  addresses). |
| **References**  1) [SPIN 2017-01,](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html) subsection 6.2.4  2) Refer to the network security zoning guidance in [ITSG-22](https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22) and [ITSG-38.](https://cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38)  3) CSE Top 10 #1  4) Related security controls: AC-3, AC-4, SC-5, SC-7, SC-7(5), SI-3, SI-3(7), SI-4 |
| **10. Cyber Defense Services** | **Objective**  Establish MOU for defensive services and threat monitoring protection services. |
| **Key Considerations**  Sign an MOU with CCCS. Contact CCCS to initiate engagement  [CDOServiceDeployments@cyber.gc.ca.](http://gcdocs2/otcsdav/nodes/389973749/mailto%3ACDOServiceDeployments%40cyber.gc.ca)  Implement defensive services including HBS, CBS, and NBS in accordance with CCCS onboarding guidance. |
| **Validation**  Confirmation from CCCS that the MOU has been signed by the Department. |
| **References**  1) [SPIN 2017-01,](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html) subsection 6.3  2) Related security controls: SI-2, SI-4 |
| **11. Logging and monitoring** | **Objective**  Enable logging for the cloud environment and for cloud-based workloads. |
| **Key Considerations**  Implement adequate level of logging and reporting, including a security audit log function in all information systems.  Identify the events within the solution that must be audited in accordance with [GC Event Logging Guidance.](https://www.gcpedia.gc.ca/gcwiki/images/e/e3/GC_Event_Logging_Strategy.pdf)  **Note:** You may need to configure your solution to send the audit log records to a centralized logging facility, if one is available, where existing auditing mechanisms will be applied.  Configure alerts and notifications to be sent to the appropriate contact/team in the organization.  Configure or use an authoritative time source for the time-stamp of the audit records generated by your solution components. |

|  |  |
| --- | --- |
|  | Continuously monitor system events and performance. |
| **Validation**  Confirm policy for event logging is implemented.  Confirm event logs are being generated.  Confirm that security contact information has been configured to receive alerts and notifications. |
| **References**  1) [SPIN 2017-01,](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html) subsection 6.3.1  2) CSE Top 10 #1, 5, 8  3) Refer to [GC Event Logging Guidance](https://www.gcpedia.gc.ca/gcwiki/images/e/e3/GC_Event_Logging_Strategy.pdf)  4) Related security controls: AU-2, AU-3, AU-6, AU-8, AU-9, AU-9(4), AU-12, SI-4 |
| **12. Configuration of Cloud**  **Marketplaces** | **Objective**  Restrict Third-Party CSP Marketplace software to GC-approved products. |
| **Key Considerations**  Only GC approved cloud marketplace products are to be consumed.  Turning on the commercial marketplace is prohibited.  Submit requests to add third-party products to marketplace to SSC Cloud  Broker. |
| **Validation**  Confirm that third-party marketplace restrictions have been implemented. |
| **References**  1) [SPIN 2017-01,](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html) subsection 6.2.5  2) Refer to [GCconnex](https://gcconnex.gc.ca/file/view/53599636/gc-cloud-broker-sci-assessed-marketplace-products-byol-freeware?language=en) for current list of approved marketplace products.  3) Related security controls: CM-2, CM-3, CM-4, CM-5, CM-8, SA-22 |

**2.2 Post 30 Days**

Departments are expected to continue implementing the security requirements as outlined in:

 [Direction on the Secure Use of Commercial Cloud Services: Security Implementation Notice](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-secure-use-commercial-cloud-services-spin.html)

[(SPIN)](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-secure-use-commercial-cloud-services-spin.html)

 [Government of Canada Security Control Profile for Cloud-Based GC Services](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/government-canada-security-control-profile-cloud-based-it-services.html)

Departments should engage with their IT Security Risk Management teams to obtain advice and guidance on integrating security assessment and authorization activities as part of the implementation of the GC cloud environment. The [Government of Canada Cloud Security Risk Management Approach](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/cloud-security-risk-management-approach-procedures.html)

[and Procedures](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/cloud-security-risk-management-approach-procedures.html) outlines activities for Departments to consider as part of the departmental risk management activities.

SSC will perform periodic audits of the Departmental tenant environment to ensure ongoing compliance to the initial 30 days guardrails.

**3. Cloud Usage Profiles**

**3.1 Overview of Cloud Usage Profiles**

The following table describes various profiles for cloud usage by a GC organization.

**Table 3-1 Cloud Usage Profiles**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Profile** | **Description** | **Applicable**  **Cloud Service**  **Model** |
| 1. | **Experimentation/**  **Sandbox** |  Cloud-based services used for experimentation/sandbox   No direct system to system network interconnections required with GC data centers | IaaS, PaaS, SaaS |
| 2. | **Non-sensitive cloud-**  **based services** |  Cloud-based services hosting non-sensitive GC content   No direct system to system network interconnections required with GC data centers | IaaS, PaaS, SaaS |
| 3. | **Sensitive (up to PB)**  **cloud-based services** |  Cloud-based services hosting sensitive (up to Protected B)  information   No direct system to system network interconnections required with GC data centers | IaaS, PaaS, SaaS |
| 4. | **Sensitive (up to PB)**  **cloud-based services for**  **GC-wide SaaS Solutions** |  Cloud-based services hosting sensitive (up to Protected B)  information for GC-wide enterprise applications (SaaS)   No direct system to system network interconnections required with GC data centers | SaaS |
| 5. | **GC to GC only (Hybrid IT -**  **Extension of GC Data**  **Centers)** |  Hybrid IT environment with an extension of GC network to  cloud-based virtual private cloud (up to Protected B)  information   GC cloud-based systems required to interact with systems in  GC data centers   Restricted environment for GC users only   No external user connections to/from GC cloud-based virtual private cloud and no publicly accessible services | IaaS, PaaS |
| 6. | **Cloud-based services with**  **External user access and interconnection to GC data centers** |  Cloud-based services hosting sensitive (up to Protected B)  information   GC cloud-based systems required to interact with systems in  GC data centers   Environment accessible for both GC users and External users and services   Solution implemented, managed and operated by a GC  department/agency | IaaS, PaaS |

**3.2 Guardrails Mapping to Cloud Usage Profiles**

The following table describes the applicability of the initial 30 days guardrails to be applied to each of the cloud usage profiles. Within each departmental cloud tenant, there will be various information

systems being provided. Each cloud sub-account or resource group should be tagged with the relevant cloud usage profile to ensure that appropriate policies and validation is performed.

**Table 3-2 Cloud Usage Profiles**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Cloud Guardrails** | **Applicable Service Model** | **Profile 1 – Experimentation/ Sandbox** | **Profile 2 – Non-sensitive cloud-based services** | **Profile 3 – Sensitive (up to PB) cloud- based services** | **Profile 4 – Sensitive (up to PB) cloud- based services for GC-wide SaaS Solutions** | **Profile 5 – GC to GC only (Hybrid IT - Extension of GC Data Centers)** | **Profile 6 –**  **Cloud-based Service Accessible to External users (Connections to GC Data Centers Required)** |
| 1. | **Protect Root /**  **Global Admins**  **Account** | IaaS, PaaS,  SaaS | Required | Required | Required | Required | Required | Required |
| 2. | **Management of**  **Administrative**  **Privileges** | IaaS, PaaS,  SaaS | Required | Required | Required | Required | Required | Required |
| 3. | **Cloud Console**  **Access** | IaaS, PaaS,  SaaS | Recommended | Required | Required | Required | Required | Required |
| 4. | **Enterprise**  **Monitoring**  **Accounts** | IaaS, PaaS,  SaaS | Required  *(for billing)* | Required | Required | Required | Required | Required |
| 5. | **Data location** | IaaS, PaaS,  SaaS | Recommended | Recommended | Required  *(in Canada for GC storage of PB and above)* | Required  *(in Canada for GC storage of PB and above)* | Required  *(in Canada for GC storage of PB and above)* | Required  *(in Canada for GC storage of PB and above)* |
| 6. | **Protection of data-**  **at-rest** | IaaS, PaaS,  SaaS | Not required | Recommended | Required | Required | Required | Required |
| 7. | **Protection of data-**  **in-transit** | IaaS, PaaS,  SaaS | Recommended | Required | Required | Required | Required | Required |
| 8. | **Segment and**  **separate** | IaaS, PaaS | Required  *(network filtering at a minimum)* | Required | Required | Required | Required | Required |
| 9. | **Network security services** | IaaS, PaaS, SaaS | Recommended | Required | Required | Required *(Restrict to GC only)* | Required *(Deny External Access policy –*  *GC only)* | Required |
| 10. | **Cyber defense services** | IaaS, PaaS, SaaS | Not required | Required | Required | Required | Required | Required |
| 11. | **Logging and monitoring** | IaaS, PaaS, SaaS | Recommended | Required | Required | Required | Required | Required |
| 12. | **Configuration of**  **Cloud**  **Marketplaces** | IaaS, PaaS,  SaaS | Required | Required | Required | Required | Required | Required |

**4. References**

**4.1 Related policy instruments**

 [*Directive on Security Management*](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611)

 [Direction on the Secure Use of Commercial Cloud Services: Security Implementation Notice](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-secure-use-commercial-cloud-services-spin.html)

[(SPIN)](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-secure-use-commercial-cloud-services-spin.html) 2017-01

**4.2 Additional references**

 [*Government of Canada Security Control Profile for Cloud-based GC Services*](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/government-canada-security-control-profile-cloud-based-it-services.html)

 [*Government of Canada Cloud Security Risk Management Approach and Procedures*](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/cloud-security-risk-management-approach-procedures.html)

 [Security categorization guide and tool](http://www.gcpedia.gc.ca/gcwiki/images/6/66/Tool-Security_Categorization.zip) (accessible only on the Government of Canada network)

 [*Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2018*](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html)

 [Concept case for digital projects](https://www.tbs-sct.gc.ca/pol-cont/doc/32593-eng.docx)

 [Enterprise security architecture (ESA) template guides](http://www.gcpedia.gc.ca/wiki/ESA_Template_Guides) (accessible only on the Government of

Canada network)

 [*Guideline on Defining Authentication Requirements*](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262)

 [*Guideline on Identity Assurance*](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678)

 [*Considerations for Cryptography in Commercial Cloud Services*](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/government-canada-consideration-use-cryptography-in-cloud.html)

 [*IT Security Risk Management: A Lifecycle Approach (ITSG-33)*](https://cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33)

 [*Guidance on Securely Configuring Network Protocols (ITSP.40.062)*](https://cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062)

 [*Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-*](https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22)

[*22)*](https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22)

 [*Network Security Zoning: Design Considerations for Placement of Services within Zones (ITSG-38)*](https://cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38)