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

Canada

# Government of Canada
# Enterprise Architecture Review Board (GC EARB)

## Treasury Board of Canada Secretariat

## GC Cloud Enablement: Cloud Connection Patterns

## (December 19, 2019)

| Presentation for: | EARB Appearance: | Contact Information: |
|---|---|---|
| X Endorsement<br>☐ Information<br>☐ Exemption | X Initial<br>☐ Follow-up<br>☐ Final Architecture | **Presenter(s):**<br>• Po Tea-Duncan (TBS) / po.tea-duncan@tbs-sct.gc.ca / 613-404-2924 |

GC Docs #31758070

Last Updated June 7, 2019

# Purpose of GC EARB Session

- The purpose of this presentation is to seek GC EARB **endorsement** on the cloud connection patterns and prioritization of departments seeking services from the Secure Cloud Enablement and Defence (SCED) initiative.

  The presentation will focus on:

  - Cloud connection patterns
  - Cloud guardrails and usage profiles

# Request – Background

- As workloads are migrated to the cloud, and the GC perimeter shifts outside of the on-premise environment, the GC must rethink how it monitors and protects these cloud-based environments.
- Establishing a risk-based adaptive service will help the government protect its cloud-based information systems and maintain continuous awareness of the cyber threat landscape.
- Further, the establishment of dedicated, private connections to Cloud Service Providers (CSP) will enable a hybrid IT environment with the extension of the GC network and data centers to GC-approved CSPs, and ensure that the GC can continue to have access to GC information systems and solutions hosted in the cloud.

# What is SCED?

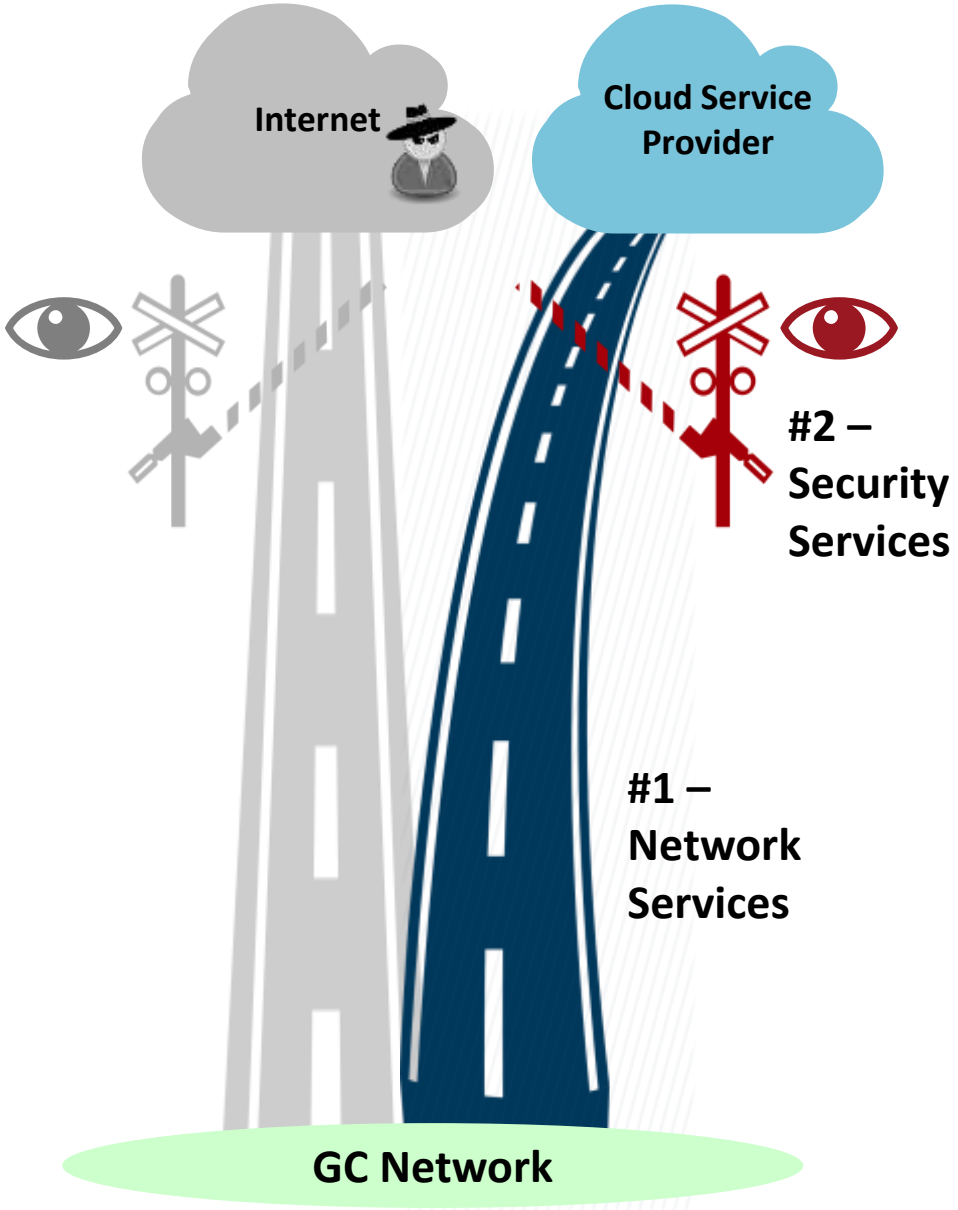
## Background

Secure Cloud Enablement and Defence (SCED) is an **initiative** funded as part of Budget 2018.

## Objectives

#1 Establish new **private, dedicated connections** to public cloud environments to minimize the proliferation of non-enterprise, ad-hoc links.

#2 Enable **full visibility and monitoring** of GC cloud environments to respond to **cyber threats.**



# Network Connection Types

| Ref. | Type | Description |
|---|---|---|
| 1 | **Enterprise Internet Service / Internet Information Services (EIS/IIS)** | • Connection provided to Public Internet.<br>• Standard user Internet surfing via EIS.<br>• Uses existing security stack (e.g. SSC managed gateways).<br>• Can be used as failover/backup connection where applicable |
| 2 | **Internet Exchange Provider (IXP)** | • Public peering at the Internet layer<br>• Available for GC approved enterprise-wide SaaS offerings<br>• Social media redirected to IXP connection |
| 3 | **Cloud Exchange Provider (CXP)** | • Provides Direct Peering with CSP<br>• Segregation of cloud connections from GC corporate internet connections |
| 4 | **External Cloud Service Provider Connection** | • Cloud-native network and security services provided by CSP |

**SCED Objective #1**

Establish new private, dedicated connections to public cloud environments

# Network Security Services & Cyber Defense

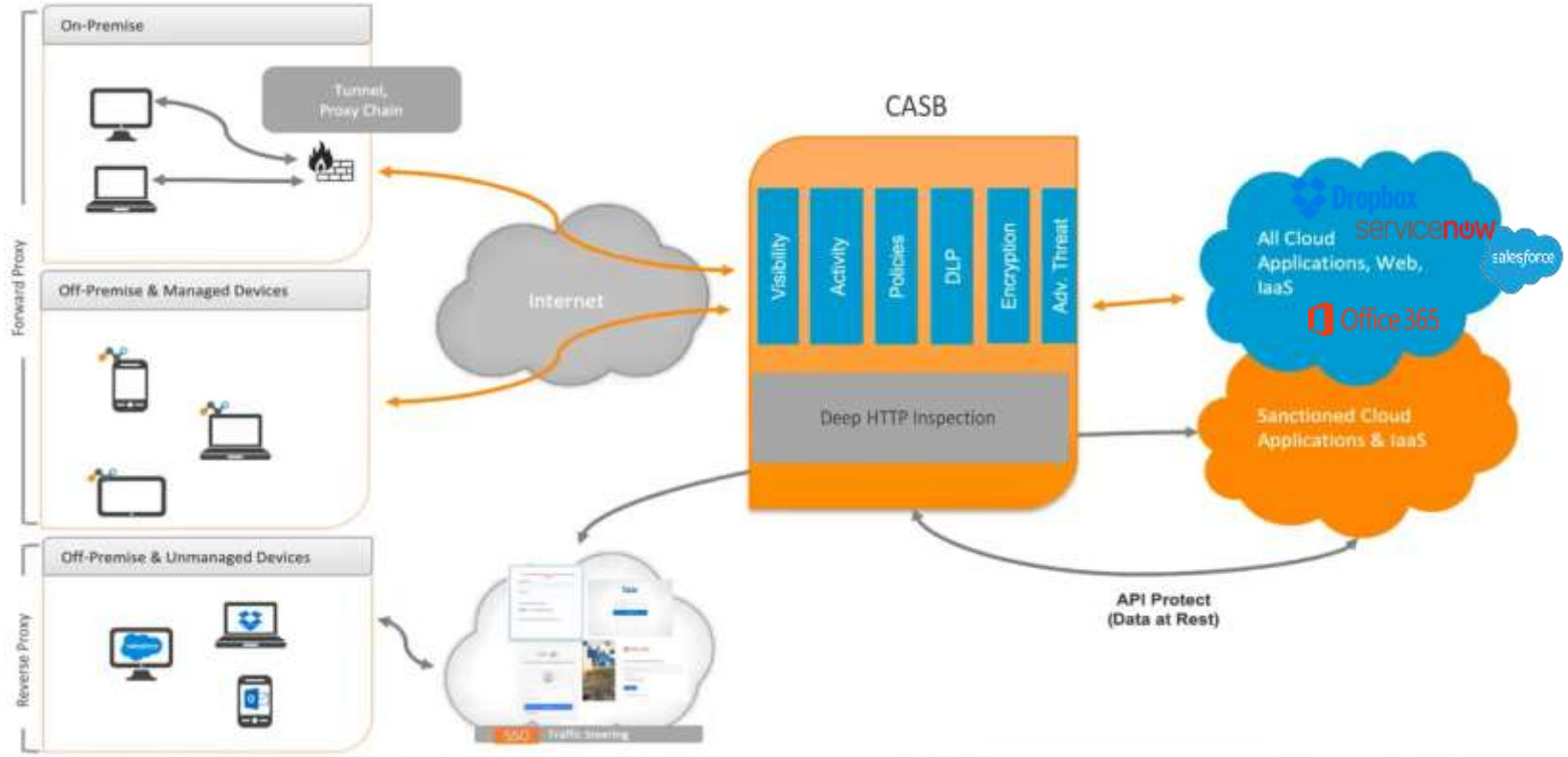
| Network Security Services |
|---|
| Routing |
| Boundary protection |
| Logging and auditing |
| Intrusion detection and prevention |
| Denial of service protection |
| Malware protection |
| Access Control |
| Proxy Service |
| Secure VPN Service |
| TLS traffic inspection (based on risk profile) |
| Threat monitoring |

- As per the SPIN 2017-01, Departments are expected to ensure that the cloud tenant environments are configured with appropriate network security services.
- Where available, centralized services should be utilized, to support a standardized, cost-effective, enterprise approach.
- For IaaS/PaaS, SCED is **PILOTING** centralized services to be delivered by SSC:
  - **GC Trusted Interconnection Points (GC-TIP)** – physical hardware stack in CXP environment
  - **GC Cloud Access Points (GC-CAP)** – virtual stack in GC-approved CSP environments
- This is supplemented by threat monitoring performed via the Canadian Centre for Cyber Security (CCCS) Cyber Defense Services:
  - **Cloud-based Sensor (CBS)**
  - **Host-based Sensor (HBS)**
  - **(Virtual) Network-based Sensor (NBS)**
- These services help to address GC Cloud Guardrails #9 for Network Security Services and #10 Cyber Defense Services.

**SCED Objective #2 -** Enable full visibility and monitoring of GC cloud environments to respond to cyber threats

**As outlined in the GC TIP Concept Paper*

# SCED Initiative - Cloud Access Security Broker




## CASB Functions

- ❑ Visibility
- ❑ Data Security
- ❑ Threat Protection/Ransomware
- ❑ Compliance
- ❑ Auditing
- ❑ Enforcement
- ❑ Coach Users
- ❑ Enterprise Integration
- ❑ Central management console

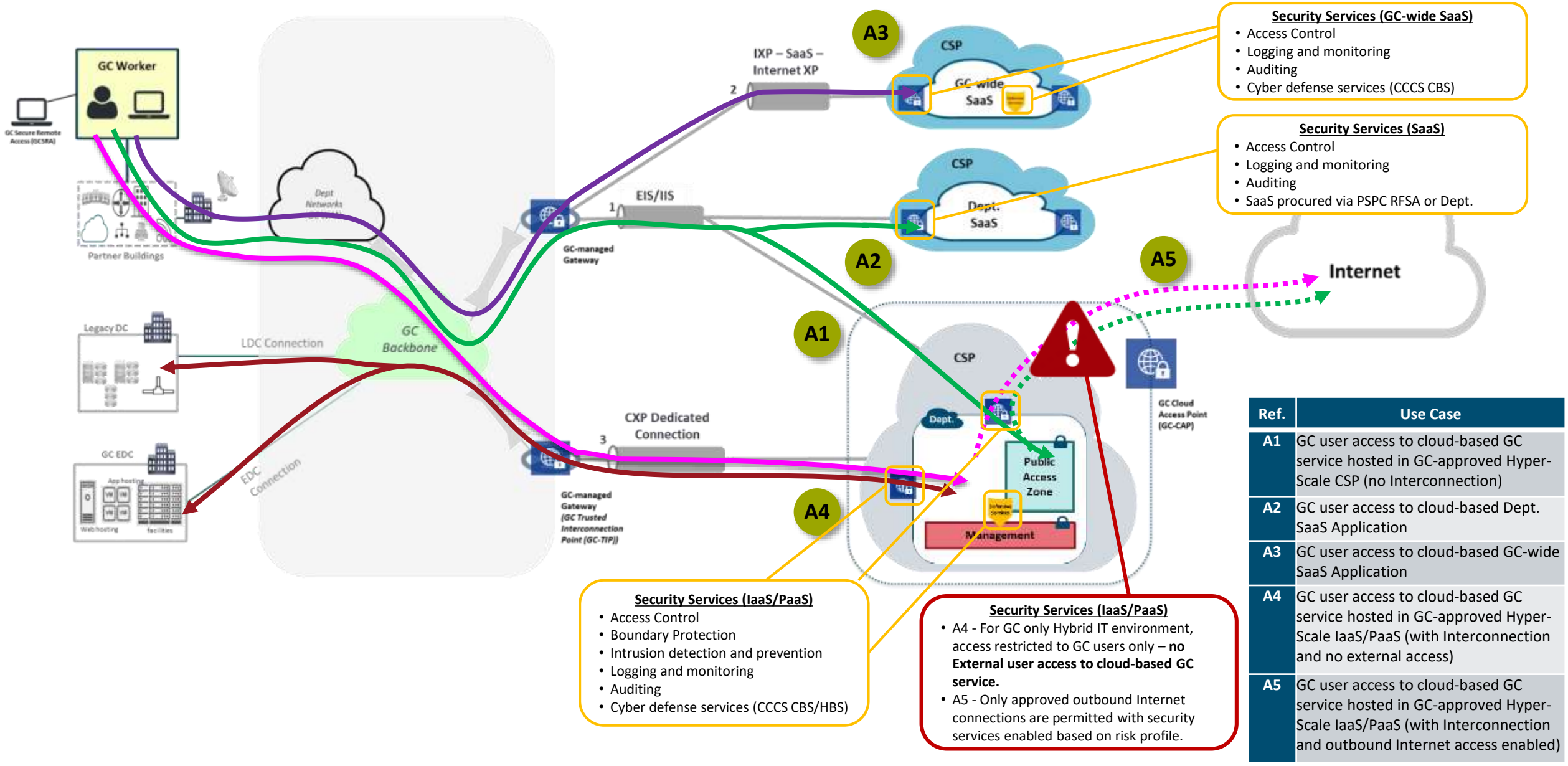
**SCED will deliver a common approach for Cloud Access Security Broker (CASB) capabilities for SaaS**

*Excerpt from SSC SCED Executive CASB Overview (CASB) – Sept 2019 Presentation*

# Cloud Access Scenarios

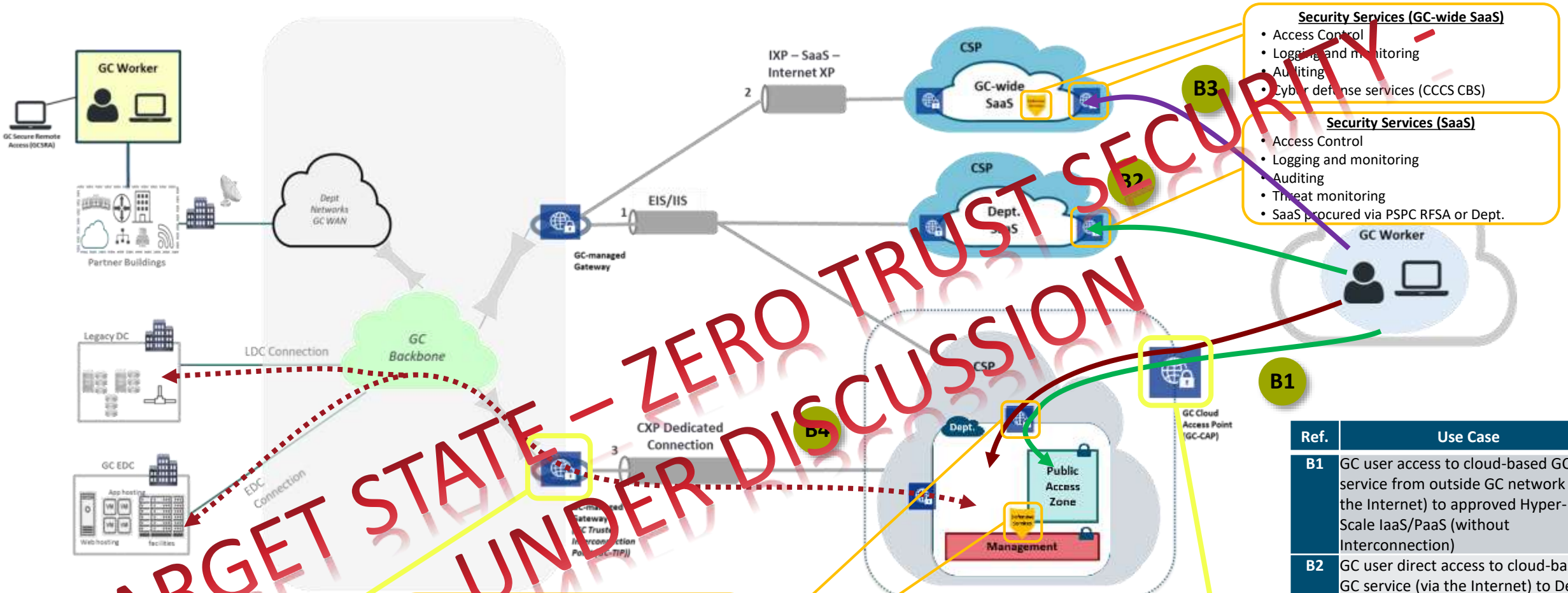
| Ref | Scenario | Description |
|---|---|---|
| A | **GC user access to cloud-based service from GC network** | A GC worker accessing a cloud-based GC service on the GC network. |
| B | **GC user access to cloud-based service from Internet** | A GC worker accessing a cloud-based GC service from outside the GC network over the public Internet. |
| C | **External user access to cloud-based service** | A non-GC external user accessing a cloud-based GC service from outside the GC network. |
| D | **Service/Application Interoperability** | Service and application communications with cloud-based GC services. |
| E | **Cloud Administration and Management Traffic** | Management of cloud-based components and support for Network Operations Center (NOC) and Security Operations Center (SOC) activities. |

# Scenario A – GC user access to cloud-based service from GC Network




| Ref. | Use Case |
|---|---|
| A1 | GC user access to cloud-based GC service hosted in GC-approved Hyper-Scale CSP (no Interconnection) |
| A2 | GC user access to cloud-based Dept. SaaS Application |
| A3 | GC user access to cloud-based GC-wide SaaS Application |
| A4 | GC user access to cloud-based GC service hosted in GC-approved Hyper-Scale IaaS/PaaS (with Interconnection and no external access) |
| A5 | GC user access to cloud-based GC service hosted in GC-approved Hyper-Scale IaaS/PaaS (with Interconnection and outbound Internet access enabled) |

# Scenario B – GC user access to cloud-based service from Internet




**Security Services (GC-wide SaaS)**
- Access Control
- Logging and monitoring
- Auditing
- Cyber defense services (CCCS CBS)

**Security Services (SaaS)**
- Access Control
- Logging and monitoring
- Auditing
- Threat monitoring
- SaaS procured via PSPC RFSA or Dept.

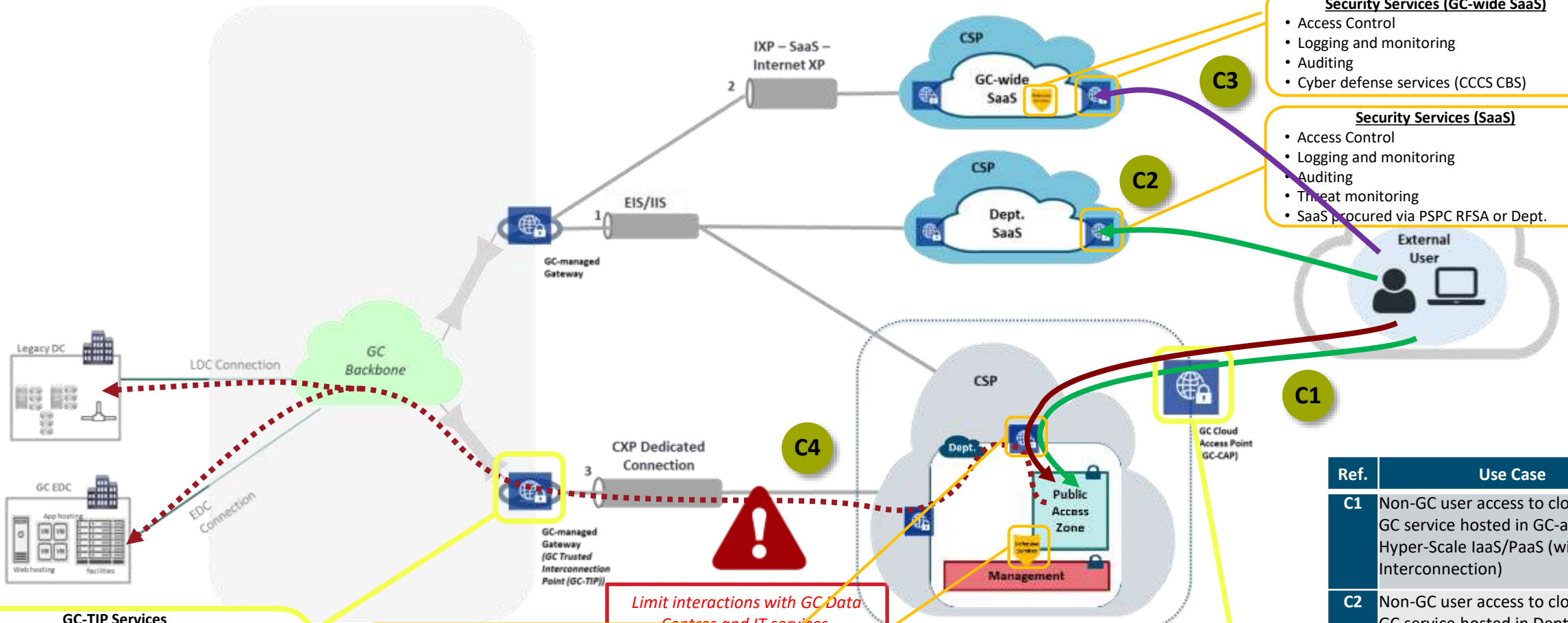
**GC-TIP Services**
- Access control
- Boundary Protection
- Intrusion detection and prevention
- Logging and monitoring
- Auditing
- Cyber defense services (NBS)

**Security Services (IaaS/PaaS)**
- Access control
- Boundary Protection
- Intrusion detection and prevention
- Logging and monitoring
- Auditing
- Denial of service protection
- Malware protection
- TLS Inspection – Ingress (depending on risk profile)
- **Cyber defense services (CCCS CBS/HBS)**

**GC-CAP Security Services**
- Access control
- Boundary Protection
- Intrusion detection and prevention
- Logging and monitoring
- Auditing
- Denial of service protection
- Malware protection
- TLS Inspection – Ingress (depending on risk profile)
- **Cyber defense services (CCCS Virtual NBS)**

| Ref. | Use Case |
|---|---|
| B1 | GC user access to cloud-based GC service from outside GC network (via the Internet) to approved Hyper-Scale IaaS/PaaS (without Interconnection) |
| B2 | GC user direct access to cloud-based GC service (via the Internet) to Dept. SaaS Application |
| B3 | GC user direct access to cloud-based GC service (via the Internet) to GC-wide SaaS Application |
| B4 | GC user access to cloud-based GC service from outside GC network (via the Internet) to approved Hyper-Scale IaaS/PaaS (with Interconnection) |

# Scenario C – External user access to cloud-based GC service




**GC-TIP Services**
- Access control
- Boundary Protection
- Intrusion detection and prevention
- Logging and monitoring
- Auditing
- Cyber defense services (NBS)

*Additional features enabled based on risk profile:*
- *Malware protection*
- *TLS Inspection – Ingress*

**Security Services (IaaS/PaaS)**
- Access control
- Boundary Protection
- Intrusion detection and prevention
- Logging and monitoring
- Auditing
- Denial of service protection
- Malware protection
- TLS Inspection – Ingress (depending on risk profile)
- **Cyber defense services (CCCS CBS/HBS)**

**GC-CAP Security Services**
- Access control
- Boundary Protection
- Intrusion detection and prevention
- Logging and monitoring
- Auditing
- Denial of service protection
- Malware protection
- TLS Inspection – Ingress (depending on risk profile)
- **Cyber defense services (CCCS Virtual NBS)**

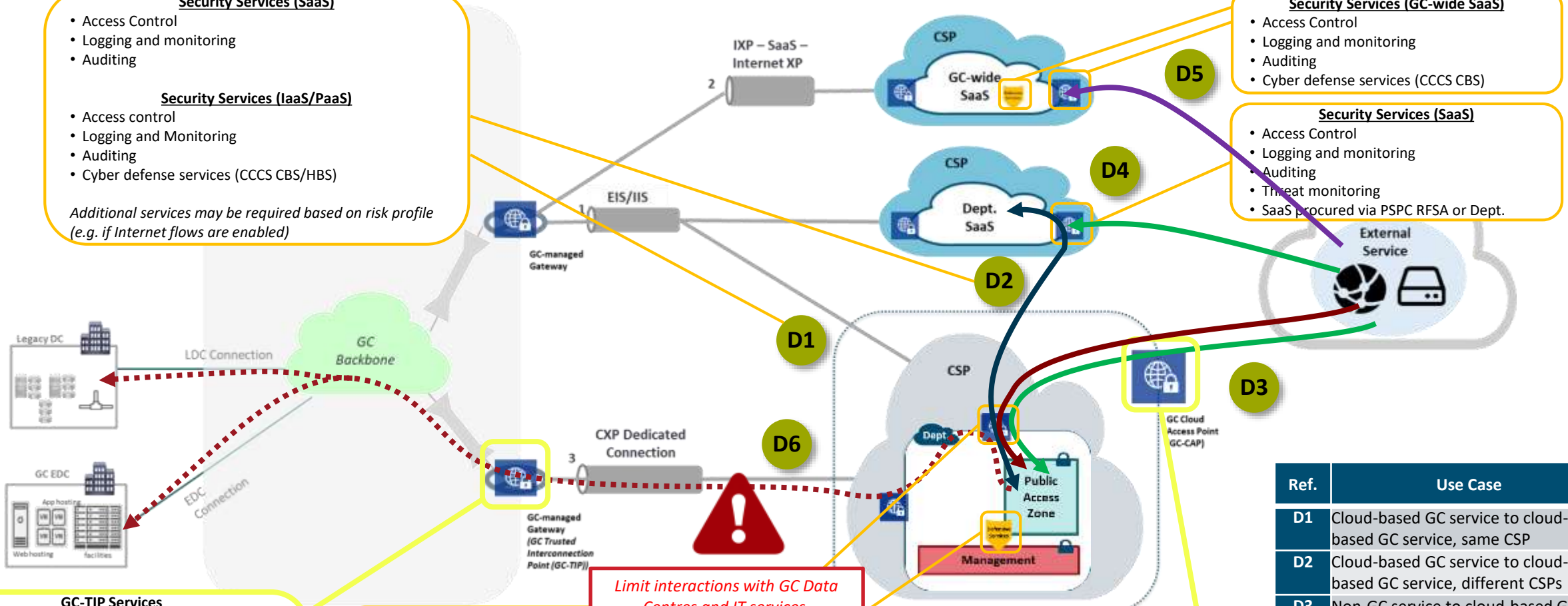
| Ref. | Use Case |
|---|---|
| C1 | Non-GC user access to cloud-based GC service hosted in GC-approved Hyper-Scale IaaS/PaaS (without Interconnection) |
| C2 | Non-GC user access to cloud-based GC service hosted in Dept. SaaS Application |
| C3 | Non-GC user access to cloud-based GC service hosted in GC-wide SaaS Application |
| C4 | Non-GC user access to cloud-based GC service hosted in GC-approved Hyper-Scale IaaS/PaaS (with Interconnection) Application |

# Scenario D – Service/Application Interoperability

**Security Services (SaaS)**
- Access Control
- Logging and monitoring
- Auditing

**Security Services (IaaS/PaaS)**
- Access control
- Logging and Monitoring
- Auditing
- Cyber defense services (CCCS CBS/HBS)

*Additional services may be required based on risk profile (e.g. if Internet flows are enabled)*




**Security Services (GC-wide SaaS)**
- Access Control
- Logging and monitoring
- Auditing
- Cyber defense services (CCCS CBS)

**Security Services (SaaS)**
- Access Control
- Logging and monitoring
- Auditing
- Threat monitoring
- SaaS procured via PSPC RFSA or Dept.

**GC-TIP Services**
- Access control
- Boundary Protection
- Intrusion detection and prevention
- Logging and monitoring
- Auditing
- Cyber defense services (NBS)

*Additional features enabled based on risk profile:*
- *Malware protection*
- *TLS Inspection – Ingress*

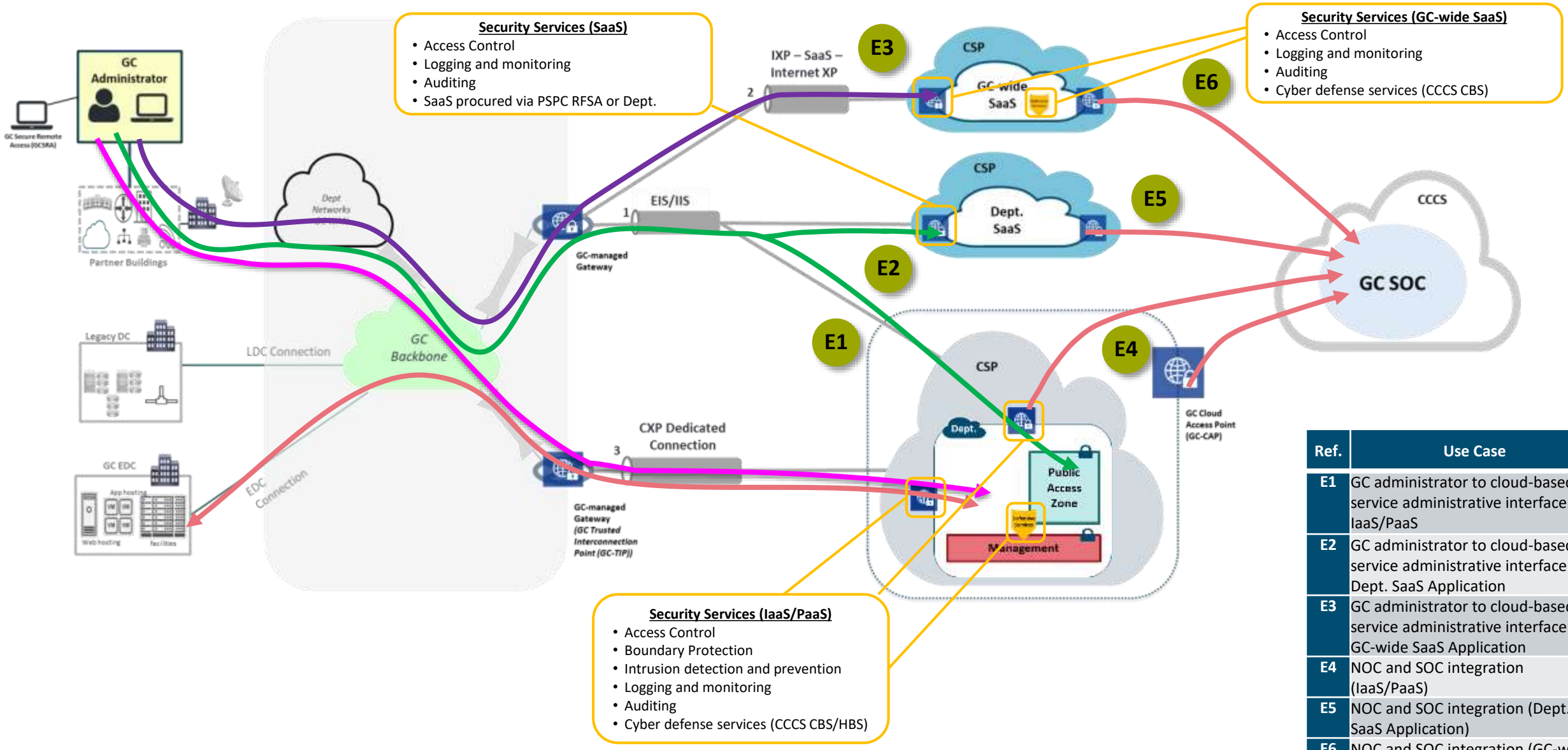
**Security Services (IaaS/**
- Access control
- Boundary Protection
- Intrusion detection and preventio
- Logging and monitoring
- Auditing
- Denial of service protection
- Malware protection
- TLS Inspection – Ingress (depending on risk profile)
- **Cyber defense services (CCCS CBS/HBS)**

*Limit interactions with GC Data Centres and IT services. Use secure **Application Programming Interfaces (API)** to expose GC data and services.*

**GC-CAP Security Services**
- Access control
- Boundary Protection
- Intrusion detection and prevention
- Logging and monitoring
- Auditing
- Denial of service protection
- Malware protection
- TLS Inspection – Ingress (depending on risk profile)
- **Cyber defense services (CCCS Virtual NBS)**

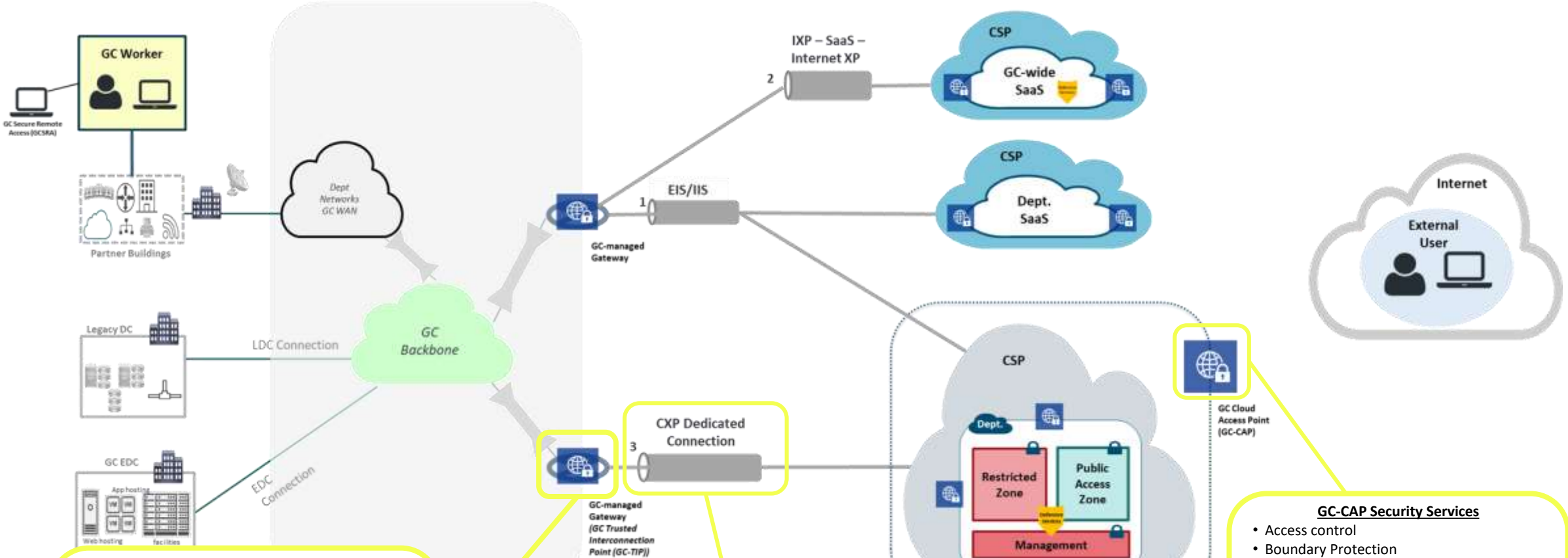
| Ref. | Use Case |
|---|---|
| D1 | Cloud-based GC service to cloud-based GC service, same CSP |
| D2 | Cloud-based GC service to cloud-based GC service, different CSPs |
| D3 | Non-GC service to cloud-based GC service for IaaS/PaaS (no interconnections) |
| D4 | Non-GC service to cloud-based GC service for Dept. SaaS Application |
| D5 | Non-GC service to cloud-based GC service for GC-wide SaaS Application |
| D6 | Non-GC service to cloud-based GC service (with interconnection) |

# Scenario E – Cloud Administration and Management Traffic




| Ref. | Use Case |
|---|---|
| E1 | GC administrator to cloud-based GC service administrative interface for IaaS/PaaS |
| E2 | GC administrator to cloud-based GC service administrative interface for Dept. SaaS Application |
| E3 | GC administrator to cloud-based GC service administrative interface for GC-wide SaaS Application |
| E4 | NOC and SOC integration (IaaS/PaaS) |
| E5 | NOC and SOC integration (Dept. SaaS Application) |
| E6 | NOC and SOC integration (GC-wide SaaS Application) |

# Where does SCED fit in?




**GC-TIP Services**

- Access control
- Boundary Protection
- Intrusion detection and prevention
- Logging and monitoring
- Auditing
- Cyber defense services (NBS)

*Additional features enabled based on risk profile:*

- *Malware protection*
- *TLS Inspection – Ingress*

**Network Services**

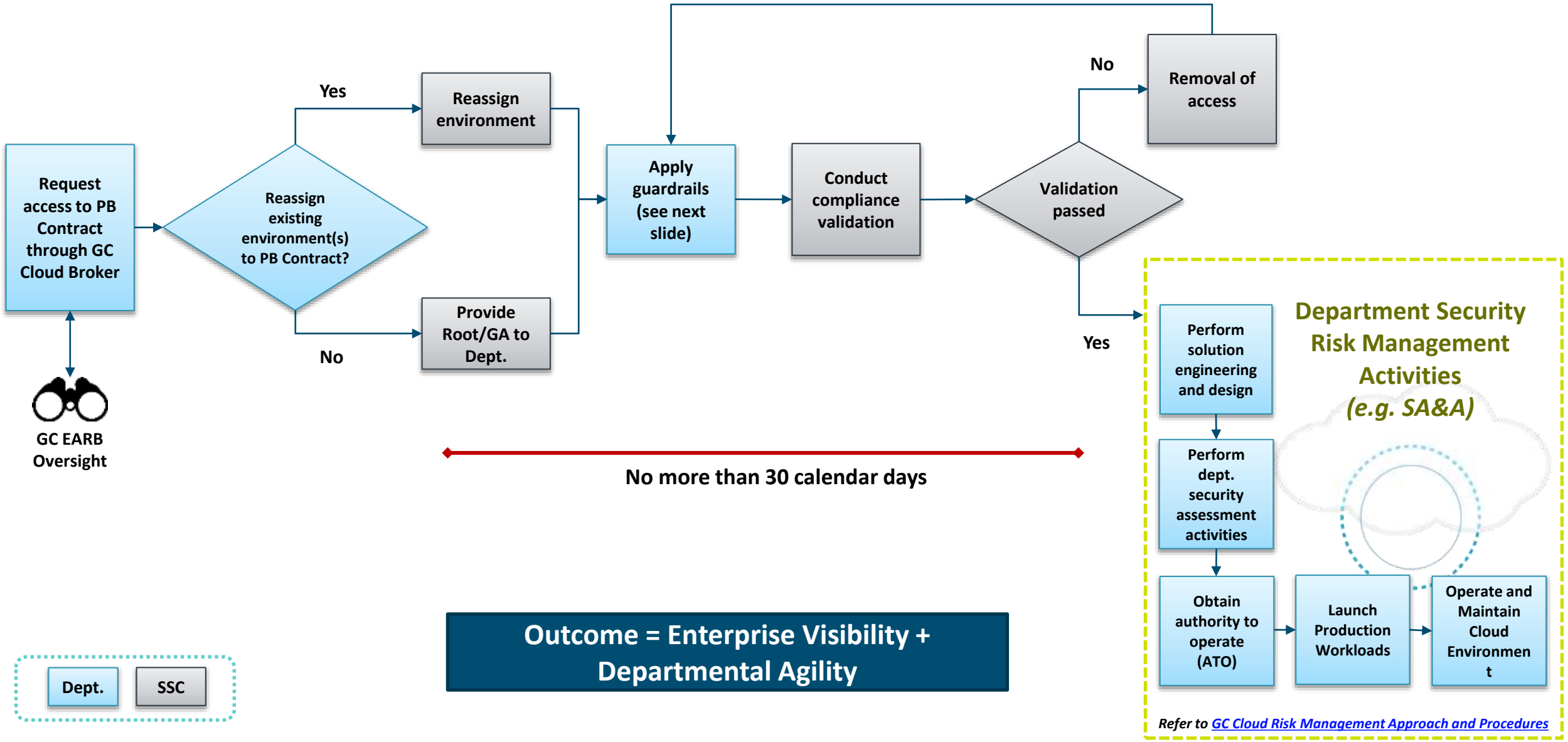
- Type 3 – Cloud Exchange Provider

**GC-CAP Security Services**

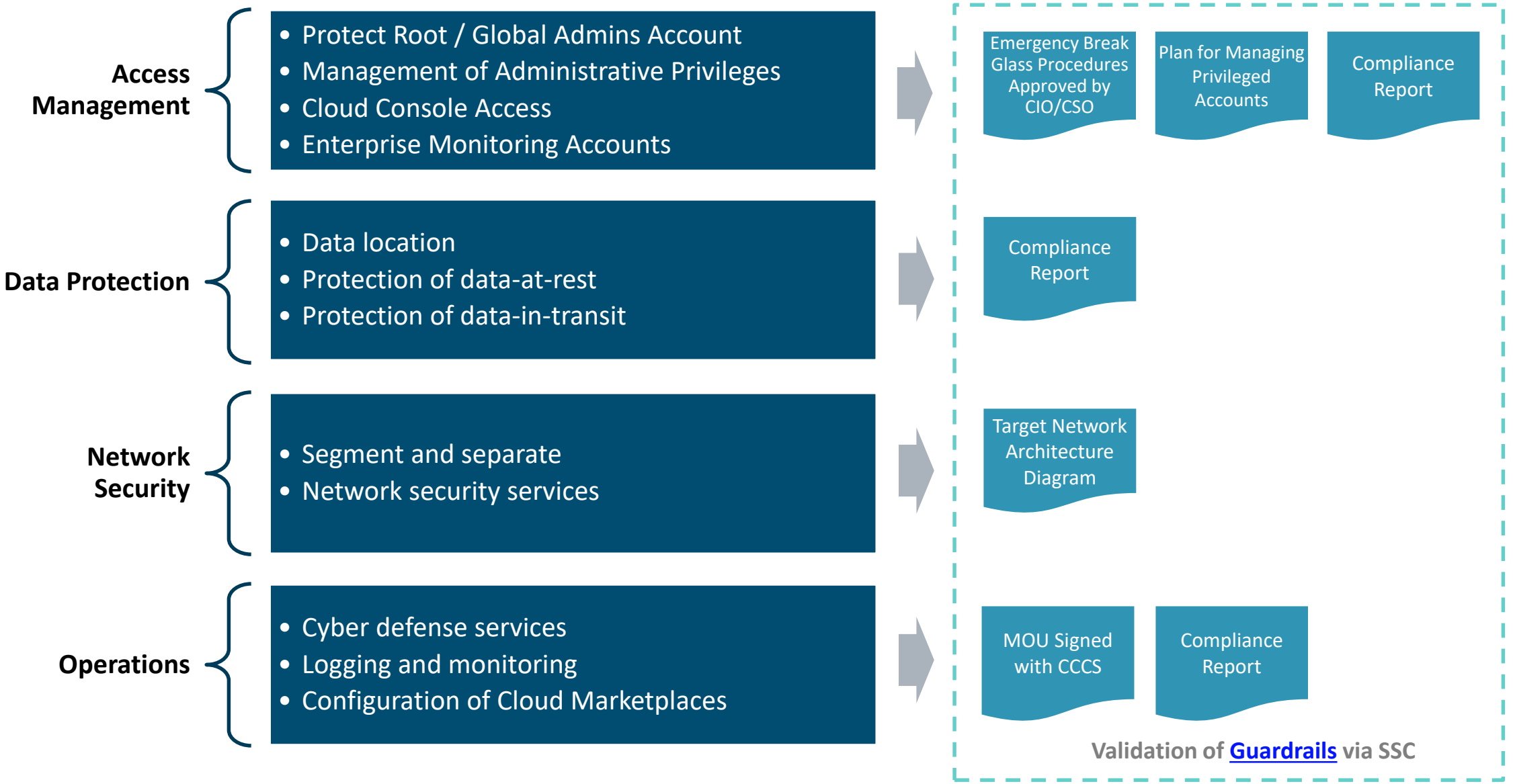
- Access control
- Boundary Protection
- Intrusion detection and prevention
- Logging and monitoring
- Auditing
- Denial of service protection
- Malware protection
- TLS Inspection – Ingress (depending on risk profile)
- **Cyber defense services (CCCS Virtual NBS)**

# Guardrails

# RECAP: Operationalization Framework



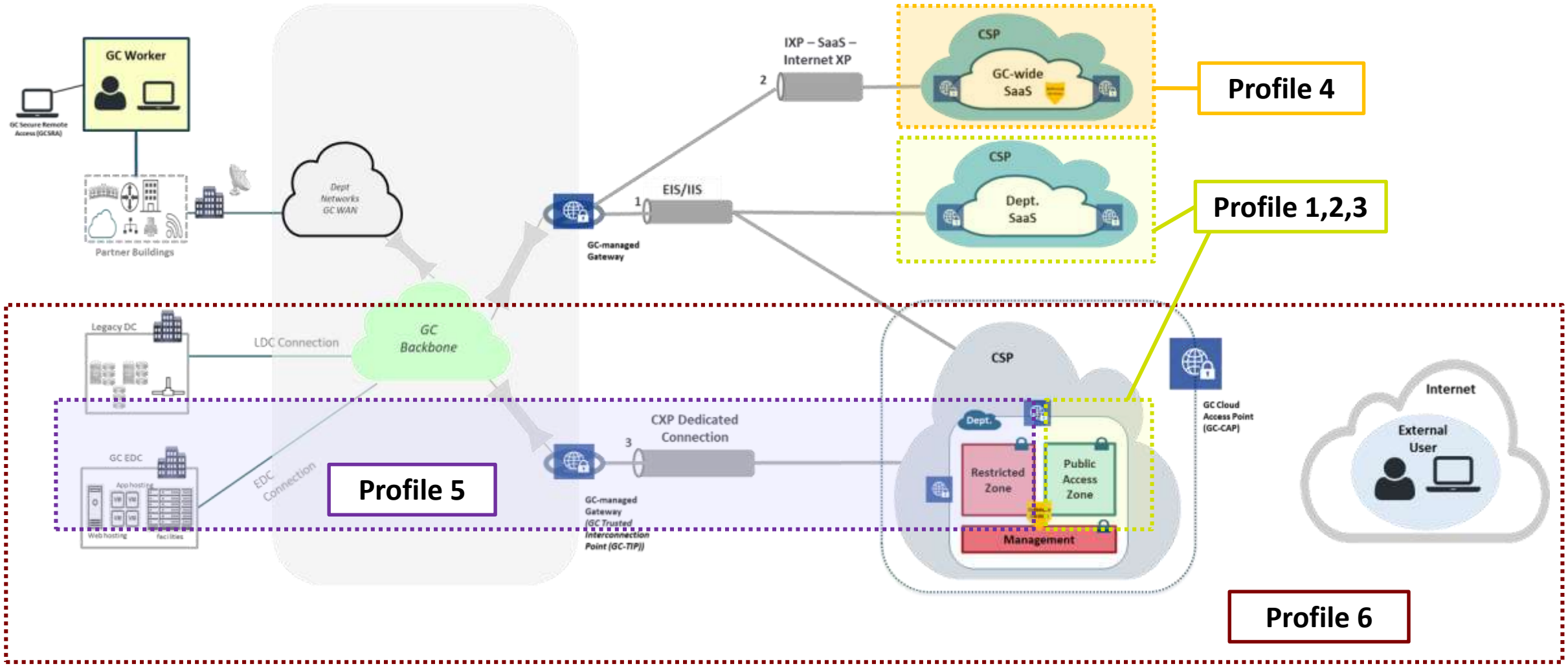
# Cloud Guardrails – First 30 Days



# Cloud Usage Profiles

| Ref. | Profile | Characteristics | Applicable Service Model | Connection Type | In scope for SCED? |
|---|---|---|---|---|---|
| 1 | **Experimentation/Sandbox** | • Cloud-based services used for experimentation/sandbox<br>• No direct system to system network interconnections required with GC data centers | IaaS, PaaS, SaaS | Type 1 – EIS/IIS | No |
| 2 | **Non-sensitive cloud-based services** | • Cloud-based services hosting non-sensitive GC content<br>• No direct system to system network interconnections required with GC data centers | IaaS, PaaS, SaaS | Type 1 – EIS/IIS | Interim – No<br><br>Future – For IaaS/PaaS, use GC-CAP with CCCS virtual NBS when available, based on risk profile. |
| 3 | **Sensitive (up to PB) cloud-based services** | • Cloud-based services hosting sensitive (up to Protected B) information<br>• No direct system to system network interconnections required with GC data centers | IaaS, PaaS, SaaS | Type 1 – EIS/IIS | Interim – No<br><br>Future – For IaaS/PaaS, use GC-CAP with CCCS virtual NBS when available, based on risk profile.<br><br>Future - For SaaS, use CASB solution, if available, based on risk profile |
| 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)<br>• No direct system to system network interconnections required with GC data centers | SaaS | Type 2 – IXP | No – protection via CCCS Cyber Defense services |
| 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<br>• GC cloud-based systems required to interact with systems in GC data centers<br>• Restricted environment for GC users only<br>• No external user connections to/from GC cloud-based virtual private cloud and no publicly accessible services | IaaS, PaaS | Type 3 - CXP | SCED Objective #1 (Network) |
| 6 | **Cloud-based services with External user access and interconnection to GC data centers** | • Cloud-based services hosting sensitive (up to Protected B) information<br>• GC cloud-based systems required to interact with systems in GC data centers<br>• Environment accessible for both GC users and External users and services<br>• Solution implemented, managed and operated by a GC department/agency | IaaS, PaaS | Type 3 - CXP | SCED Objective #1 (Network) and #2 (Security via GC-CAP) |

# Cloud Usage Profiles

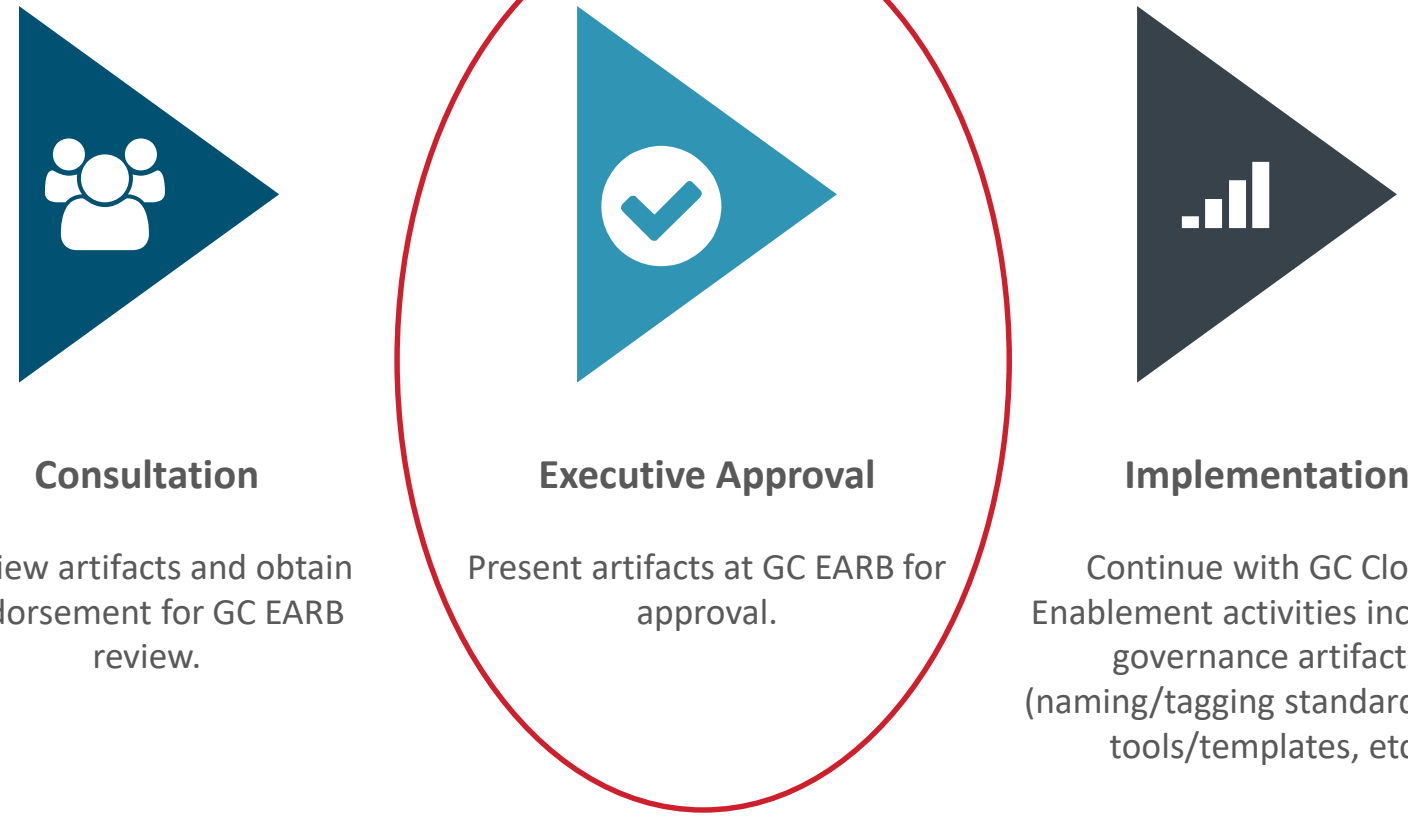


# Mandatory Guardrails – Compliance Monitoring

Minimum, mandatory, guardrails a department must implement within 30 days of gaining access to their account(s). **Non-adherence is violation of terms of use.**

| 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) |
|---|---|---|---|---|---|---|---|---|
| 01 | Protect root / global admins account | IaaS, PaaS, SaaS | Required | Required | Required | Required | Required | Required |
| 02 | Management of administrative privileges | IaaS, PaaS, SaaS | Required | Required | Required | Required | Required | Required |
| 03 | Cloud console access | IaaS, PaaS, SaaS | Recommended | Required | Required | Required | Required | Required |
| 04 | Enterprise monitoring accounts | IaaS, PaaS, SaaS | Required *(for billing)* | Required | Required | Required | Required | Required |
| 05 | 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)* |
| 06 | Protection of data-at-rest | IaaS, PaaS, SaaS | Not required | Recommended | Required | Required | Required | Required |
| 07 | Protection of data-in-transit | IaaS, PaaS, SaaS | Recommended | Required | Required | Required | Required | Required |
| 08 | Segment and separate | IaaS, PaaS | Required *(network filtering at a minimum)* | Required | Required | Required | Required | Required |
| 09 | 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 |

# Next Steps



**Consultation**

Review artifacts and obtain endorsement for GC EARB review.

**Executive Approval**

Present artifacts at GC EARB for approval.

**Implementation**

Continue with GC Cloud Enablement activities including governance artifacts (naming/tagging standards) and tools/templates, etc.

# Questions?

## Contact us:

TBS OCIO
Cyber Security
ZZTBSCYBERS@tbs-sct.gc.ca

SSC Cloud Broker
ssc.cloud-infonuagique.spc@canada.ca

# References

## TB Policies & Standards

- Policy on Management of Information Technology
- Policy on Government Security
- Direction for Electronic Data Residency, ITPIN No: 2017-02
- Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)

## Guidance

*TBS*

- Government of Canada Security Control Profile for Cloud-Based GC IT Services
- Government of Canada Cloud Security Risk Management Approach and Procedures
- Guidance on Cloud Authentication for the Government of Canada
- Recommendations for Two-Factor User Authentication Within the Government of Canada Enterprise Domain
- Considerations for the use of Cryptography in Commercial Cloud
- GC Event Logging Guidance
- Standard Operating Procedure for GC Cloud Event Management

*CCCS*

- CCCS ITSG-22 Baseline Security Requirements for Network Security Zones in the Government of Canada
- CCCS ITSG-38 Network Security Zoning - Design Considerations for Placement of Services within Zones
- CCCS ITSP.30.031 V2 User Authentication Guidance for Information Technology Systems
- CCCS ITSP.40.062 Guidance on Securely Configuring Network Protocols
- CCCS ITSM.50.100 Cloud Service Provider Information Technology Security Assessment Process

## Tools & Templates

*Guardrails*

- GC Cloud Guardrails
- https://github.com/canada-ca/cloud-guardrails
- https://github.com/canada-ca/cloud-guardrails-azure
- https://github.com/canada-ca/cloud-guardrails-aws

*Design Patterns*

- GC ESA SaaS Design Patterns

*Playbooks*

- Security Playbook for Information System Solutions

*Templates*

- https://gccode.ssc-spc.gc.ca/GCCloudEnablement
- https://github.com/canada-ca/accelerators_accelerateurs-azure
- https://github.com/canada-ca/accelerators_accelerateurs-aws