Government of Canada
Enterprise Architecture Review Board

Changes to the GC Cloud Guardrails Process
August 13, 2020

Presentation for:	EARB Appearance:	Contact Information:
X Endorsement X Information ☐ Exemption	☐ Initial X Follow-up ☐ Final Architecture	**Presenter(s):** • Scott Levac • Ari Rizvi

Purpose of GC EARB Session

- The purpose of this presentation is to seek GC EARB **endorsement** to:

  - Endorse a new escalation process for guardrail drift (item 1)
  - Including, remediation actions for accounts that have drifted outside of the guardrails

  - Endorse an update to the GC Public Cloud Roles & Responsibilities Document (item 2)

  And, provide **information** on:

  - Current status of accounts that have drifted outside of the guardrails

  - The way forward for including the Office 365 guardrails

Request Background

- In August of 2019, SSC qualified the first two cloud service providers on the GC Cloud Services Framework Agreement, the first providers to be qualified to host Protected B data

- With a higher sensitivity of information, there was a desire to ensure every department using cloud put minimum protections in place

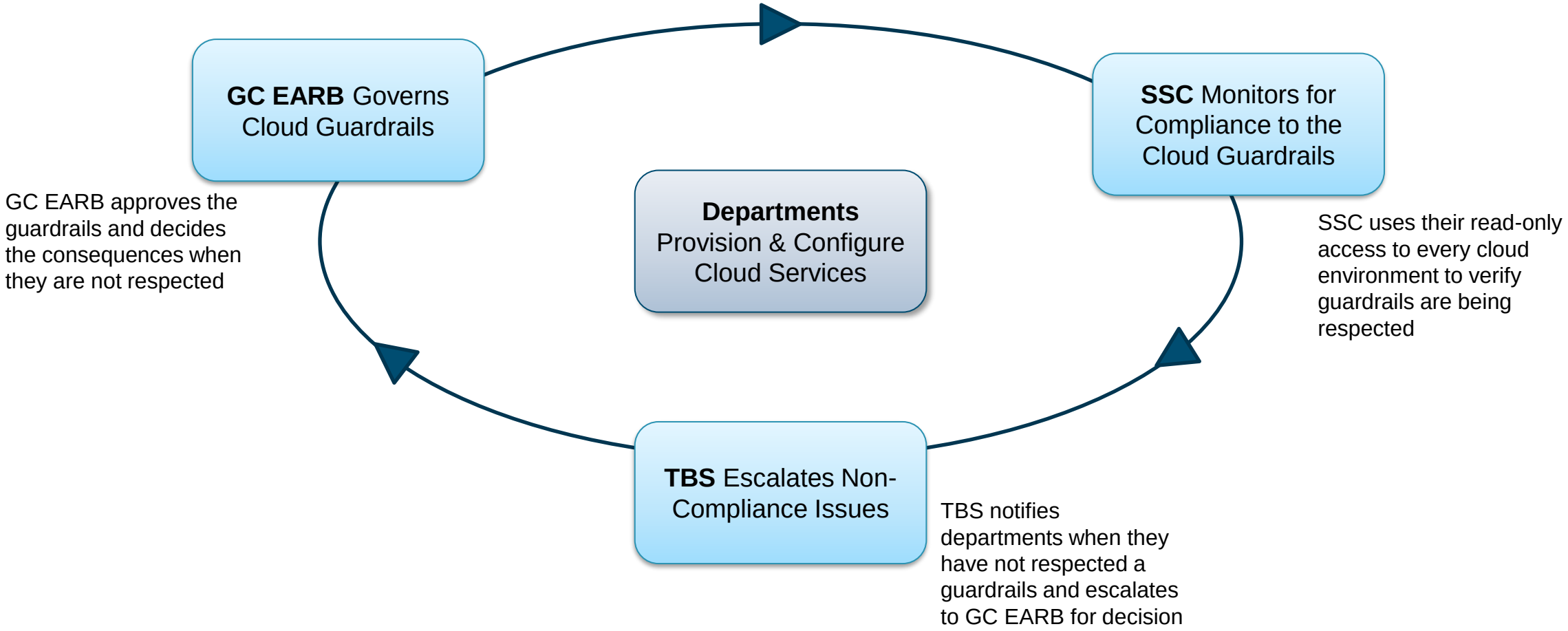
- In September 2019, the GC Enterprise Architecture Review Board (EARB) approved the Operationalization Framework; a process for monitoring compliance to guardrails for cloud accounts

- The purpose of the Operationalization Framework was to provide departments the agility to provision and configure cloud services (without gates) while providing enterprise-level visibility over departmental actions (stay within the guardrails)

From: Sept 19th, GC EARB

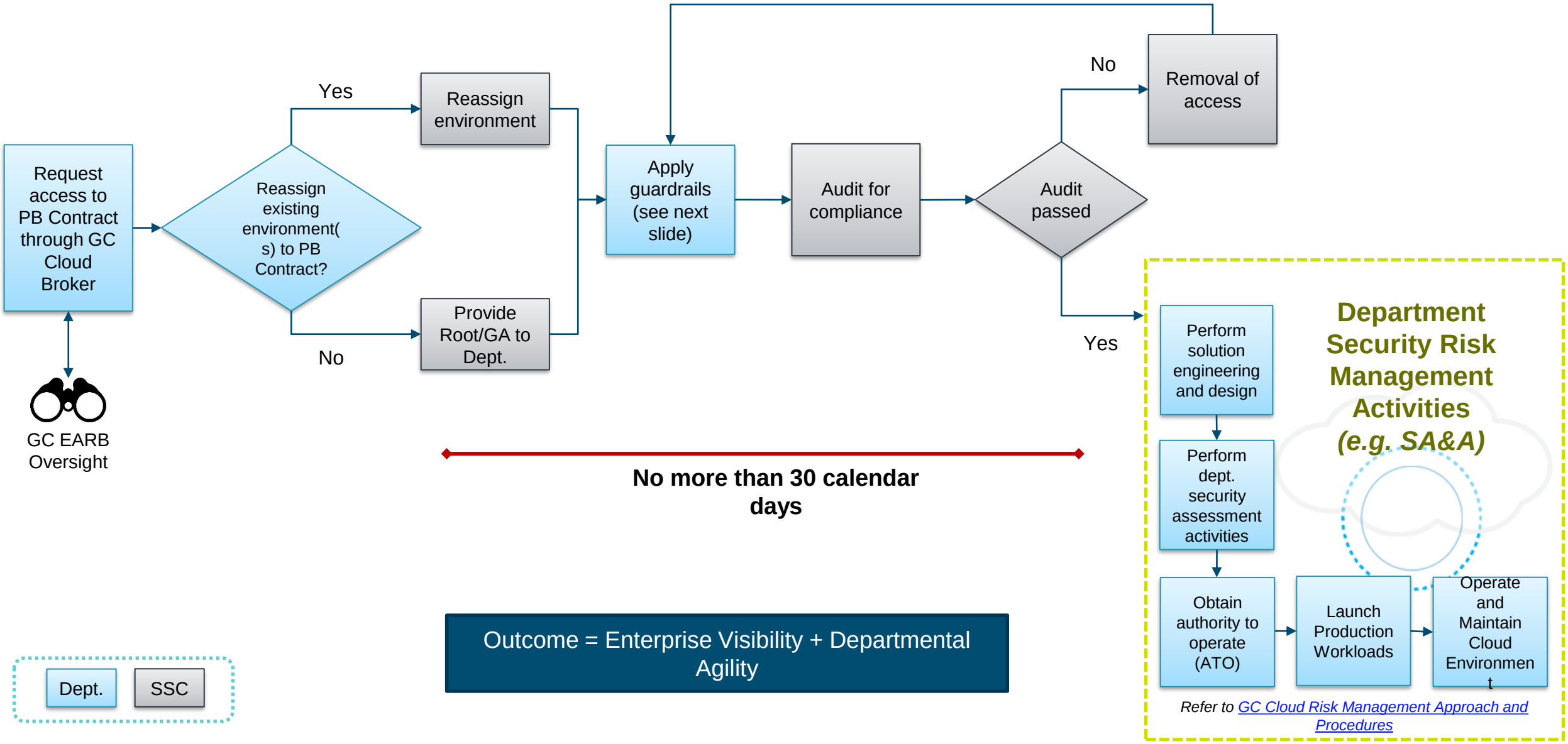
Governing by Guardrails: Enterprise Visibility, Departmental Agility

A ***trust, but verify model*** is used: departments are trusted to safely operate their cloud accounts, but the enterprise has the ability to verify their usage. Rather than a traditional gating governance, a guardrails approach to governance was implemented. As long as guardrails are respected, departments can keep using the self-service features of cloud uninterrupted.



From: Sept 19th, GC EARB

Background: Operationalization Framework



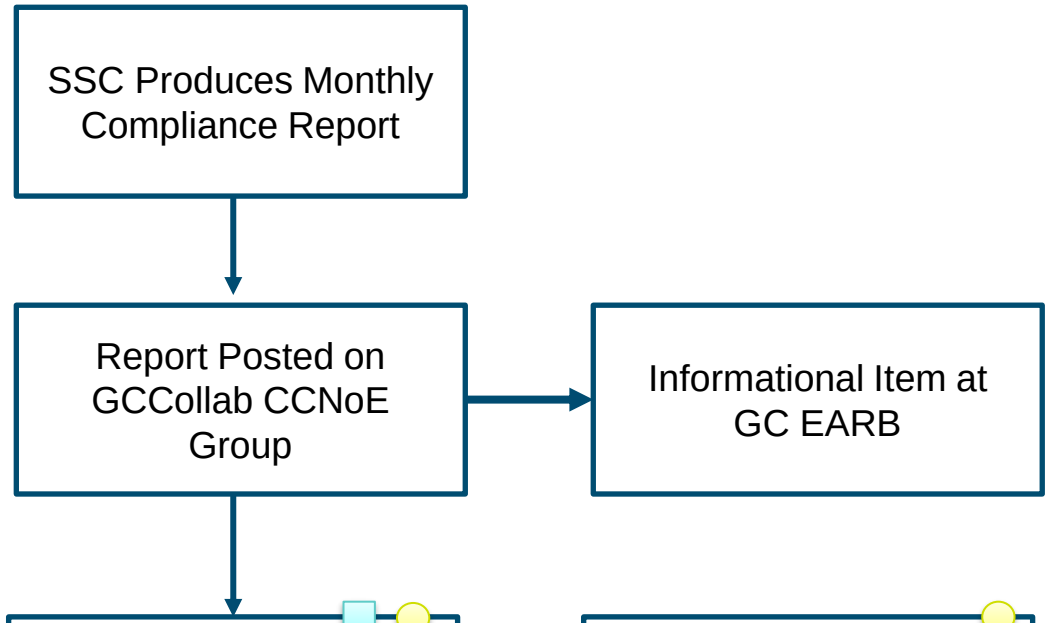
Background: Continuous Improvement

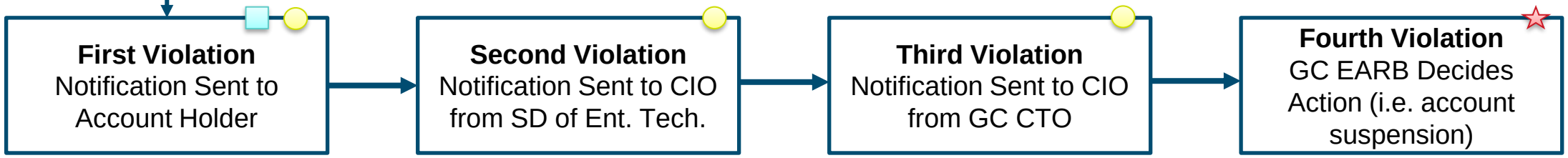
Continuous improvement is driving the need to:

- Change the GC Cloud Guardrail escalation process to immediately notify senior executives of guardrail drift
- Decrease the detection time for guardrail drift
- Decrease the time to take corrective actions against accounts that have drifted out of compliance
- Update the Public Cloud Roles & Responsibilities document to reflect the responsibilities for the GC Guardrails
- Expand the scope of monitoring to include the Office 365 guardrails

Item 1: Escalation Process (Current)

The ***trust, but verify*** model requires departments take corrective actions when their accounts drift outside the guardrails.

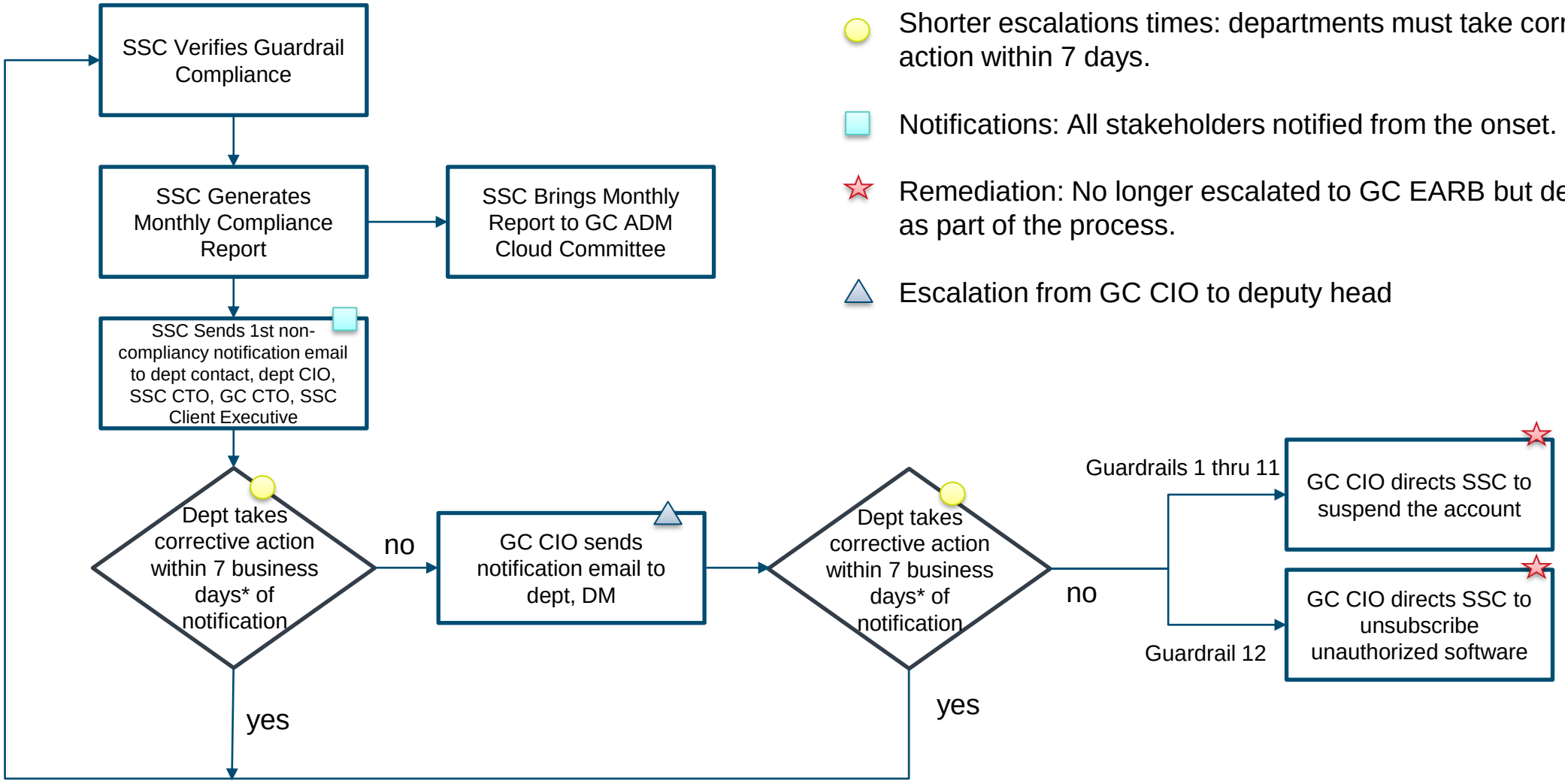




Challenges with current process:

- Long escalations process: many notifications must take place. Time elapse between each notification is not clear
- Notifications: Departmental CIO remains unaware until second notification
- Remediation: Not clear and must be decided by GC EARB on a case-by-case basis.

Item 1: Escalation Process (Proposed)



Changes include:

- Shorter escalations times: departments must take corrective action within 7 days.
- Notifications: All stakeholders notified from the onset.
- Remediation: No longer escalated to GC EARB but defined as part of the process.
- Escalation from GC CIO to deputy head

Item 2: Update Roles and Responsibilities

"The GC Enterprise Architecture Review Board will therefore review all proposals for cloud based, enterprise-wide services and decide when service in the cloud will be mandatory or optional for departments. Decisions about roles and responsibilities for cloud will be recorded as part of a matrix and made available to departments and agencies."

GC Cloud Adoption Strategy

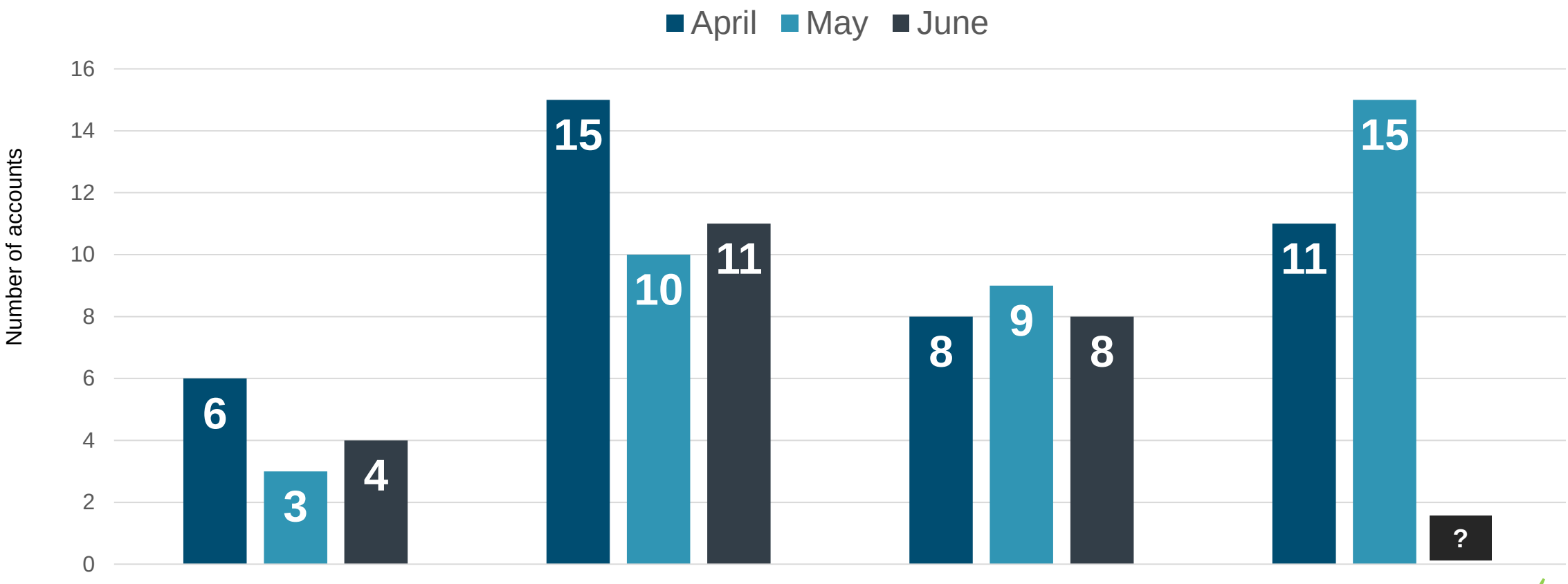
Section	Responsibilities	GC / TBS-CIOB	SSC	CSE	PSPC	RCMP	Departments and Agencies
1.0	**Establish GC-wide governance for cloud**	**A,R**	**C**	**C**	**C**	**C**	**C**
2.0	**Establish GC-wide cloud adoption framework**	**A,R**	**C**	**C**	**C**	**C**	**C**
2.17	Set Guardrails for GC Cloud Environments	**R**					
2.18	Decide upon remediation actions for Guardrail drift	**R**					
3.0	**Establish third-party security assurance**	**C**	**C**	**A,R**	**C**	**C**	**C**
4.0	**Acquire commercial cloud services**	**C**	**A,R**	**C**	**A,R**	**C**	**C**
5.0	**Provide GC cloud brokering services**	**C**	**A,R**	**C**	**C**	**C**	**C**
6.0	**Provide network integration services to cloud-based services**	**C**	**A,R**	**C**			**C**
7.0	**Provide ICAM to cloud-based services**	**C**	**A,R**	**C**			**C**
8.0	**Provide implementation and operation guidance to departments and agencies**	**C**	**A,R**	**C**			**C**
9.0	**Monitor GC-wide cloud operations**	**C**	**A,R**	**C**			**C**
10.0	**Establish departmental governance for cloud-based services**	**C**	**C**	**C**			**A,R**
11.0	**Establish departmental cloud adoption framework**	**C**	**C**	**C**			**A,R**
12.0	**Implement cloud-based services**	**C**	**C**	**C**			**A,R**
13.0	**Operate and maintain cloud-based services**	**I**	**C**	**C**			**A,R**
13.27	Implement and monitor Guardrails						**R**
14.0	**Monitor departmental cloud operations**	**I**	**C**	**C**			**A,R**
15.0	**Perform continuous monitoring of cloud-based services**	**I**	**C**	**C**			**A,R**
15.4	Verify Guardrail compliance		**R**				**I**

The current version of the RACI does not include the roles and responsibilities for the guardrails. With an GC EARB endorsement, the document will be updated.

https://gccollab.ca/file/view/1785973/engc-cloud-roles-and-responsibilities-matrixfr

Accounts Have Drifted, Little Improvement Over Time

Aggregate view of the April, May, and June compliance reports show little improvement over time.



Next Steps

- Endorse the proposed escalation process (item 1)
- Endorse updates the proposed updates to the GC Public Cloud Roles & Responsibilities document (item 2)
- Implement the new notification and escalation process
- The Cloud and Computing Network of Expertise will test new automation capabilities and build a roadmap for including Office 365 guardrails

Annex: Mandatory Guardrails – Compliance Monitoring

From: Sept 19th, GC EARB

Minimum, mandatory, guardrails a department must implement within 30 days. **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
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

Annex: Community Built Automation

The community has responded by building open source automation to verify the guardrails.

Prowler

The community has built GC-specific extensions for the open source tool Prowler that scans AWS accounts for compliance.

https://github.com/canada-ca/cloud-guardrails-aws/tree/master/tools/prowler

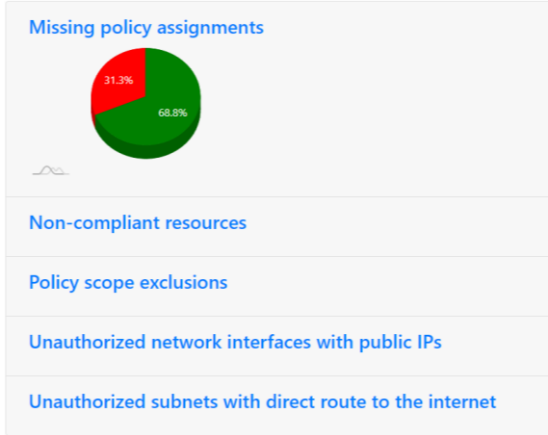
CDS

CDS SNC

CDS has built a guardrails verification tool for AWS using GO than can also be connected to a deployment pipeline.

https://github.com/canada-ca/cloud-guardrails-aws/tree/master/tools/cds_tool

Azure Blueprints



The community has built guardrail policy checks for Azure environments.

https://github.com/canada-ca/cloud-guardrails-azure/tree/master/toolbox