Technical Design Document

PBMM (Protected B, Medium Integrity/Medium Availability) Landing Zone

Date: February 11, 2022

Authors: Google Professional Services

Prepared for: Government of Canada Departments and Agencies

Document type: **TDD**

Contents

Documentation overview

This document assists Google Cloud customers with implementing and formalizing PBMM, Protected B, Medium Integrity, Medium Availability security controls for information systems in GCP. Through this implementation, customers can determine for themselves using the processes required for a PBMM certification for systems and applications hosted in GCP.

The Communications Security Establishment (CSE) has provided Government of Canada (GC) departments and agencies with an Information Security Risk Management framework published as the Information Technology Security Guidance (ITSG-33). Annex 3 of ITSG-33 documents suggested security controls and control enhancements. ITSG-33 is aligned with version 4 of NIST 800-53. Based on ITSG-33, the Canadian Centre for Cyber Security published a set of Cloud Security control profiles for Low (Unclassified), Medium (Protected B), High (Secret and above) workloads. Specifically, for environments with information having the PBMM security category, this document captures the details of a cloud-hosted information system, including the system architecture specifications and security controls implementation.

Google provides two artifacts to assist GC departments and agencies with their PBMM posture - a Landing Zone code repository and this Technical Design Document (TDD) inclusive of an appendix to help map PBMM controls and the methods by which the Landing Zone addresses them:

- **The Landing Zone,** which is a GitHub-hosted, Terraform-based, PBMM compliant Google Cloud Landing Zone that Canadian governments can clone to their own repository, set variables, and deploy.
- **The TDD** (this document) details the system architecture specifications. The included PBMM mapping details the security controls implementation, and documents which controls the Landing Zone environment has inherited from Google, and which controls the department or agency has implemented.

GC departments and agencies can use these two artifacts to provide ITSG-33/PBMM details to any interested parties for their GCP-hosted information system.

Intended audience

This document, along with the included PBMM mapping, are intended to be used by the following personnel within a customer's organization:

- Information System Owner - *primary Google Stakeholder*
- Department or Agency Independent Assessor or 3rd Party Assessment Organization
- GCP Administrators for the Information System
- Department or Agency Security Personnel: CIOs, CTOs, ISSMs, ISSOs, etc.

ITSG-33/PBMM compliance disclaimer

Google maintains alignment to compliance standards on many cloud services to allow customers to build compliant applications and general support systems; however, individual departments and agencies are ultimately responsible for assuring that their IT systems are ITSG-33/PBMM compliant when required.

This Technical Design Document (TDD) outlines the ITSG-33/PBMM aligned Landing Zone implementation and configuration components.

1. Landing Zone Overview

At the lowest level, resources are the fundamental components that make up all Google Cloud services. Examples of resources include Compute Engine Virtual Machines (VMs), Pub/Sub topics, Cloud Storage buckets, App Engine instances. All these lower level resources can only be parented by projects, which represent the first grouping mechanism of the Google Cloud resource hierarchy.

Google Cloud resources are organized hierarchically. Starting from the bottom of the hierarchy, **projects are the first level**, and they contain other resources. **The Organization resource is the root node** of the Google Cloud resource hierarchy and all resources that belong to an organization are grouped under the organization node. This provides central visibility and control over every resource that belongs to an organization.

Folders are an additional grouping mechanism on top of projects. You are required to have an Organization resource as a prerequisite to use folders. Folders and projects are all mapped under the Organization resource.

1.1 The Environment's Bootstrap

This module sets up the initial permissions structure against the Organization Node and enables core GCP services such as Google Cloud Storage so that a repository can be instantiated for Terraform to validate and run the Plan.
This is hosted in subdirectory:
/environments/bootstrap

1.2 Folder Structure

This module creates a baseline folder grouping structure using the naming convention specified.
This is hosted in subdirectory:
/modules/folder

1.3 The Landing Zone's Bootstrap

This module provides the initial structure for the environment including creation of the bootstrap project, storage bucket, service account, and its roles to be used to deploy various Landing Zone infrastructure components.
This is hosted in subdirectory:
modules / landing-zone-bootstrap

1.4 Naming Standard

This module sets the naming convention for the deployed Landing Zone using set variables. This will be used to generate names for resources, roles, and accounts when requested by other modules of the Landing Zone. Each subdirectory hosts code for resources, their configurations, and their variables. Examples include cloud functions, storage, and subnet(s). This is hosted in subdirectory:
/modules/naming-standard/modules/gcp

1.5 Organizational Policy

Organization Policy Constraints enforce compliance at the GCP Organization, folder, or project level. They are a set of predefined rules that prevent certain actions from happening. These built-in policies are defined by Google and enabled by the organization consuming GCP and do not currently offer customization capabilities. These policies help protect the security boundary of the platform.

Several policies are configured by default and these are noted in the code. Some examples include:

- Limiting the regions where resources can be deployed
- Defining allowed external IPs for VM instances
- Restricting allowed Google Cloud APIs and Services
- Enabling Domain Restricted Sharing
- Enforcing uniform bucket-level access
- Requiring OS Login
- Skipping default network creation
- Restricting VM IP Forwarding
- Defining trusted image projects

This is hosted in subdirectory:
/modules/organization-policy

1.6 Project

This module is used to create projects with the appropriate naming convention and inclusive of the default and custom roles and configurations pulled in from modules such as Terraform Project among others.

This is hosted in subdirectory:
/modules/project

1.7 Terraform Project

This module is leveraged by the Network and Bootstrap modules as a way to instantiate new projects. It is also usable in an extended state to use for deploying application projects into the Landing Zone

This is hosted in subdirectory:
/modules/terraform-project

2.0 Identity and Access Management (IAM)

Google Cloud Identity is the product used for managing users, groups, and domain-wide security settings for Workspace and Google Cloud Platform. Cloud Identity is tied to a unique DNS domain that needs to be enabled for receiving email (for example, has an appropriate MX configured) so that users and groups configured with responsibilities in GCP can receive generated notifications.

Cloud Identity configurations are made in the Admin Console. Existing Workspace customers can use their Workspace Admin Console for Cloud Identity. Customers without an existing Workspace account can create a Cloud Identity in the "IAM" section of the GCP Cloud Console.

IAM policies are available for configuration in the Google Cloud Console. IAM roles are available for users, groups of users, and service accounts that allow granular control of permissions to access resources. The organization resource provides a way to unify all projects under a single organization with permission inheritance across the organization.

Identity Aware Proxy (IAP) provides an authenticated proxy that verifies all connections against an access control policy (See Reference: Identity Aware Proxy). It can be used to access resources in a VPC where the source system does not have a route to the destination system, or a firewall rule blocks direct access. All connections through IAP are required to authenticate, and once authenticated, will be routed to the destination service where they can interact with it. This interaction can be simple TCP traffic such as a web service, or more complex like an RDP or SSH session where a credential to access the system would also be required. All IAP traffic is encrypted via TLS.

Access is controlled through IAM roles and is assigned directly to groups, users, or service accounts. This enables granularity in controlling access to systems and ensures that the principle of least privilege is adhered to. Thus, instead of managing bastion hosts, SSH keys, and other components that can cause operational burden, the Landing Zone will be taking advantage of IAP capabilities.

2.1 IAM Configuration

This module is used to create and configure service accounts and users. It is also used to set the appropriate permissions via assignment of roles. Though current functionality is limited to several use cases, it is expandable in the future to support novel use cases and greater ease of automated configuration.

This is hosted in subdirectory:
/modules/iam/

2.2 Organizational Custom Roles

This module is used to create custom roles at the Organization level that can be assigned at the Organization, Folder or Project level. It leverages inputs from Naming Standards and other sources and is called by several other modules in the course of Landing Zone instantiation.

This is hosted in subdirectory:
/modules/org-custom-roles/

3.0 Networking & Resources

Google's worldwide infrastructure consists of regions and, within those regions, zones. Google offers several connectivity options for physical connectivity through direct peering or Google Carrier Interconnect across multiple geographies. Virtual private networks can be built on top of this physical layer and the Cloud Router is available to manage dynamic routes using BGP once that connection is configured. The use of Shared VPCs allows you to centralize networking infrastructure in a single host project and allow other service projects to consume networking resources from the host project.

3.1 DNS

Cloud DNS supports both public (internet resolvable) and private zones (See Reference: DNS Overview). This module is used to create and manage a private zone into each host project, production and non-production and the perimeter project. It also establishes DNS Peering between these two private zones in each host project, and between the production and perimeter projects. The instance of Cloud DNS which is deployed in the perimeter VPC will be configured as a forwarding zone for all other private zones in the Landing Zone. The forwarding zone will handle requests from GCP to domains on-premises. Requests from on-premises to GCP will be resolved using an inbound policy which will be configured in Cloud DNS within the perimeter project.

This is hosted in subdirectory:

/modules/dns-zone/

3.2 Firewall

The GCP VPC Firewall allows for the creation of tag-based flows. This enables GCP instances to be grouped together with common firewall tags and subsequent flow control decisions that can be made based on these tags. Network segmentation is accomplished using network tags to allow traffic between resources on an "as-required" basis, not by restricting traffic at the boundaries of the network segment. As part of the Landing Zone design, all traffic within the VPC, ingress or egress, will be explicitly denied by default. The result of this is a zero-trust network model. This model allows for a more secure network state where east-west network traffic is restricted in the same fashion as north-south traffic.

This module is used to configure GCP firewall settings. Based on the above decisions there are several rules pre-defined and the code allows for custom rules to override them.

This is hosted in subdirectory:
/modules/firewall/

3.2.1 Firewall: Fortigate Appliance

This optional module is available if a Fortigate firewall appliance is desired. This type of NVA firewall will provide functionality including, but not limited to:

- Deep packet inspection
- IDS Capabilities
- WAF Capabilities
- FQDN Filtering

If used, all traffic will first flow through the virtual appliance, before exiting to the public Internet. Traffic which is destined for on-premises will also flow through the NVA before egress to the on-prem environment.

This is hosted in subdirectory:
/modules/fortigate-appliance/

3.3 Network Host Project

This module creates a GCP host network project, VPC, and subnets. Multiple instances of this module can be used to create separate host projects and networks for both production, and non-production.

This is hosted in subdirectory:
network-host-project/

3.4 Network

This module adds a network when it's time to promote a project.

This is hosted in subdirectory:
/modules/network/

3.5 Virtual Machine

This module provides code that can be used to create a Linux or Windows VM with an option to add disks and snapshot policies.

This is hosted in subdirectory:
/modules/virtual-machine/

3.6 VPC Service Controls

To protect from data exfiltration, manage data access controls and data privacy, VPC Service Control will be implemented as part of the Landing Zone (See Reference: VPC Service Control). A single VPC Service Control perimeter will be created for the GCP organization. The on-premises IP ranges, and any required identities will be such that they are recognized and permitted. A VPC Service Control makes sure that data in most GCP services cannot exit the perimeter to an un-recognized network IP, even if they have the appropriate IAM credentials such as a user account or service account.

This module provides code to configure VPC Service Controls. Among the topics available to configure are Organization Access Policy, Access Levels, Regular Service Perimeter, and more.

This is hosted in subdirectory:
/modules/vpc-service-controls/

4.0 Logging

Monitoring and Logging within GCP is provided by two different products, Cloud Monitoring (See Reference: Cloud Monitoring) and Cloud Logging (See Reference: Cloud Logging). These GCP services, in conjunction with Security Command Center, enable a holistic view of resource health in all GCP projects.

Log bunkering is included as part of the Landing Zone configuration. Log bunkering refers to an environment with tight controls to store unaltered logs for a set retention period. These logs are made available for forensic purposes.

This module is designed to work with the requirements for the GCP Landing Zone and is used to satisfy the 30-Day Guardrail requirement for storing unaltered logs. The module creates an audit project with one or many organization log sinks and buckets which can be filtered to store specific logs. The default configuration retains Admin Activity logs, Data Access logs, VPC Flow logs, Firewall Rule logs, and Google Admin logs. These are all bunkered in the separate bunker project. Logs will be collected at the organization level and directly streamed into a locked bucket which is configured with a retention policy. After the bucket is created, configured, and locked, no one can unlock and make any modifications to the bucket or to the logs within the bucket. This ensures that all stored logs are in their original format and unaltered.

This is hosted in subdirectory:
/modules/audit-bunker/

5.0 Automation

These modules provide code that both help deploy and manage the Landing Zone.

5.1 Cloud Build

Terraform is used to deploy and manage changes to the code. Terraform pull requests are picked up by Cloud Build and a Terraform "plan" operation is performed to confirm the change's impact on the environment. Terraform changes merged to the main branch of the bootstrap repository are picked up by Cloud Build, and a Terraform "apply" operation is performed.

This module contains code to create a virtual machine with the cloud builder and the rest of the code needed to begin building the CI/CD pipeline.

This is hosted in subdirectory:
/modules/cloudbuild/

5.2 Guardrails

This module provides code that can be used to create a Google Cloud Function that will import guardrails that can be used to examine a preliminary baseline set of controls within the cloud-based environments.

This is hosted in subdirectory:
/modules/guardrails/

6. Security

6.1 Detective Scanning

Forseti Security (See Reference: Forseti Security) has typically been the recommended approach to detective scanning in a Google Cloud Platform environment. In addition to Forseti, Google is also working on a new feature named *Custom Governance*. This feature is currently in beta, but is the recommended approach for detective scanning after it is generally available.

For now, guardrails will be satisfied using a combination of documentation which defines how the Google Cloud Platform environment will be configured, and asset export validation which will validate some controls using REGO query language. (See Reference: GCP Cloud Guardrails). All asset violation reports will be stored within a GCS Bucket.

At a high level, the validation tool which uses REGO can be broken down into the three following workflows:

1. Export asset inventory
2. Run validation on asset inventory
3. Update validation policy templates

Workflow	Triggered By	Output Artifact
Export Asset Inventory	Cloud Scheduler (Runs Daily)	Asset Inventory (JSON Dump) stored in GCS Bucket
Run Validation on Asset Inventory	Changes in the asset inventory bucket (bucket event notification)	Report of findings
Validation Policy Update	Commit to the guardrails-policies repository	Guardrails Validation Container

6.2 Security Command Center

Security Command Center is a risk management platform for Google Cloud. It is used to surface, understand, and remediate GCP security and data risks across an organization (See Reference: Security Command Center). It is recommended to implement Security Command Center to centralize events of interest across the environment.

Event types that will be gathered are as follows:

- Audit Logs
- VPC flow logs
- Firewall rule logs

Note: *Security Command Center is not currently listed as an approved service on the cloud broker site. A decision would need to be made by the department or agency to allow for an exception where feasible.*

6.3 Secret Management

GCP offers a native secret management solution in the format of GCP Secret Manager (See Reference: Secret Manager). This service provides a central location for applications, application teams, and application operators to access secrets such as application secrets, certificates, and other credentials.

GCP uses IAM to enforce the principle of least privileged where IAM can be assigned at all 4 levels of the GCP organization.

Scope	Access
Organization	All secrets in all projects belonging to the organization
Folder	All secrets in all projects within a given folder
Project	All secrets in a project

Secret / Secret Version	A specific secret or secret version

Platform operators should have access to project level access to secrets in platform team managed projects, but they should not have access to application secrets. Application operators will have access to manage application secrets, which includes creating, updating, or decommissioning secrets in Secrets Manager. In addition to this, the application's own service accounts will have access to individual secret/secret versions, but these service accounts will not be able to read any other secrets.

Secrets Manager has encryption at rest by default using Google Managed Encryption keys. The option to use Customer Managed Encryption Keys is also available and recommended (See Reference: Secrets Manager - Customer Managed Encryption Keys).

Appendix 1: Mapping Controls to Code

Notes:

- Meeting ITSG-33/PBMM requirements will require configuration(s) in additional Google systems (for example, user identities and attributes such as usernames, passwords, multi-factor authentication (MFA), 2-step verification (2SV), and single sign-on (SSO) are configured and managed via Google Workspace or Cloud Identity).
- The controls listed in this document often do not have a 1:1 mapping between the control itself and a singular code block where it can be invoked.
- The header row is automatically pinned so it will appear at the top of each page.
- Rows are configured so they do not break across page boundaries

Table: Controls and code mapping

ITSG-33/PBMM Control Name	Control ID (Enhancement ID)	Control Management	Notes
ACCOUNT MANAGEMENT	AC-2	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity.	Organizations are responsible for managing all aspects of access control for GCP users. This may be achieved by using a managed SAML-based Single Sign-On system and synchronizing this system with GCP. This control is typically addressed via

			breakglass strategy.
ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT	AC-2(1)	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Organizations are responsible for managing all aspects of access control for GCP users. This may be achieved by using a managed SAML-based Single Sign-On system and synchronizing this system with GCP. Organizations are responsible for employing automated mechanisms to support the management of information system accounts used to access GCP; this can include synchronizing access to the existing directory service. This control is typically addressed via breakglass strategy and the initial IdP configuration.
ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES	AC-2(7)	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Organizations are responsible for managing all aspects of access control for GCP users. This may be achieved by using a managed SAML-based Single Sign-On system and synchronizing this system with GCP. Organizations are responsible for utilizing a role-based access scheme for accounts used to access GCP. Organizations are responsible for monitoring privileged roles, assigning, and revoking accounts used for privileged access to GCP. The Landing Zone template uses custom roles and Cloud IAM to provide example roles in role-based access schemes.
ACCESS ENFORCEMENT	AC-3	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles /modules/organization	Organizations are responsible for managing all aspects of access control for GCP users. This may be achieved by using a managed SAML-based Single Sign-On system and synchronizing this system with GCP. Organizations are responsible for enforcing access for users to GCP resources in accordance with applicable access control policies. The Landing Zone template uses custom roles, Cloud IAM, and GCP organizational policies to limit unnecessary access.

		-policy Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	
INFORMATION FLOW ENFORCEMENT	AC-4	Variables for environment, region, org policy, and more must be configured here: /environments/bootstrap Information flow control is configured using a combination of sources here: /modules/dns-zone /modules/fortigate-appliance /modules/network-host-project /modules/network /modules/vpc-service-controls Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Organizations are responsible for controlling the flow of information within the organization's system, including components built in GCP, and between the organization's system and other interconnected systems. Organizations using GCP-hosted resources employing a Google-managed SaaS Runtime component are responsible for establishing and configuring a global load balancer and Cloud NAT device within the GCP project to support connection to API backends and API clients. The organization must then configure these devices to control the flow of information between backend services and consumers of the organization's APIs. The organization also provides configuration information to the GCP Console to configure the VPCs to communicate with the GCP project. The Landing Zone template uses DNS-zones, Network Virtual Appliance Firewalls, Virtual Private Cloud (VPC) networking, and VPC service controls to satisfy this requirement.
SEPARATION OF DUTIES	AC-5	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Organizations are responsible for defining separation of duties through assigned group and role authorization for GCP users. The Landing Zone uses predefined roles, custom IAM roles, and service accounts to appropriately restrict resource configuration and separation of duties.
LEAST PRIVILEGE	AC-6	Controls are inherited from the selected IdM platform, e.g. Google	Organizations are responsible for employing least privilege within the organization's system, including components built in GCP.

		Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	GCP's Cloud Console service is part of the GCP Management Tools product family and is used by Organizations to manage their GCP services. To help address the least privilege requirement Organizations may elect to limit Cloud Console administrative access to a security group that contains only users who require that access. The Landing Zone uses predefined roles, custom IAM roles, and service accounts to appropriately restrict resource configuration and separation of duties. Role assignment determines the user's abilities to affect resource configuration. The system also offers IAM recommendations.
LEAST PRIVILEGE | PRIVILEGED ACCOUNTS	AC-6(5)	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Organizations are responsible for defining personnel or roles appropriate for being assigned to privileged accounts. The Landing Zone template uses GCP Service Account access to these privileged accounts. The Organizational Administrator role should be used sparingly in alignment with the breakglass strategy.
LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	AC-6(10)	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code	Organizations are responsible for preventing non-privileged users from executing privileged functions for all organization controlled components hosted on GCP. GCP allows Organizations to assign administrative and non-administrative roles to user accounts within GCP. Non-administrative roles cannot perform privileged functions within the GCP project, including disabling, circumventing, or altering implemented security safeguards/countermeasures. The Landing Zone template uses GCP Service Account access to these privileged accounts. The Organizational Administrator role should be used sparingly in alignment with the breakglass strategy.

		provided here: /modules/cloudbuild	
REMOTE ACCESS | AUTOMATED MONITORING / CONTROL	AC-17 (1)	Logs and controls are available from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Organizations are responsible for monitoring and controlling remote access methods to systems. The Landing Zone template deploys an immutable log bunker for collecting logging data. Organizations can use these logs for performing automated actions. The Landing Zone template also uses the Identity Aware Proxy, a feature that uses identity and context to guard access to services and VMs.
AUDITABLE EVENTS	AU-2	Logs and controls are available from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Google Cloud system and audit logs are managed in the operations suite. Configurations of resources such as cloud storage bucket(s) and log sink(s), and their attributes such as storage class and retention policy may be configured using using code here: /modules/audit-bunker Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	GCP allows developers to write code and manage cloud resources to determine what audit logs are generated and for how long they are retained. It is the organization's responsibility to ensure that developed systems hosted on GCP and managed by the organization are capable of auditing the appropriate auditable events. GCP has identified the following additional types of auditable events reviewed and managed by Google but pertaining to information systems hosted on GCP: account management events, privilege changes, authentication checks, authorization checks, data deletions, data changes, and permission changes. The Landing Zone template deploys a locked storage bucket as an immutable log bunker for storing forensic log data (for audit purposes) by using an organizational log sink. The retention length is configurable.
CONTENT OF AUDIT RECORDS	AU-3	Logs and controls are available from the selected IdM platform, e.g. Google Workspace or Cloud	GCP allows developers to write code and manage cloud resources to determine what audit records are generated and what information is contained within audit records. The GCP admin activity log produces audit

		Identity. Google Cloud system and audit logs are managed in the operations suite.	records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, the source of the event, the outcome of the event, and the identity of any user/subject associated with the event. In the case of the admin activity log, "where the event occurred" is implied as occurring within the GCP projects, folders or organizations. In addition to the admin log available through the GCP Cloud Console, application logs on application activity are available through the GCP Cloud Console and Organizations have the option to customize logs for their applications. Organizations may elect to use several GCP tools like Admin Audit Logs and Data Access Logs to ensure that sufficient logging exists to establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. Organizations should ensure that they properly configure appropriate GCP audit logs where applicable and set up additional logs where needed. The Landing Zone template deploys a locked storage bucket as an immutable log bunker for storing forensic log data (for audit purposes) by using an organizational log sink. The retention length is configurable.
CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT	AU-3(2)	Logs and controls are available from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Google Cloud system and audit logs are managed in the operations suite.	The Landing Zone template deploys a locked storage bucket as an immutable log bunker for storing forensic log data (for audit purposes) by using an organizational log sink. The retention length is configurable.
RESPONSE TO AUDIT PROCESSING FAILURES	AU-5	Logs and controls are available from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Google Cloud system and audit logs are managed in the operations suite.	In the event of an audit processing task failure, Google's infrastructure automatically re-assigns the failed task to another available resource. This usually results in no actual audit processing failure. Manual intervention in this process is rarely required. If manual intervention is required, alerting is performed to allow responsible groups to fix the audit processing components that fail. The GCP Site Reliability Engineering (SRE) Team is alerted. As a first line of action, the

			SRE Team isolates the failed components and disconnects them from the network. Organizations are responsible for monitoring and remediating audit processing failure for their systems and applications
AUDIT REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS	AU-6(4)	Logs and controls are available from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Google Cloud system and audit logs are managed in the operations suite.	For GCP, Google retains online data access audit logs for thirty (30) days. It will then be the organization's responsibility to offload those audit log records from the GCP console within that 30-day window. At that point, the organization will be responsible for its own audit log review for any anomalous behavior within its GCP instance. The Landing Zone template deploys a locked storage bucket as an immutable log bunker for storing forensic log data (for audit purposes) by using an organizational log sink. The retention length is configurable.
TIME STAMPS	AU-8	Logs and controls are available from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Google Cloud system and audit logs are managed in the operations suite.	GCP allows developers to write code and manage cloud resources. This includes using time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and provides at least one second granularity of time measurement for audit logs that are generated by systems hosted in GCP. Organizations can leverage or reference the Cloud Operations suite of tools to help meet this requirement for their IT system(s) on Google Cloud
PROTECTION OF AUDIT INFORMATION	AU-9	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Only authorized users can use Google's proprietary audit tools. Access to the audit tools is restricted using Machine ACL system groups. Audit tools will not provide a result to the user unless access to view logs is granted. Audit information is protected from unauthorized modification and deletion through checksums of the records it reads from production machines. A verification protocol is used to verify the integrity of log files stored in the log repository. Organizations are responsible for protecting audit information and audit tools from unauthorized access, modification, and deletion. The Landing Zone uses predefined roles, custom IAM roles, and service accounts to appropriately restrict resource configuration. Additionally, a locked log bunker is deployed for logs storage. Care should be given to access to this resource.
PROTECTION OF	AU-9(4)	Controls are inherited	GCP allows developers to write code and

AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS		from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	manage cloud resources. Many GCP services generate audit logs for systems built on those GCP services. Only users/groups can view the audit logs with specific Identity and Access Management roles. Organizations can configure who can view and export their audit logs within their GCP project or organization. The Landing Zone uses predefined roles, custom IAM roles, and service accounts to appropriately restrict resource configuration. Additionally, a locked log bunker is deployed for logs storage. Care should be given to access to this resource. Service accounts are deployed as part of the Landing Zone template. These can be used to control access to resources by only privileged users.
AUDIT GENERATION	AU-12	Logs and controls are available from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Google Cloud system and audit logs are managed in the operations suite.	The Google Security Team requires that all components of the production environment and applications are capable of generating the defined auditable events as described in AU-2. This is accomplished via the Security Logging Policy. Organizations are responsible to determine the roles and responsibilities to select which auditable events are to be audited by specific components of the information system to satisfy their obligations for compliance.
BASELINE CONFIGURATION	CM-2	Variables for environment, region, org policy, and more must be configured here: /environments/bootstrap Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Organizations are responsible for developing, documenting, and maintaining under configuration control the baseline configurations of their GCP information system resources. Organizations may elect to use the GCP's Cloud Deployment Manager or Terraform which allows Organizations to develop a repeatable process for creating and managing configuration baselines. Configurations are maintained via Cloud Build CI/CD pipelines, guided by the organization's standard change procedures.
CONFIGURATION CHANGE CONTROL	CM-3	Variables for environment, region, org policy, and more must be configured here: /environments/bootstrap Modifications to the configuration(s) can be made using code provided here:	Organizations are responsible for reviewing, documenting, implementing, and recording configuration-controlled changes to systems and applications. Configurations are maintained via Cloud Build CI/CD pipelines, guided by the organization's standard change procedures.

		/modules/cloudbuild	
ACCESS RESTRICTIONS FOR CHANGE	CM-5	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Google defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Any and all changes to the information system require logical access. Engineering teams are physically segregated from the datacenter in which the equipment is housed. Those with physical access do not have logical access permissions to make changes. Organizations are responsible for defining, documenting, approving, and enforcing logical access restrictions associated with changes to their information system. The Landing Zone uses predefined roles, custom IAM roles, and service accounts to appropriately restrict resource configuration. A hierarchical folder structure provides another means of centralized access control. Labels can be used as an additional means of managing resources.
LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING	CM-7(5)	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Organizations are responsible for configuring their information system to provide only essential capabilities; and prohibiting or restricting the use of the following functions, ports, protocols, and/or services in accordance with their compliance regime. Binary Authorization allows for deploy-time security controls to ensure that only trusted container images are deployed on Kubernetes. Requires images to be signed by trusted authorities during development and enforces signature validation during deployment. Configurations are maintained via Cloud Build CI/CD pipelines, guided by the organization's standard change procedures. Leveraging additional tooling like Binary Authorization is optional and up to the organization.
INFORMATION SYSTEM COMPONENT INVENTORY	CM-8	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here:	Cloud Resource Manager allows for the Hierarchically managed resources by project, folder, and organization. Centrally control org & access policies and asset inventories. Label resources for better management. Inventory of assets can be viewed through this interface. Additionally the Cloud Asset Inventory service provides inventory services based on a time series database. This database keeps a five-week history of Google Cloud asset

		/modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	metadata. Cloud Asset Inventory allows you to: ● Search asset metadata by using a custom query language ● Export all asset metadata at a certain timestamp or export event change history during a specific timeframe ● Monitor asset changes by subscribing to real-time notifications ● Analyze IAM policy to find out who has access to what
ALTERNATE PROCESSING SITE	CP-7	Variables for environment, region, org policy, and more must be configured here: /environments/bootstrap Processing site(s) selection may be configured using a combination of sources here: /modules/dns-zone /modules/fortigate-appliance /modules/network-host-project /modules/network Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Google does not use traditional alternative site arrangements, but instead the Google Global Capacity Delivery (GCD) team maintains a number of concurrently operating locations. Google databases use a combination of synchronous and asynchronous replication methods that write data to multiple clusters Data replication on the backend is continuous and spans multiple data centers, in order to prevent data loss in case of local failure up to and including loss of an entire data center. Consequently, Google does not design 'recovery' or 'reconstitution' procedures based on a Business Impact Analysis to calculate tolerances for alternative site processing timelines but instead employs the techniques described below to minimize downtime. Google has designed the production infrastructure and operations with potential failure of components in order to plan for and address traditional contingencies faced by organizations such as hardware failure, data center outages, denial of service attacks, office space unavailability and people related emergencies. Google plans for these traditional contingencies through Failure prevention, Scalable operations, Redundant architecture, Continuous global operations & trained workforce. Organizations are responsible for: ● Establishing an alternate processing site including necessary agreements to permit the transfer and resumption of information system operations for essential missions/business functions when the primary processing capabilities are unavailable; ● Ensuring that equipment and supplies

			required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined duration for transfer/resumption; and ● Ensuring that the alternate processing site provides information security safeguards equivalent to that of the primary site. Organizations using services built on GCP should configure their use of the service to provision multiple regions to ensure their data storage and processing is replicated between multiple geographically dispersed sites. The Landing Zone template defaults to northamerica-northeast1 (Montreal) and can be modified to be northamerica-northeast2 (Toronto). The organization chooses the best suitable location.
IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	IA-2	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Organizations are responsible for managing all aspects of authentication for GCP users. This may be achieved by using a managed SAML-based Single Sign-On system and synchronizing this system with GCP. This control is typically addressed via breakglass strategy.
IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS	IA-2 (1)	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles	Organizations are responsible for managing all aspects of authentication for GCP users, including implementing multi-factor authentication for access to privileged accounts. This may be achieved by using a managed SAML-based Single Sign-On system and synchronizing this system with GCP. The Landing Zone uses predefined roles, custom IAM roles, and service accounts to appropriately restrict resource configuration. The Landing Zone template also uses the Identity Aware Proxy, a feature that uses identity and context to guard access to services and VMs. IAP can be used to

		Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	provide a secure tunnel to GCP resources and replaces the Bastion Host concept (referenced in the project and firewall modules).
IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS	IA-2 (2)	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Organizations are responsible for managing all aspects of authentication for GCP users, including implementing multi-factor authentication for access to privileged accounts. This may be achieved by using a managed SAML-based Single Sign-On system and synchronizing this system with GCP. The Landing Zone uses predefined roles, custom IAM roles, and service accounts to appropriately restrict resource configuration. The Landing Zone template also uses the Identity Aware Proxy, a feature that uses identity and context to guard access to services and VMs. IAP can be used to provide a secure tunnel to GCP resources and replaces the Bastion Host concept (referenced in the project and firewall modules).
IDENTIFICATION AND AUTHENTICATION | REMOTE ACCESS - SEPARATE DEVICE	IA-2 (11)	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Organizations are responsible for managing all aspects of authentication for GCP users, including implementing multi-factor authentication for users and ensuring that the devices used by their multi-factor authentication system for access to the Google Cloud is provided by a device separate from the system gaining access and that the device meets FIPS 140-2, NIAP Certification, or NSA approval. This may be achieved by using a managed SAML-based Single Sign-On system and synchronizing this system with GCP via Google Cloud Directory Sync. Organizations are responsible for using multi-factor authentication for users and ensuring that the devices used by their multi-factor authentication system for access to the Google Cloud is provided by a device separate from the system gaining access and that the device meets FIPS 140-2, NIAP Certification, or NSA approval. The Landing Zone uses predefined roles, custom IAM roles, and service accounts to appropriately restrict resource configuration. The Landing Zone template also uses the Identity Aware Proxy, a feature that uses identity and context to guard access to services and VMs. IAP can be used to provide a secure tunnel to GCP resources

			and replaces the Bastion Host concept (referenced in the project and firewall modules).
IDENTIFIER MANAGEMENT	IA-4	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Organizations are responsible for managing all aspects of authentication for GCP users, including creating user accounts within their own authentication system and for obtaining authorization from the appropriate administrator before assigning identifiers to their users. This may be achieved by using a managed SAML-based Single Sign-On system and synchronizing this system with GCP. These users will carry over to IAM through the sync to Google.
AUTHENTICATOR MANAGEMENT	IA-5	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Organizations are responsible for managing all aspects of authentication for GCP users, including creating user accounts within their own authentication system and for obtaining authorization from the appropriate administrator before assigning identifiers to their users. This may be achieved by using a managed SAML-based Single Sign-On system and synchronizing this system with GCP. These users will carry over to IAM through the sync to Google. Organizations are responsible for verifying the identity of users as part of their initial authenticator distribution process. Organizations are responsible for establishing initial authenticator content for user accounts. Organizations are responsible for ensuring that authenticators meet authenticator strength requirements. Organizations are responsible for establishing and implementing procedures for the distribution, loss, and revoking of users' authenticators.
AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION	IA-5(1)	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts	Organizations are responsible for managing all aspects of authentication for GCP users. This includes, if temporary passwords are used in the system, issuing temporary passwords for system logons with an immediate change to a permanent password. This may be achieved by using a managed SAML-based Single Sign-On system and synchronizing this system with GCP

		using code provided here: /modules/iam /modules/org-custom-roles	
AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS	IA-5 (7)	Controls are inherited. Google Cloud protects information at rest by default (Google Security Whitepaper)	Organizations are responsible for ensuring that static authenticators are not embedded in applications, access scripts or stored on function keys.
AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS	IA-5 (13)	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Password and 2SV settings are configured in the IdM platform.	Organizations are responsible for managing all aspects of authentication for GCP users, including prohibiting the use of cached authenticators after a defined period. This may be achieved by using a managed SAML-based Single Sign-On system and synchronizing this system with GCP. Users are continually synced to Google and users removed from the sync will lose their account within GCP.
AUTHENTICATOR FEEDBACK	IA-6	Controls are inherited. Google Cloud protects information at rest by default (Google Security Whitepaper)	Organizations are responsible for managing all aspects of authentication for GCP users, including ensuring that authenticator feedback is obscured during the authentication process. This may be achieved by using a managed SAML-based Single Sign-On system and synchronizing this system with GCP.
IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	IA-8	Controls are inherited from the selected IdM platform, e.g. Google Workspace or Cloud Identity. Permissions may be applied to provisioned users, groups, and service accounts using code provided here: /modules/iam /modules/org-custom-roles Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Non-organizational users are not permitted access to the production network. Organizations who access production services are discussed under the responsibilities in IA-2, which outlines the requirements for Organizations to identify and authenticate the organizational users. Organizations are responsible for managing all aspects of authentication for GCP users. This includes uniquely identifying and authenticating non-organizational users (or processes acting on behalf of non-organizational users). This may be achieved by using a managed SAML-based Single Sign-On system and synchronizing this system with GCP The Landing Zone template deploys an organizational policy to enforce domain restricted sharing. This will only allow directory IDs within the allowed domain list as a GCP IAM entity, effectively blocking all other organizational accounts, such as and not limited to Gmail accounts.
VULNERABILITY SCANNING	RA-5	Vulnerability scanning for containers may be	The Google Security Team performs monthly infrastructure and web application scans, and

		done via Google Artifact Registry, Cloud Security Command Center, and/or Kubernetes Engine's Binary Authorization. Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	proprietary database checks as part of Google's vulnerability management process as part of Google's continuous monitoring exercise. Monthly scans consist of internal scans of the Google Cloud Infrastructure using a combination of Commercial Off the Shelf (COTS) and Google's proprietary vulnerability scanning tools. A 3PAO using a COTS vulnerability scan tool scans external web applications monthly. The 3PAO also regularly audits Google's internal scan tools to ensure that they are working correctly. Google also has in place a Vulnerability Rewards Program (VRP) that encourages crowdsourced vulnerability reporting on its GCI. More information about Google VRP can be found at https://www.google.com/about/appsecurity/reward-program/. The Landing Zone template includes a guardrails module that routinely scans for compliance. Cloud Security Command Center offers centralized vulnerability and threat reporting features.
DENIAL OF SERVICE PROTECTION	SC-5	Variables for environment, region, org policy, and more must be configured here: /environments/bootstrap Application-level DoS protection is configured using Cloud Armor and/or a combination of sources here: /modules/network-host-project /modules/network /modules/vpc-service-controls Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Organizations are responsible for assuring that their information systems resources built on GCP are protected against or limits the effects of denial of service attacks. Organization VMs are not behind the Google Front End (GFE) and require additional protection from DDOS attacks. Organizations may elect to use the GCN multi-region load balancer in the Compute Engine product to get DDoS protection from Google; enable Google Cloud HTTP(s) and SSL proxy load balancing for their GCE instances to mitigate DDoS attacks; or purchase and configure another commercial product. Google Cloud Load balancers can handle a sudden spike in traffic by distributing the traffic across all the back ends with available capacity. Organizations using GCP-hosted resources are responsible for configuring denial of service protections for assets hosted in GCP projects. The GCP CloudArmor service is typically utilized for this protection.
BOUNDARY PROTECTION	SC-7	Variables for environment, region, org policy, and more must be configured here:	Organizations are responsible for ensuring their GCP systems resources are connected to external network systems through managed interfaces that are consistent with organization's security architecture. Not all

		/environments/bootstrap Boundary protection is configured using a combination of sources here: /modules/network-host-project /modules/network /modules/vpc-service-controls Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	user and application traffic is monitored by Google. Applications hosted on GCP may bypass the GFE if they are using Cloud VPN, Cloud Interconnect, single instance VM (since it uses a public IP address by default), or support public endpoint access, e.g., GKE clusters. Organizations can segment their networks with a global distributed firewalls to restrict access to certain instances. Organizations using GCP-hosted resources have the capability to host their own GCP resources on the ingress and egress points. Organizations are responsible for implementing managed interfaces and controlling communications at these boundaries, as the nature of the traffic to APIs is known and managed by administrators. Organizations will typically utilize load balancers and Cloud NAT to provide these functions. The Landing Zone template includes an option to deploy a network virtual appliance as part of the perimeter environment's protection scheme. VPC service controls also provide data protection.
BOUNDARY PROTECTION | ACCESS POINTS	SC-7(3)	Variables for environment, region, org policy, and more must be configured here: /environments/bootstrap Boundary protection is configured using a combination of sources here: /modules/network-host-project /modules/network /modules/vpc-service-controls Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Organizations are responsible for limiting the number of external network connections for systems utilizing GCP. Additionally, Organizations are required to ensure that machines connecting to Google Cloud are configured to use appropriate encryption for Google-to-agency communications. The Landing Zone template includes an option to deploy a network virtual appliance as part of the perimeter environment's protection scheme. VPC service controls also provide data protection.
BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION	SC-7(5)	Variables for environment, region, org policy, and more must be configured here: /environments/bootstrap	Organizations are responsible for implementing a deny all; permit by exception policy at their managed interfaces. This is the default posture within GCP Organizations using GCP-hosted resources are responsible for implementing a deny all; permit by exception policy at their managed

		Boundary protection is configured using a combination of sources here: /modules/network-host-project /modules/network /modules/vpc-service-controls Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	interfaces connecting to the runtime. The Landing Zone template has a default deny posture for the VPC firewall rules; a rule match must exist to allow for traffic to traverse the VPC. The ingress/egress to the environment is restricted via the perimeter project and VPC.
TRANSMISSION CONFIDENTIALITY AND INTEGRITY	SC-8	Variables for environment, region, org policy, and more must be configured here: /environments/bootstrap Boundary protection is configured using a combination of sources here: /modules/network-host-project /modules/network /modules/vpc-service-controls Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	Organizations are required to ensure that machines connecting to Google Cloud are configured to use an encryption for Google-to-agency communications that meets Agency requirements. All traffic within the Google Cloud environment is encrypted by default. The Landing Zone template ensures that TLS encryption is required for all load balancers.
CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC-12	Controls for generating, managing, using, rotating, and destroying cryptographic keys are made via the Cloud Key Management Service.	Organizations are responsible for establishing and managing cryptographic keys for cryptography employed within their GCP instance. Organizations may elect to use the Cloud Key Management Service which allows Organizations to manage encryptions for their GCP cloud services the same way they do in their local environment. The Cloud Key Management Service allows Organizations to generate, use, rotate and destroy FIPS 140-2 compliant cryptographic encryption keys.
PUBLIC KEY INFRASTRUCTURE CERTIFICATES	SC-17	Public key certificates are managed by Google Cloud load balancers. Modifications to the configuration(s) can be made using code	Organizations using GCP-hosted resources are responsible for key management supporting encrypted network connections with their use of the services, including generating keys, sending private keys, and updating keys. The Cloud Key Management Service allows Organizations to generate, use, rotate and destroy FIPS 140-2 compliant

		provided here: /modules/cloudbuild	cryptographic encryption keys. Organizations should follow their certificate policy.
PROTECTION OF INFORMATION AT REST	SC-28	Controls are inherited. Google Cloud protects information at rest by default (Google Security Whitepaper)	Google effectively establishes and manages cryptographic keys in accordance with Google-specific practices. Google follows formal practices for key generation, distribution, storage, access and destruction that are informed by industry best practices and NIST SP 800-57 - Recommendation for Key Management. Encryption utilized within the GCP environment is FIPS 140-2 certified (cert #3678, #3383, #3384). Google transparently encrypts core content data at rest for user-generated Drive data. Data stored is uniquely labeled and inventoried to allow the file system to identify the location and ownership of end-user data. Data is not stored in a typical file structure but in data "chunks" that are stored on local disks and identified by a unique chunkID. A file is represented as a collection of stripes. A stripe is a list of pointers to chunks in chunkID/location pairs. Google encrypts data as it is written to disk with a unique combination of a per-chunk encryption key and per end-user Access Control List (ACL) permissions. Google uses a proprietary service to manage the distribution, generation and rotation of cryptographic keys. Files or data structures with user-generated content are encrypted with a key. This key is encrypted by the Key Management Service with a restricted ACL of services allowed to request the Key Management Service to decrypt it. The encrypted key is stored alongside the encrypted data. The wrapping keys needed to decrypt user data are only known to the Key Management Service. All access to/from the Key Management Service is controlled by ACLs. Access is restricted to a limited number of individuals and applications, and auditing is enabled to determine whether access is appropriate. Key Management Google uses a proprietary service to manage the generation, distribution, storage, access, rotation and destruction of cryptographic keys. Files or data structures with user-generated content written by services

			are encrypted with a key. This key is encrypted by the Key Management Service with a restricted ACL of services allowed to request the Key Management Service to decrypt it. The encrypted key is stored alongside the encrypted data. The wrapping keys needed to decrypt user data are only known to the Key Management Service. All access to/from the Key Management Service is controlled by ACLs. Access is restricted to a limited number of individuals and applications, and auditing is enabled to determine whether access is appropriate. Key Management Server The Key Management Service is hosted on a custom-designed operating system based on a stripped-down and hardened version of Linux. Google's servers and their OS are designed for the sole purpose of providing Client Services. This homogeneous environment is maintained by proprietary software that continually monitors systems for binary modifications. If a modification is found that differs from the standard Google image, the system is automatically returned to its official state. These automated, self-healing mechanisms are designed to enable Google to monitor and remediate destabilizing events, receive notifications about incidents, and slow down potential compromise on the network. Key Rotations Google uses a proprietary system to periodically generate and rotate an encryption key used to protect user data at rest on average at least every 90 days. New wrapped encryption keys are generated for each new Google storage file (a Google file is defined in Encryption of Data Stored at Google above). The system helps ensure that key rotations are managed appropriately and that data is not encrypted with a discarded key. GCP provides encryption at rest by default. There are no additional settings included in the Landing Zone template to change this posture.
FLAW REMEDIATION	SI-2	Controls are inherited from the Security Command Center	Google identifies, reports, and corrects information system flaws on the network and within Google applications as part of the Continuous Monitoring program.

			Configurations are maintained via Cloud Build CI/CD pipelines, guided by the organization's standard change procedures.
MALICIOUS CODE PROTECTION	SI-3	Controls are inherited from the Security Command Center	Google employs malicious code protection mechanisms at relevant production entry and exit points. The malicious code protection mechanisms employed include antivirus software, phishing detection software, and use of secure coding for externally facing systems to prevent malicious code injections. It is the organization's responsibility to ensure their tenant is protected from malicious code. There are several GCP services that can be leveraged to do this including but not limited to: Cloud Security Scanner - Automatically scan App Engine, Compute Engine, and Kubernetes Engine applications for common vulnerabilities such as XXS, flash injection, mixed HTTP(S) content, outdated and insecure libraries https://cloud.google.com/security-scanner/ Container Registry: Container Analysis - Scan container images stored in Container Registry for common vulnerabilities https://cloud.google.com/container-registry/docs/container-analysis Cloud Armor - Protect your infrastructure and web applications from Distributed Denial of Service (DDoS) attacks https://cloud.google.com/armor/ The Landing Zone template includes an option to deploy a network virtual appliance as a perimeter device. Individual vendor technology may be used to protect against malicious code.
MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT	SI-3(1)	Controls are inherited from the Security Command Center	Google employs several malicious code mechanisms that are centrally managed by Google Engineering. Malicious code protection mechanisms are updated on a continuous basis and as new signatures that need to be eradicated are identified. The anti-virus software on machines is configured to check for signature definition updates every hour. Content filtering mechanisms are updated by internal Google groups in response to new patterns and/or activities identified in traffic that need to be protected against. Malicious code protection mechanisms perform scans at least weekly to provide

			protection against malicious code. Cloud Security Command Center offers centralized vulnerability and threat reporting features. The Landing Zone template includes an option to deploy a network virtual appliance as a perimeter device. It, too, could be used as a central point of management.
MALICIOUS CODE PROTECTION | NONSIGNATURE-BASED DETECTION	SI-3(7)	Controls are inherited from the Security Command Center	Google also implements non-signature-based malicious code detection mechanisms through the use of heuristics when performing threat profiling, antivirus and antimalware functions. Some attachments are run in a sandboxed virtual machine and evaluated to attempt to determine whether malicious activity occurs. This sandboxing and evaluation occurs automatically in order to attempt to prevent malicious attachments from being delivered to the user. Additionally, Google uses its proprietary event management tool to monitor potential signals that indicates suspicious or malicious behavior such as that exhibited by malicious code. Machine events are collected into a centralized log repository and automatically analyzed by Google-defined rules. For more information on the Google proprietary event management tool. The Landing Zone template includes an option to deploy a network virtual appliance as a perimeter device. Individual vendor technology may offer non-signature based detection.
INFORMATION SYSTEM MONITORING	SI-4	Google Cloud system and audit logs are managed in the operations suite. Configurations of resources such as cloud storage bucket(s) and log sink(s), and their attributes such as storage class and retention policy may be configured using using code here: /modules/audit-bunker Modifications to the configuration(s) can be made using code provided here: /modules/cloudbuild	The Google Security Team continuously monitors internal and industry trends, including alerts from advisory bodies like US-CERT. This ranges from individual vulnerabilities and malware indicators to general attacker behaviors. Google measures the number of events and incidents over time and analyze these metrics based on dimensions such as product area, type and priority. Google's Cloud Operations Suite is Google's embedded observability suite designed to monitor, troubleshoot, and improve cloud infrastructure, software, and application performance. Cloud Operations Suite's components include: Logging, Error Reporting, Debugger, Profiler, and Trace. The Landing Zone template deploys an immutable log bunker for collecting logging data. This information could be imported into a centralized SIEM tool.