

# CIS Google Cloud Platform Foundation Benchmark

v3.0.0 - 03-29-2024

# Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

# Table of Contents

<b>Terms of Use .....</b>	<b>1</b>
<b>Table of Contents .....</b>	<b>2</b>
<b>Overview .....</b>	<b>6</b>
Intended Audience.....	6
Consensus Guidance .....	7
Typographical Conventions.....	8
<b>Recommendation Definitions.....</b>	<b>9</b>
Title.....	9
Assessment Status.....	9
Automated .....	9
Manual.....	9
Profile .....	9
Description.....	9
Rationale Statement .....	9
Impact Statement.....	10
Audit Procedure.....	10
Remediation Procedure.....	10
Default Value.....	10
References .....	10
CIS Critical Security Controls® (CIS Controls®).....	10
Additional Information.....	10
Profile Definitions .....	11
Acknowledgements .....	12
<b>Recommendations .....</b>	<b>14</b>
<b>1 Identity and Access Management.....</b>	<b>14</b>
1.1 Ensure that Corporate Login Credentials are Used (Manual) .....	15
1.2 Ensure that Multi-Factor Authentication is 'Enabled' for All Non-Service Accounts (Manual) .....	17
1.3 Ensure that Security Key Enforcement is Enabled for All Admin Accounts (Manual) .....	19
1.4 Ensure That There Are Only GCP-Managed Service Account Keys for Each Service Account (Automated) .....	21
1.5 Ensure That Service Account Has No Admin Privileges (Automated) .....	24
1.6 Ensure That IAM Users Are Not Assigned the Service Account User or Service Account Token Creator Roles at Project Level (Automated) .....	28
1.7 Ensure User-Managed/External Keys for Service Accounts Are Rotated Every 90 Days or Fewer (Automated) .....	32

1.8 Ensure That Separation of Duties Is Enforced While Assigning Service Account Related Roles to Users (Automated) .....	35
1.9 Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible (Automated) .....	38
1.10 Ensure KMS Encryption Keys Are Rotated Within a Period of 90 Days (Automated) .....	41
1.11 Ensure That Separation of Duties Is Enforced While Assigning KMS Related Roles to Users (Automated) .....	44
1.12 Ensure API Keys Only Exist for Active Services (Automated) .....	47
1.13 Ensure API Keys Are Restricted To Use by Only Specified Hosts and Apps (Manual) ...	49
1.14 Ensure API Keys Are Restricted to Only APIs That Application Needs Access (Automated) .....	52
1.15 Ensure API Keys Are Rotated Every 90 Days (Automated) .....	55
1.16 Ensure Essential Contacts is Configured for Organization (Automated) .....	58
1.17 Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager (Manual) .....	61
<b>2 Logging and Monitoring .....</b>	<b>66</b>
2.1 Ensure That Cloud Audit Logging Is Configured Properly (Automated) .....	67
2.2 Ensure That Sinks Are Configured for All Log Entries (Automated) .....	71
2.3 Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket Lock (Automated) .....	74
2.4 Ensure Log Metric Filter and Alerts Exist for Project Ownership Assignments/Changes (Automated) .....	77
2.5 Ensure That the Log Metric Filter and Alerts Exist for Audit Configuration Changes (Automated) .....	82
2.6 Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes (Automated) .....	86
2.7 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes (Automated) .....	90
2.8 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes (Automated) .....	94
2.9 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes (Automated) .....	98
2.10 Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes (Automated) .....	102
2.11 Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes (Automated) .....	106
2.12 Ensure That Cloud DNS Logging Is Enabled for All VPC Networks (Automated) .....	110
2.13 Ensure Cloud Asset Inventory Is Enabled (Automated) .....	113
2.14 Ensure 'Access Transparency' is 'Enabled' (Manual) .....	116
2.15 Ensure 'Access Approval' is 'Enabled' (Automated) .....	119
2.16 Ensure Logging is enabled for HTTP(S) Load Balancer (Automated) .....	123
<b>3 Networking .....</b>	<b>125</b>
3.1 Ensure That the Default Network Does Not Exist in a Project (Automated) .....	126
3.2 Ensure Legacy Networks Do Not Exist for Older Projects (Automated) .....	129
3.3 Ensure That DNSSEC Is Enabled for Cloud DNS (Automated) .....	131
3.4 Ensure That RSASHA1 Is Not Used for the Key-Signing Key in Cloud DNS DNSSEC (Automated) .....	133
3.5 Ensure That RSASHA1 Is Not Used for the Zone-Signing Key in Cloud DNS DNSSEC (Automated) .....	135
3.6 Ensure That SSH Access Is Restricted From the Internet (Automated) .....	137
3.7 Ensure That RDP Access Is Restricted From the Internet (Automated) .....	140
3.8 Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network (Automated) .....	143
3.9 Ensure No HTTPS or SSL Proxy Load Balancers Permit SSL Policies With Weak Cipher Suites (Manual) .....	147

3.10 Use Identity Aware Proxy (IAP) to Ensure Only Traffic From Google IP Addresses are 'Allowed' (Manual) .....	151
<b>4 Virtual Machines .....</b>	<b>154</b>
4.1 Ensure That Instances Are Not Configured To Use the Default Service Account (Automated) .....	155
4.2 Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs (Automated) .....	158
4.3 Ensure "Block Project-Wide SSH Keys" Is Enabled for VM Instances (Automated) .....	161
4.4 Ensure Oslogin Is Enabled for a Project (Automated) .....	164
4.5 Ensure 'Enable Connecting to Serial Ports' Is Not Enabled for VM Instance (Automated) .....	167
4.6 Ensure That IP Forwarding Is Not Enabled on Instances (Automated) .....	170
4.7 Ensure VM Disks for Critical VMs Are Encrypted With Customer-Supplied Encryption Keys (CSEK) (Automated) .....	173
4.8 Ensure Compute Instances Are Launched With Shielded VM Enabled (Automated) .....	176
4.9 Ensure That Compute Instances Do Not Have Public IP Addresses (Automated) .....	179
4.10 Ensure That App Engine Applications Enforce HTTPS Connections (Manual) .....	183
4.11 Ensure That Compute Instances Have Confidential Computing Enabled (Automated) .....	185
4.12 Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects (Manual) .....	188
<b>5 Storage .....</b>	<b>195</b>
5.1 Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible (Automated) .....	196
5.2 Ensure That Cloud Storage Buckets Have Uniform Bucket-Level Access Enabled (Automated) .....	199
<b>6 Cloud SQL Database Services .....</b>	<b>202</b>
<b>6.1 MySQL Database .....</b>	<b>203</b>
6.1.1 Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges (Manual) .....	204
6.1.2 Ensure 'Skip_show_database' Database Flag for Cloud SQL MySQL Instance Is Set to 'On' (Automated) .....	207
6.1.3 Ensure That the 'Local_infile' Database Flag for a Cloud SQL MySQL Instance Is Set to 'Off' (Automated) .....	210
<b>6.2 PostgreSQL Database .....</b>	<b>213</b>
6.2.1 Ensure 'Log_error_verbosity' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'DEFAULT' or Stricter (Automated) .....	214
6.2.2 Ensure That the 'Log_connections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On' (Automated) .....	217
6.2.3 Ensure That the 'Log_disconnections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On' (Automated) .....	220
6.2.4 Ensure 'Log_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set Appropriately (Automated) .....	223
6.2.5 Ensure that the 'Log_min_messages' Flag for a Cloud SQL PostgreSQL Instance is set at minimum to 'Warning' (Automated) .....	226
6.2.6 Ensure 'Log_min_error_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Error' or Stricter (Automated) .....	229
6.2.7 Ensure That the 'Log_min_duration_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to '-1' (Disabled) (Automated) .....	232
6.2.8 Ensure That 'cloudsql.enable_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging (Automated) .....	235
<b>6.3 SQL Server .....</b>	<b>240</b>
6.3.1 Ensure 'external scripts enabled' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated) .....	241

6.3.2 Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated) .....	244
6.3.3 Ensure 'user Connections' Database Flag for Cloud Sql Sql Server Instance Is Set to a Non-limiting Value (Automated) .....	247
6.3.4 Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured (Automated) .....	250
6.3.5 Ensure 'remote access' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated) .....	253
6.3.6 Ensure '3625 (trace flag)' database flag for all Cloud SQL Server instances is set to 'on' (Automated) .....	256
6.3.7 Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is not set to 'on' (Automated) .....	259
6.4 Ensure That the Cloud SQL Database Instance Requires All Incoming Connections To Use SSL (Automated) .....	262
6.5 Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses (Automated) .....	264
6.6 Ensure That Cloud SQL Database Instances Do Not Have Public IPs (Automated) .....	267
6.7 Ensure That Cloud SQL Database Instances Are Configured With Automated Backups (Automated) .....	270
<b>7 BigQuery .....</b>	<b>273</b>
7.1 Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible (Automated) .....	274
7.2 Ensure That All BigQuery Tables Are Encrypted With Customer-Managed Encryption Key (CMEK) (Automated) .....	276
7.3 Ensure That a Default Customer-Managed Encryption Key (CMEK) Is Specified for All BigQuery Data Sets (Automated) .....	278
7.4 Ensure all data in BigQuery has been classified (Manual) .....	280
<b>8 Dataproc .....</b>	<b>282</b>
8.1 Ensure that Dataproc Cluster is encrypted using Customer-Managed Encryption Key (Automated) .....	283
<b>Appendix: Summary Table .....</b>	<b>287</b>
<b>Appendix: CIS Controls v7 IG 1 Mapped Recommendations .....</b>	<b>295</b>
<b>Appendix: CIS Controls v7 IG 2 Mapped Recommendations .....</b>	<b>298</b>
<b>Appendix: CIS Controls v7 IG 3 Mapped Recommendations .....</b>	<b>302</b>
<b>Appendix: CIS Controls v7 Unmapped Recommendations .....</b>	<b>307</b>
<b>Appendix: CIS Controls v8 IG 1 Mapped Recommendations .....</b>	<b>308</b>
<b>Appendix: CIS Controls v8 IG 2 Mapped Recommendations .....</b>	<b>311</b>
<b>Appendix: CIS Controls v8 IG 3 Mapped Recommendations .....</b>	<b>316</b>
<b>Appendix: CIS Controls v8 Unmapped Recommendations .....</b>	<b>321</b>
<b>Appendix: Change History .....</b>	<b>322</b>

# Overview

All CIS Benchmarks focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This security configuration benchmark covers foundational elements of Google Cloud Platform. The recommendations detailed here are important security considerations when designing your infrastructure on Google Cloud Platform. Most of the recommendations provided with this release of the benchmark covers security considerations only at individual Project level and not at the organization level. To obtain the latest version of this guide, please visit <http://benchmarks.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at [BenchmarkInfo@cisecurity.org](mailto:BenchmarkInfo@cisecurity.org).

## Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, platform deployment, and/or DevOps personnel who plan to develop, deploy, assess, or secure solutions on Google Cloud Platform.

## Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.



## Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<i>&lt;italic font in brackets&gt;</i>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to denote the title of a book, article, or other publication.
<b>Note</b>	Additional information or caveats

# Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

## Title

Concise description for the recommendation's intended configuration.

## Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

### Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

### Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

## Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

## Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

## Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

## **Impact Statement**

Any security, functionality, or operational consequences that can result from following the recommendation.

## **Audit Procedure**

Systematic instructions for determining if the target system complies with the recommendation.

## **Remediation Procedure**

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

## **Default Value**

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

## **References**

Additional documentation relative to the recommendation.

## **CIS Critical Security Controls® (CIS Controls®)**

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

## **Additional Information**

Supplementary information that does not correspond to any other field but may be useful to the user.

## Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Items in this profile intend to:

- be practical and prudent;
- provide security focused best practice hardening of a technology; and
- limit impact to the utility of the technology beyond acceptable means.

- **Level 2**

This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is more critical than manageability and usability
- acts as defense in depth measure
- may impact the utility or performance of the technology
- may include additional licensing, cost, or addition of third party software

## Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

### **Contributor**

Parag Patil  
Shobha H D  
Pravin Goyal  
Aditi Sahasrabudhe  
Mike Wicks  
Jacqueline Kenny  
Colin Estep  
Iulia Ion  
Anmol Baansal  
Robin Drake  
Nathael Leblanc  
Geoff Uyleman  
Jeremy Phillips  
David Lu  
Bhushan Bhat  
Prateek Khatri  
Nandhini C  
Viktor Gazdag  
Jacek Juriewicz  
Richard Rives  
Gareth Boyes  
Antonio Fontes  
Krishna Rayavaram  
RAHUL PAREEK  
Colin Brum  
Shambhu Hegde

### **Editor**

Prabhu Angadi  
Pradeep R B  
Andrew Kiggins  
Logan McMillan  
Rachel Rice  
Zan Liffick  
Iben Rodriguez



# Recommendations

## 1 Identity and Access Management

This section covers recommendations addressing Identity and Access Management on Google Cloud Platform.

## 1.1 *Ensure that Corporate Login Credentials are Used (Manual)*

### Profile Applicability:

- Level 1

### Description:

Use corporate login credentials instead of consumer accounts, such as Gmail accounts.

### Rationale:

It is recommended fully-managed corporate Google accounts be used for increased visibility, auditing, and controlling access to Cloud Platform resources. Email accounts based outside of the user's organization, such as consumer accounts, should not be used for business purposes.

### Impact:

There will be increased overhead as maintaining accounts will now be required. For smaller organizations, this will not be an issue, but will balloon with size.

### Audit:

For each Google Cloud Platform project, list the accounts that have been granted access to that project:

#### From Google Cloud CLI

```
gcloud projects get-iam-policy PROJECT_ID
```

Also list the accounts added on each folder:

```
gcloud resource-manager folders get-iam-policy FOLDER_ID
```

And list your organization's IAM policy:

```
gcloud organizations get-iam-policy ORGANIZATION_ID
```

No email accounts outside the organization domain should be granted permissions in the IAM policies. This excludes Google-owned service accounts.

### Remediation:

Remove all consumer Google accounts from IAM policies. Follow the documentation and setup corporate login accounts.

### Prevention:

To ensure that no email addresses outside the organization can be granted IAM permissions to its Google Cloud projects, folders or organization, turn on the Organization Policy for Domain Restricted Sharing. Learn more at:

<https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains>







## Default Value:

By default, no email addresses outside the organization's domain have access to its Google Cloud deployments, but any user email account can be added to the IAM policy for Google Cloud Platform projects, folders, or organizations.

## References:

1. <https://support.google.com/work/android/answer/6371476>
2. <https://cloud.google.com/sdk/gcloud/reference/projects/get-iam-policy>
3. <https://cloud.google.com/sdk/gcloud/reference/resource-manager/folders/get-iam-policy>
4. <https://cloud.google.com/sdk/gcloud/reference/organizations/get-iam-policy>
5. <https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains>
6. <https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.6 Centralize Account Management</b> Centralize account management through a directory or identity service.			
v7	<b>16.2 Configure Centralized Point of Authentication</b> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			

## *1.2 Ensure that Multi-Factor Authentication is 'Enabled' for All Non-Service Accounts (Manual)*

### **Profile Applicability:**

- Level 1

### **Description:**

Setup multi-factor authentication for Google Cloud Platform accounts.

### **Rationale:**

Multi-factor authentication requires more than one mechanism to authenticate a user. This secures user logins from attackers exploiting stolen or weak credentials.

### **Audit:**

#### **From Google Cloud Console**

For each Google Cloud Platform project, folder, or organization:

1. Identify non-service accounts.
2. Manually verify that multi-factor authentication for each account is set.

### **Remediation:**

#### **From Google Cloud Console**

For each Google Cloud Platform project:

1. Identify non-service accounts.
2. Setup multi-factor authentication for each account.





### **Default Value:**

By default, multi-factor authentication is not set.

### **References:**

1. <https://cloud.google.com/solutions/securing-gcp-account-u2f>
2. <https://support.google.com/accounts/answer/185839>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.3 <u>Require MFA for Externally-Exposed Applications</u></b> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.			
v7	<b>16.3 <u>Require Multi-factor Authentication</u></b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

## 1.3 Ensure that Security Key Enforcement is Enabled for All Admin Accounts (Manual)

### Profile Applicability:

- Level 2

### Description:

Setup Security Key Enforcement for Google Cloud Platform admin accounts.

### Rationale:

Google Cloud Platform users with Organization Administrator roles have the highest level of privilege in the organization. These accounts should be protected with the strongest form of two-factor authentication: Security Key Enforcement. Ensure that admins use Security Keys to log in instead of weaker second factors like SMS or one-time passwords (OTP). Security Keys are actual physical keys used to access Google Organization Administrator Accounts. They send an encrypted signature rather than a code, ensuring that logins cannot be phished.

### Impact:

If an organization administrator loses access to their security key, the user could lose access to their account. For this reason, it is important to set up backup security keys.

### Audit:

1. Identify users with Organization Administrator privileges:

```
gcloud organizations get-iam-policy ORGANIZATION_ID
```

Look for members granted the role "roles/resourcemanager.organizationAdmin".

2. Manually verify that Security Key Enforcement has been enabled for each account.

### Remediation:

1. Identify users with the Organization Administrator role.
2. Setup Security Key Enforcement for each account. Learn more at: <https://cloud.google.com/security-key/>





### Default Value:

By default, Security Key Enforcement is not enabled for Organization Administrators.

## References:

1. <https://cloud.google.com/security-key/>
2. [https://gsuite.google.com/learn-more/key\\_for\\_working\\_smarter\\_faster\\_and\\_more\\_securely.html](https://gsuite.google.com/learn-more/key_for_working_smarter_faster_and_more_securely.html)

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.3 <u>Require MFA for Externally-Exposed Applications</u></b> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.			
v7	<b>16.3 <u>Require Multi-factor Authentication</u></b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

## *1.4 Ensure That There Are Only GCP-Managed Service Account Keys for Each Service Account (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

User-managed service accounts should not have user-managed keys.

### **Rationale:**

Anyone who has access to the keys will be able to access resources through the service account. GCP-managed keys are used by Cloud Platform services such as App Engine and Compute Engine. These keys cannot be downloaded. Google will keep the keys and automatically rotate them on an approximately weekly basis. User-managed keys are created, downloadable, and managed by users. They expire 10 years from creation.

For user-managed keys, the user has to take ownership of key management activities which include:

- Key storage
- Key distribution
- Key revocation
- Key rotation
- Protecting the keys from unauthorized users
- Key recovery

Even with key owner precautions, keys can be easily leaked by common development malpractices like checking keys into the source code or leaving them in the Downloads directory, or accidentally leaving them on support blogs/channels.

It is recommended to prevent user-managed service account keys.

### **Impact:**

Deleting user-managed service account keys may break communication with the applications using the corresponding keys.

### **Audit:**

#### **From Google Cloud Console**

1. Go to the IAM page in the GCP Console using <https://console.cloud.google.com/iam-admin/iam>
2. In the left navigation pane, click `Service accounts`. All service accounts and their corresponding keys are listed.

3. Click the service accounts and check if keys exist.

### From Google Cloud CLI

List All the service accounts:

```
gcloud iam service-accounts list
```

Identify user-managed service accounts which have an account EMAIL ending with iam.gserviceaccount.com

For each user-managed service account, list the keys managed by the user:

```
gcloud iam service-accounts keys list --iam-account=<Service Account> --managed-by=user
```

No keys should be listed.

### Remediation:

#### From Google Cloud Console

1. Go to the IAM page in the GCP Console using <https://console.cloud.google.com/iam-admin/iam>
2. In the left navigation pane, click Service accounts. All service accounts and their corresponding keys are listed.
3. Click the service account.
4. Click the edit and delete the keys.

### From Google Cloud CLI

To delete a user managed Service Account Key,

```
gcloud iam service-accounts keys delete --iam-account=<user-managed-service-account-EMAIL> <KEY-ID>
```

### Prevention:

You can disable service account key creation through the Disable service account key creation Organization policy by visiting <https://console.cloud.google.com/iam-admin/orgpolicies/iam-disableServiceAccountKeyCreation>. Learn more at: <https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts>

In addition, if you do not need to have service accounts in your project, you can also prevent the creation of service accounts through the Disable service account creation Organization policy: <https://console.cloud.google.com/iam-admin/orgpolicies/iam-disableServiceAccountCreation>.

### Default Value:

By default, there are no user-managed keys created for user-managed service accounts.

### References:

1. [https://cloud.google.com/iam/docs/understanding-service-accounts#managing\\_service\\_account\\_keys](https://cloud.google.com/iam/docs/understanding-service-accounts#managing_service_account_keys)

2. <https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts>

**Additional Information:**

A user-managed key cannot be created on GCP-Managed Service Accounts.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			



## 1.5 Ensure That Service Account Has No Admin Privileges (Automated)

### Profile Applicability:

- Level 1

### Description:

A service account is a special Google account that belongs to an application or a VM, instead of to an individual end-user. The application uses the service account to call the service's Google API so that users aren't directly involved. It's recommended not to use admin access for ServiceAccount.

### Rationale:

Service accounts represent service-level security of the Resources (application or a VM) which can be determined by the roles assigned to it. Enrolling ServiceAccount with Admin rights gives full access to an assigned application or a VM. A ServiceAccount Access holder can perform critical actions like delete, update change settings, etc. without user intervention. For this reason, it's recommended that service accounts not have Admin rights.

### Impact:

Removing `*Admin` or `*admin` or `Editor` or `Owner` role assignments from service accounts may break functionality that uses impacted service accounts. Required role(s) should be assigned to impacted service accounts in order to restore broken functionalities.

### Audit:

#### From Google Cloud Console

1. Go to IAM & admin/IAM using `https://console.cloud.google.com/iam-admin/iam`
2. Under the IAM Tab look for VIEW BY PRINCIPALS
3. Filter PRINCIPALS using type : Service account
4. Look for the Service Account with the nomenclature:  
`SERVICE_ACCOUNT_NAME@PROJECT_ID.iam.gserviceaccount.com`
5. Ensure that there are no such Service Accounts with roles containing `*Admin` or `*admin` or role matching `Editor` or role matching `Owner` under Role column.

#### From Google Cloud CLI

1. Get the policy that you want to modify, and write it to a JSON file:

```
gcloud projects get-iam-policy PROJECT_ID --format json > iam.json
```

2. The contents of the JSON file will look similar to the following. Note that `role` of `members` group associated with each `serviceaccount` does not contain `*Admin` or `*admin` or does not match `roles/editor` or does not match `roles/owner`.

This recommendation is only applicable to User-Managed user-created service accounts. These accounts have the nomenclature:

`SERVICE_ACCOUNT_NAME@PROJECT_ID.iam.gserviceaccount.com`. Note that some Google-managed, Google-created service accounts have the same naming format, and should be excluded (e.g., `appsdev-apps-dev-script-auth@system.gserviceaccount.com` which needs the Owner role).

#### Sample Json output:

```
{
  "bindings": [
    {
      "members": [
        "serviceAccount:our-project-123@appspot.gserviceaccount.com",
      ],
      "role": "roles/appengine.appAdmin"
    },
    {
      "members": [
        "user:email1@gmail.com"
      ],
      "role": "roles/owner"
    },
    {
      "members": [
        "serviceAccount:our-project-123@appspot.gserviceaccount.com",
        "serviceAccount:123456789012-compute@developer.gserviceaccount.com"
      ],
      "role": "roles/editor"
    }
  ],
  "etag": "BwUjMhCsNvY=",
  "version": 1
}
```

#### Remediation:

##### From Google Cloud Console

1. Go to IAM & admin/IAM using <https://console.cloud.google.com/iam-admin/iam>
2. Under the IAM Tab look for VIEW BY PRINCIPALS
3. Filter PRINCIPALS using type : Service account
4. Look for the Service Account with the Principal nomenclature: `SERVICE_ACCOUNT_NAME@PROJECT_ID.iam.gserviceaccount.com`
5. Identify User-Managed user created service account with roles containing `*Admin` or `*admin` or role matching `Editor` or role matching `Owner` under Role Column.
6. Click on Edit (Pencil Icon) for the Service Account, it will open all the roles which are assigned to the Service Account.

7. Click the `Delete` bin icon to remove the role from the Principal (service account in this case)

### From Google Cloud CLI

```
gcloud projects get-iam-policy PROJECT_ID --format json > iam.json
```

1. Using a text editor, Remove Role which contains `roles/*Admin` or `roles/*admin` or matched `roles/editor` or matches `'roles/owner'`. Add a role to the bindings array that defines the group members and the role for those members.

For example, to grant the role `roles/appengine.appViewer` to the `ServiceAccount` which is `roles/editor`, you would change the example shown below as follows:

```
{
  "bindings": [
    {
      "members": [
        "serviceAccount:our-project-123@appspot.gserviceaccount.com",
      ],
      "role": "roles/appengine.appViewer"
    },
    {
      "members": [
        "user:email1@gmail.com"
      ],
      "role": "roles/owner"
    },
    {
      "members": [
        "serviceAccount:our-project-123@appspot.gserviceaccount.com",
        "serviceAccount:123456789012-compute@developer.gserviceaccount.com"
      ],
      "role": "roles/editor"
    }
  ],
  "etag": "BwUjMhCsNvY="
}
```

2. Update the project's IAM policy:

```
gcloud projects set-iam-policy PROJECT_ID iam.json
```

### Default Value:

User Managed (and not user-created) default service accounts have the `Editor` (`roles/editor`) role assigned to them to support GCP services they offer.

By default, there are no roles assigned to User Managed User created service accounts.







## References:

1. <https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/>
2. <https://cloud.google.com/iam/docs/understanding-roles>
3. <https://cloud.google.com/iam/docs/understanding-service-accounts>

## Additional Information:

Default (user-managed but not user-created) service accounts have the `Editor` (`roles/editor`) role assigned to them to support GCP services they offer. Such Service accounts are: `PROJECT_NUMBER-compute@developer.gserviceaccount.com`, `PROJECT_ID@appspot.gserviceaccount.com`.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	<b><u>4.3 Ensure the Use of Dedicated Administrative Accounts</u></b> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

## *1.6 Ensure That IAM Users Are Not Assigned the Service Account User or Service Account Token Creator Roles at Project Level (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

It is recommended to assign the `Service Account User` (`iam.serviceAccountUser`) and `Service Account Token Creator` (`iam.serviceAccountTokenCreator`) roles to a user for a specific service account rather than assigning the role to a user at project level.

### **Rationale:**

A service account is a special Google account that belongs to an application or a virtual machine (VM), instead of to an individual end-user. Application/VM-Instance uses the service account to call the service's Google API so that users aren't directly involved. In addition to being an identity, a service account is a resource that has IAM policies attached to it. These policies determine who can use the service account.

Users with IAM roles to update the App Engine and Compute Engine instances (such as App Engine Deployer or Compute Instance Admin) can effectively run code as the service accounts used to run these instances, and indirectly gain access to all the resources for which the service accounts have access. Similarly, SSH access to a Compute Engine instance may also provide the ability to execute code as that instance/Service account.

Based on business needs, there could be multiple user-managed service accounts configured for a project. Granting the `iam.serviceAccountUser` or `iam.serviceAccountTokenCreator` roles to a user for a project gives the user access to all service accounts in the project, including service accounts that may be created in the future. This can result in elevation of privileges by using service accounts and corresponding Compute Engine instances.

In order to implement `least privileges` best practices, IAM users should not be assigned the `Service Account User` or `Service Account Token Creator` roles at the project level. Instead, these roles should be assigned to a user for a specific service account, giving that user access to the service account. The `Service Account User` allows a user to bind a service account to a long-running job service, whereas the `Service Account Token Creator` role allows a user to directly impersonate (or assert) the identity of a service account.

## Impact:

After revoking `Service Account User` or `Service Account Token Creator` roles at the project level from all impacted user account(s), these roles should be assigned to a user(s) for specific service account(s) according to business needs.

## Audit:

### From Google Cloud Console

1. Go to the IAM page in the GCP Console by visiting <https://console.cloud.google.com/iam-admin/iam>
2. Click on the filter table text bar, Type `Role: Service Account User`.
3. Ensure no user is listed as a result of the filter.
4. Click on the filter table text bar, Type `Role: Service Account Token Creator`.
5. Ensure no user is listed as a result of the filter.

### From Google Cloud CLI

To ensure IAM users are not assigned `Service Account User` role at the project level:

```
gcloud projects get-iam-policy PROJECT_ID --format json | jq
'.bindings[].role' | grep "roles/iam.serviceAccountUser"

gcloud projects get-iam-policy PROJECT_ID --format json | jq
'.bindings[].role' | grep "roles/iam.serviceAccountTokenCreator"
```

These commands should not return any output.

## Remediation:

### From Google Cloud Console

1. Go to the IAM page in the GCP Console by visiting: <https://console.cloud.google.com/iam-admin/iam>.
2. Click on the filter table text bar. Type `Role: Service Account User`
3. Click the `Delete Bin` icon in front of the role `Service Account User` for every user listed as a result of a filter.
4. Click on the filter table text bar. Type `Role: Service Account Token Creator`
5. Click the `Delete Bin` icon in front of the role `Service Account Token Creator` for every user listed as a result of a filter.

### From Google Cloud CLI

1. Using a text editor, remove the bindings with the `roles/iam.serviceAccountUser` or `roles/iam.serviceAccountTokenCreator`.

For example, you can use the `iam.json` file shown below as follows:

```
{
  "bindings": [
    {
      "members": [
        "serviceAccount:our-project-123@appspot.gserviceaccount.com",
      ],
      "role": "roles/appengine.appViewer"
    },
    {
      "members": [
        "user:email1@gmail.com"
      ],
      "role": "roles/owner"
    },
    {
      "members": [
        "serviceAccount:our-project-123@appspot.gserviceaccount.com",
        "serviceAccount:123456789012-compute@developer.gserviceaccount.com"
      ],
      "role": "roles/editor"
    }
  ],
  "etag": "BwUjMhCsNvY="
}
```

## 2. Update the project's IAM policy:

```
gcloud projects set-iam-policy PROJECT_ID iam.json
```

### Default Value:

By default, users do not have the Service Account User or Service Account Token Creator role assigned at project level.

### References:

1. <https://cloud.google.com/iam/docs/service-accounts>
2. <https://cloud.google.com/iam/docs/granting-roles-to-service-accounts>
3. <https://cloud.google.com/iam/docs/understanding-roles>
4. <https://cloud.google.com/iam/docs/granting-changing-revoking-access>
5. <https://console.cloud.google.com/iam-admin/iam>







### Additional Information:

To assign the role `roles/iam.serviceAccountUser` or `roles/iam.serviceAccountTokenCreator` to a user role on a service account instead of a project:

1. Go to <https://console.cloud.google.com/projectselector/iam-admin/serviceaccounts>
2. Select Target Project

3. Select `target service account`. Click `Permissions` on the top bar. It will open permission pane on right side of the page
4. Add desired members with `Service Account User` or `Service Account Token Creator` role.

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			



## *1.7 Ensure User-Managed/External Keys for Service Accounts Are Rotated Every 90 Days or Fewer (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

Service Account keys consist of a key ID (`Private_key_Id`) and Private key, which are used to sign programmatic requests users make to Google cloud services accessible to that particular service account. It is recommended that all Service Account keys are regularly rotated.

### **Rationale:**

Rotating Service Account keys will reduce the window of opportunity for an access key that is associated with a compromised or terminated account to be used. Service Account keys should be rotated to ensure that data cannot be accessed with an old key that might have been lost, cracked, or stolen.

Each service account is associated with a key pair managed by Google Cloud Platform (GCP). It is used for service-to-service authentication within GCP. Google rotates the keys daily.

GCP provides the option to create one or more user-managed (also called external key pairs) key pairs for use from outside GCP (for example, for use with Application Default Credentials). When a new key pair is created, the user is required to download the private key (which is not retained by Google). With external keys, users are responsible for keeping the private key secure and other management operations such as key rotation. External keys can be managed by the IAM API, `gcloud` command-line tool, or the Service Accounts page in the Google Cloud Platform Console. GCP facilitates up to 10 external service account keys per service account to facilitate key rotation.

### **Impact:**

Rotating service account keys will break communication for dependent applications. Dependent applications need to be configured manually with the new key ID displayed in the `Service account keys` section and the private key downloaded by the user.

### **Audit:**

#### **From Google Cloud Console**

1. Go to `APIs & Services\Credentials` using <https://console.cloud.google.com/apis/credentials>
2. In the section `Service Account Keys`, for every External (user-managed) service account key listed ensure the `creation date` is within the past 90 days.

## From Google Cloud CLI

1. List all Service accounts from a project.

```
gcloud iam service-accounts list
```

2. For every service account list service account keys.

```
gcloud iam service-accounts keys list --iam-account  
[Service_Account_Email_Id] --format=json
```

3. Ensure every service account key for a service account has a "validAfterTime" value within the past 90 days.

## Remediation:

### From Google Cloud Console

#### Delete any external (user-managed) Service Account Key older than 90 days:

1. Go to APIs & Services\Credentials using <https://console.cloud.google.com/apis/credentials>
2. In the Section Service Account Keys, for every external (user-managed) service account key where creation date is greater than or equal to the past 90 days, click Delete Bin Icon to Delete Service Account key

#### Create a new external (user-managed) Service Account Key for a Service Account:

1. Go to APIs & Services\Credentials using <https://console.cloud.google.com/apis/credentials>
2. Click Create Credentials and Select Service Account Key.
3. Choose the service account in the drop-down list for which an External (user-managed) Service Account key needs to be created.
4. Select the desired key type format among JSON or P12.
5. Click Create. It will download the private key. Keep it safe.
6. Click Close if prompted.
7. The site will redirect to the APIs & Services\Credentials page. Make a note of the new ID displayed in the Service account keys section.

## Default Value:

GCP does not provide an automation option for External (user-managed) Service key rotation.

## References:

1. [https://cloud.google.com/iam/docs/understanding-service-accounts#managing\\_service\\_account\\_keys](https://cloud.google.com/iam/docs/understanding-service-accounts#managing_service_account_keys)
2. <https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/keys/list>
3. <https://cloud.google.com/iam/docs/service-accounts>

## Additional Information:

For user-managed Service Account key(s), key management is entirely the user's responsibility.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

## *1.8 Ensure That Separation of Duties Is Enforced While Assigning Service Account Related Roles to Users (Automated)*

### **Profile Applicability:**

- Level 2

### **Description:**

It is recommended that the principle of 'Separation of Duties' is enforced while assigning service-account related roles to users.

### **Rationale:**

The built-in/predefined IAM role `Service Account admin` allows the user/identity to create, delete, and manage service account(s). The built-in/predefined IAM role `Service Account User` allows the user/identity (with adequate privileges on Compute and App Engine) to assign service account(s) to Apps/Compute Instances.

Separation of duties is the concept of ensuring that one individual does not have all necessary permissions to be able to complete a malicious action. In Cloud IAM - service accounts, this could be an action such as using a service account to access resources that user should not normally have access to.

Separation of duties is a business control typically used in larger organizations, meant to help avoid security or privacy incidents and errors. It is considered best practice.

No user should have `Service Account Admin` and `Service Account User` roles assigned at the same time.

### **Impact:**

The removed role should be assigned to a different user based on business needs.

### **Audit:**

#### **From Google Cloud Console**

1. Go to IAM & Admin/IAM using `https://console.cloud.google.com/iam-admin/iam`.
2. Ensure no member has the roles `Service Account Admin` and `Service account User` assigned together.

#### **From Google Cloud CLI**

1. List all users and role assignments:

```
gcloud projects get-iam-policy [Project_ID] --format json | \
jq -r '[
  ([ "Service_Account_Admin_and_User" ] | (., map(length*"-"))),
  (
    [
      .bindings[] |
      select(.role == "roles/iam.serviceAccountAdmin" or .role ==
"roles/iam.serviceAccountUser").members[]
    ] |
    group_by(.) |
    map({User: ., Count: length}) |
    .[] |
    select(.Count == 2).User |
    unique
  )
] |
.[0] |
@tsv'
```

2. All common users listed under `Service_Account_Admin_and_User` are assigned both the `roles/iam.serviceAccountAdmin` and `roles/iam.serviceAccountUser` roles.

## Remediation:

### From Google Cloud Console

1. Go to IAM & Admin/IAM using <https://console.cloud.google.com/iam-admin/iam>.
2. For any member having both `Service Account Admin` and `Service account User` roles granted/assigned, click the `Delete Bin` icon to remove either role from the member.  
Removal of a role should be done based on the business requirements.







## References:

1. <https://cloud.google.com/iam/docs/service-accounts>
2. <https://cloud.google.com/iam/docs/understanding-roles>
3. <https://cloud.google.com/iam/docs/granting-roles-to-service-accounts>

## Additional Information:

Users granted with Owner (`roles/owner`) and Editor (`roles/editor`) have privileges equivalent to `Service Account Admin` and `Service Account User`. To avoid the misuse, Owner and Editor roles should be granted to very limited users and Use of these primitive privileges should be minimal. These requirements are addressed in separate recommendations.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

## 1.9 Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible (Automated)

### Profile Applicability:

- Level 1

### Description:

It is recommended that the IAM policy on Cloud KMS `cryptokeys` should restrict anonymous and/or public access.

### Rationale:

Granting permissions to `allUsers` or `allAuthenticatedUsers` allows anyone to access the dataset. Such access might not be desirable if sensitive data is stored at the location. In this case, ensure that anonymous and/or public access to a Cloud KMS `cryptokey` is not allowed.

### Impact:

Removing the binding for `allUsers` and `allAuthenticatedUsers` members denies accessing `cryptokeys` to anonymous or public users.

### Audit:

#### From Google Cloud CLI

1. List all Cloud KMS `Cryptokeys`.

```
gcloud kms keys list --keyring=[key_ring_name] --location=global --format=json | jq '[][.name]'
```

2. Ensure the below command's output does not contain `allUsers` or `allAuthenticatedUsers`.

```
gcloud kms keys get-iam-policy [key_name] --keyring=[key_ring_name] --location=global --format=json | jq '.bindings[].members[]'
```

### Remediation:

#### From Google Cloud CLI

1. List all Cloud KMS `Cryptokeys`.

```
gcloud kms keys list --keyring=[key_ring_name] --location=global --format=json | jq '[][.name]'
```

2. Remove IAM policy binding for a KMS key to remove access to `allUsers` and `allAuthenticatedUsers` using the below command.

```
gcloud kms keys remove-iam-policy-binding [key_name] --  
keyring=[key_ring_name] --location=global --member='allAuthenticatedUsers' --  
role='[role]'
```

```
gcloud kms keys remove-iam-policy-binding [key_name] --  
keyring=[key_ring_name] --location=global --member='allUsers' --role='[role]'
```

### Default Value:

By default Cloud KMS does not allow access to `allUsers` or `allAuthenticatedUsers`.

### References:

1. <https://cloud.google.com/sdk/gcloud/reference/kms/keys/remove-iam-policy-binding>
2. <https://cloud.google.com/sdk/gcloud/reference/kms/keys/set-iam-policy>
3. <https://cloud.google.com/sdk/gcloud/reference/kms/keys/get-iam-policy>
4. [https://cloud.google.com/kms/docs/object-hierarchy#key\\_resource\\_id](https://cloud.google.com/kms/docs/object-hierarchy#key_resource_id)

### Additional Information:

[key\_ring\_name] : Is the resource ID of the key ring, which is the fully-qualified Key ring name. This value is case-sensitive and in the form:  
projects/PROJECT\_ID/locations/LOCATION/keyRings/KEY\_RING

You can retrieve the key ring resource ID using the Cloud Console:

1. Open the `Cryptographic Keys` page in the Cloud Console.
2. For the key ring whose resource ID you are retrieving, click the `More icon` (3 vertical dots).
3. Click `Copy Resource ID`. The resource ID for the key ring is copied to your clipboard.

[key\_name] : Is the resource ID of the key, which is the fully-qualified `CryptoKey` name. This value is case-sensitive and in the form:  
projects/PROJECT\_ID/locations/LOCATION/keyRings/KEY\_RING/cryptoKeys/KEY







You can retrieve the key resource ID using the Cloud Console:

1. Open the `Cryptographic Keys` page in the Cloud Console.
2. Click the name of the key ring that contains the key.
3. For the key whose resource ID you are retrieving, click the `More icon` (3 vertical dots).
4. Click `Copy Resource ID`. The resource ID for the key is copied to your clipboard.

[role] : The role to remove the member from.



## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

## 1.10 Ensure KMS Encryption Keys Are Rotated Within a Period of 90 Days (Automated)

### Profile Applicability:

- Level 1

### Description:

Google Cloud Key Management Service stores cryptographic keys in a hierarchical structure designed for useful and elegant access control management.

The format for the rotation schedule depends on the client library that is used. For the `gcloud` command-line tool, the next rotation time must be in `ISO` or `RFC3339` format, and the rotation period must be in the form `INTEGER[UNIT]`, where units can be one of seconds (s), minutes (m), hours (h) or days (d).

### Rationale:

Set a key rotation period and starting time. A key can be created with a specified `rotation period`, which is the time between when new key versions are generated automatically. A key can also be created with a specified next rotation time. A key is a named object representing a `cryptographic key` used for a specific purpose. The key material, the actual bits used for `encryption`, can change over time as new key versions are created.

A key is used to protect some `corpus of data`. A collection of files could be encrypted with the same key and people with `decrypt` permissions on that key would be able to decrypt those files. Therefore, it's necessary to make sure the `rotation period` is set to a specific time.

### Impact:

After a successful key rotation, the older key version is required in order to decrypt the data encrypted by that previous key version.

### Audit:

#### From Google Cloud Console

1. Go to `Cryptographic Keys` by visiting:  
<https://console.cloud.google.com/security/kms>.
2. Click on each key ring, then ensure each key in the keyring has `Next Rotation` set for less than 90 days from the current date.

#### From Google Cloud CLI

1. Ensure rotation is scheduled by `ROTATION_PERIOD` and `NEXT_ROTATION_TIME` for each key :

```
gcloud kms keys list --keyring=<KEY_RING> --location=<LOCATION> --  
format=json'(rotationPeriod)'
```

Ensure outcome values for `rotationPeriod` and `nextRotationTime` satisfy the below criteria:

`rotationPeriod` is `<= 129600m`

`rotationPeriod` is `<= 7776000s`

`rotationPeriod` is `<= 2160h`

`rotationPeriod` is `<= 90d`

`nextRotationTime` is `<= 90days` from current DATE

## Remediation:

### From Google Cloud Console

1. Go to Cryptographic Keys by visiting:  
<https://console.cloud.google.com/security/kms>.
2. Click on the specific key ring
3. From the list of keys, choose the specific key and Click on Right side pop up the blade (3 dots).
4. Click on Edit rotation period.
5. On the pop-up window, Select a new rotation period in days which should be less than 90 and then choose Starting on date (date from which the rotation period begins).

### From Google Cloud CLI

1. Update and schedule rotation by `ROTATION_PERIOD` and `NEXT_ROTATION_TIME` for each key:

```
gcloud kms keys update new --keyring=KEY_RING --location=LOCATION --next-  
rotation-time=NEXT_ROTATION_TIME --rotation-period=ROTATION_PERIOD
```

## Default Value:

By default, KMS encryption keys are rotated every 90 days.




## References:

1. [https://cloud.google.com/kms/docs/key-rotation#frequency\\_of\\_key\\_rotation](https://cloud.google.com/kms/docs/key-rotation#frequency_of_key_rotation)
2. <https://cloud.google.com/kms/docs/re-encrypt-data>

### Additional Information:

- Key rotation does NOT re-encrypt already encrypted data with the newly generated key version. If you suspect unauthorized use of a key, you should re-encrypt the data protected by that key and then disable or schedule destruction of the prior key version.
- It is not recommended to rely solely on irregular rotation, but rather to use irregular rotation if needed in conjunction with a regular rotation schedule.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	<b>14.8 <u>Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

## 1.11 Ensure That Separation of Duties Is Enforced While Assigning KMS Related Roles to Users (Automated)

### Profile Applicability:

- Level 2

### Description:

It is recommended that the principle of 'Separation of Duties' is enforced while assigning KMS related roles to users.

### Rationale:

The built-in/predefined IAM role `Cloud KMS Admin` allows the user/identity to create, delete, and manage service account(s). The built-in/predefined IAM role `Cloud KMS CryptoKey Encrypter/Decrypter` allows the user/identity (with adequate privileges on concerned resources) to encrypt and decrypt data at rest using an encryption key(s).

The built-in/predefined IAM role `Cloud KMS CryptoKey Encrypter` allows the user/identity (with adequate privileges on concerned resources) to encrypt data at rest using an encryption key(s). The built-in/predefined IAM role `Cloud KMS CryptoKey Decrypter` allows the user/identity (with adequate privileges on concerned resources) to decrypt data at rest using an encryption key(s).

Separation of duties is the concept of ensuring that one individual does not have all necessary permissions to be able to complete a malicious action. In Cloud KMS, this could be an action such as using a key to access and decrypt data a user should not normally have access to. Separation of duties is a business control typically used in larger organizations, meant to help avoid security or privacy incidents and errors. It is considered best practice.

No user(s) should have `Cloud KMS Admin` and any of the `Cloud KMS CryptoKey Encrypter/Decrypter`, `Cloud KMS CryptoKey Encrypter`, `Cloud KMS CryptoKey Decrypter` roles assigned at the same time.

### Impact:

Removed roles should be assigned to another user based on business needs.

### Audit:

#### From Google Cloud Console

1. Go to IAM & Admin/IAM by visiting: <https://console.cloud.google.com/iam-admin/iam>
2. Ensure no member has the roles `Cloud KMS Admin` and any of the `Cloud KMS CryptoKey Encrypter/Decrypter`, `Cloud KMS CryptoKey Encrypter`, `Cloud KMS CryptoKey Decrypter` assigned.

## From Google Cloud CLI

1. List all users and role assignments:

```
gcloud projects get-iam-policy PROJECT_ID
```

2. Ensure that there are no common users found in the member section for roles `cloudkms.admin` and any one of `Cloud KMS CryptoKey Encrypter/Decrypter`, `Cloud KMS CryptoKey Encrypter`, `Cloud KMS CryptoKey Decrypter`

## Remediation:

### From Google Cloud Console

1. Go to IAM & Admin/IAM using <https://console.cloud.google.com/iam-admin/iam>
2. For any member having `Cloud KMS Admin` and any of the `Cloud KMS CryptoKey Encrypter/Decrypter`, `Cloud KMS CryptoKey Encrypter`, `Cloud KMS CryptoKey Decrypter` roles granted/assigned, click the `Delete Bin` icon to remove the role from the member.

Note: Removing a role should be done based on the business requirement.




## References:




1. <https://cloud.google.com/kms/docs/separation-of-duties>

## Additional Information:

Users granted with Owner (roles/owner) and Editor (roles/editor) have privileges equivalent to `Cloud KMS Admin` and `Cloud KMS CryptoKey Encrypter/Decrypter`. To avoid misuse, Owner and Editor roles should be granted to a very limited group of users. Use of these primitive privileges should be minimal.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><b>14.6 <u>Protect Information through Access Control Lists</u></b></p> <p>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.</p>			

## 1.12 Ensure API Keys Only Exist for Active Services (Automated)

### Profile Applicability:

- Level 2

### Description:

API Keys should only be used for services in cases where other authentication methods are unavailable. Unused keys with their permissions in tact may still exist within a project. Keys are insecure because they can be viewed publicly, such as from within a browser, or they can be accessed on a device where the key resides. It is recommended to use standard authentication flow instead.

### Rationale:

To avoid the security risk in using API keys, it is recommended to use standard authentication flow instead. Security risks involved in using API-Keys appear below:

- API keys are simple encrypted strings
- API keys do not identify the user or the application making the API request
- API keys are typically accessible to clients, making it easy to discover and steal an API key

### Impact:

Deleting an API key will break dependent applications (if any).

### Audit:

#### From Console:

1. From within the Project you wish to audit Go to `APIs & Services\Credentials`.
2. In the section `API Keys`, no API key should be listed.

#### From Google Cloud Command Line

1. Run the following from within the project you wish to audit `gcloud services api-keys list --filter`.
2. There should be no keys listed at the project level.

### Remediation:

#### From Console:

1. Go to `APIs & Services\Credentials` using
2. In the section `API Keys`, to delete API Keys: Click the `Delete Bin Icon` in front of every API Key Name.



## From Google Cloud Command Line

1. Run the following from within the project you wish to audit `gcloud services api-keys list --filter`
2. **\*\*Pipe the results into \*\***  
`gcloud alpha services api-keys delete`

### Default Value:

By default, API keys are not created for a project.

### References:






1. <https://cloud.google.com/docs/authentication/api-keys>
2. <https://cloud.google.com/sdk/gcloud/reference/services/api-keys/list>
3. <https://cloud.google.com/docs/authentication>
4. <https://cloud.google.com/sdk/gcloud/reference/alpha/services/api-keys/delete>

### Additional Information:

Google recommends using the standard authentication flow instead of using API keys. However, there are limited cases where API keys are more appropriate. For example, if there is a mobile application that needs to use the Google Cloud Translation API, but doesn't otherwise need a backend server, API keys are the simplest way to authenticate to that API.

If a business requires API keys to be used, then the API keys should be secured properly.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>16.10 Apply Secure Design Principles in Application Architectures</u></b> Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.			
v7	<b><u>16.8 Disable Any Unassociated Accounts</u></b> Disable any account that cannot be associated with a business process or business owner.			

## 1.13 Ensure API Keys Are Restricted To Use by Only Specified Hosts and Apps (Manual)

### Profile Applicability:

- Level 2

### Description:

API Keys should only be used for services in cases where other authentication methods are unavailable. In this case, unrestricted keys are insecure because they can be viewed publicly, such as from within a browser, or they can be accessed on a device where the key resides. It is recommended to restrict API key usage to trusted hosts, HTTP referrers and apps. It is recommended to use the more secure standard authentication flow instead.

### Rationale:

Security risks involved in using API-Keys appear below:

- API keys are simple encrypted strings
- API keys do not identify the user or the application making the API request
- API keys are typically accessible to clients, making it easy to discover and steal an API key

In light of these potential risks, Google recommends using the standard authentication flow instead of API keys. However, there are limited cases where API keys are more appropriate. For example, if there is a mobile application that needs to use the Google Cloud Translation API, but doesn't otherwise need a backend server, API keys are the simplest way to authenticate to that API.

In order to reduce attack vectors, API-Keys can be restricted only to trusted hosts, HTTP referrers and applications.

### Impact:

Setting `Application Restrictions` may break existing application functioning, if not done carefully.

### Audit:

#### From Google Cloud Console

1. Go to `APIs & Services\Credentials` using <https://console.cloud.google.com/apis/credentials>
2. In the section `API Keys`, Click the `API Key Name`. The API Key properties display on a new page.

3. For every API Key, ensure the section `Key restrictions` parameter `Application restrictions` is not set to `None`.

Or,

1. Ensure `Application restrictions` is set to `HTTP referrers` and the referrer is not set to wild-cards (`*` or `*.[TLD]` or `*.[TLD]/*`) allowing access to any/wide HTTP referrer(s)

Or,

1. Ensure `Application restrictions` is set to `IP addresses` and referrer is not set to any host (`0.0.0.0` or `0.0.0.0/0` or `::0`)

## From Google Cloud Command Line

1. Run the following from within the project you wish to audit

```
gcloud services api-keys list --filter="-restrictions:*" --format="table[box] (displayName:label='Key With No Restrictions')
```

## Remediation:

### From Google Cloud Console *Leaving Keys in Place*

1. Go to `APIs & Services\Credentials` using <https://console.cloud.google.com/apis/credentials>
2. In the section `API Keys`, Click the `API Key Name`. The `API Key` properties display on a new page.
3. In the `Key restrictions` section, set the application restrictions to any of `HTTP referrers`, `IP addresses`, `Android apps`, `iOS apps`.
4. Click `Save`.
5. Repeat steps 2,3,4 for every unrestricted API key.  
**Note:** Do not set `HTTP referrers` to wild-cards (`*` or `*.[TLD]` or `.[TLD]/`) allowing access to any/wide HTTP referrer(s)  
Do not set `IP addresses` and referrer to any host (`0.0.0.0` or `0.0.0.0/0` or `::0`)

### *Removing Keys*

Another option is to remove the keys entirely.

1. Go to `APIs & Services\Credentials` using <https://console.cloud.google.com/apis/credentials>
2. In the section `API Keys`, select the checkbox next to each key you wish to remove
3. Select `Delete` and confirm.



## Default Value:

By default, Application Restrictions are set to None.

## References:

1. <https://cloud.google.com/docs/authentication/api-keys>
2. <https://cloud.google.com/sdk/gcloud/reference/services/api-keys/list>
3. <https://cloud.google.com/sdk/gcloud/reference/alpha/services/api-keys/update>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>16.10 Apply Secure Design Principles in Application Architectures</b> Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.			
v7	<b>0.0 Explicitly Not Mapped</b> Explicitly Not Mapped			

## 1.14 Ensure API Keys Are Restricted to Only APIs That Application Needs Access (Automated)

### Profile Applicability:

- Level 2

### Description:

API Keys should only be used for services in cases where other authentication methods are unavailable. API keys are always at risk because they can be viewed publicly, such as from within a browser, or they can be accessed on a device where the key resides. It is recommended to restrict API keys to use (call) only APIs required by an application.

### Rationale:

Security risks involved in using API-Keys are below:

- API keys are simple encrypted strings
- API keys do not identify the user or the application making the API request
- API keys are typically accessible to clients, making it easy to discover and steal an API key

In light of these potential risks, Google recommends using the standard authentication flow instead of API-Keys. However, there are limited cases where API keys are more appropriate. For example, if there is a mobile application that needs to use the Google Cloud Translation API, but doesn't otherwise need a backend server, API keys are the simplest way to authenticate to that API.

In order to reduce attack surfaces by providing `least privileges`, API-Keys can be restricted to use (call) only APIs required by an application.

### Impact:

Setting `API restrictions` may break existing application functioning, if not done carefully.

### Audit:

#### From Console:

1. Go to `APIs & Services\Credentials` using `https://console.cloud.google.com/apis/credentials`
2. In the section `API Keys`, Click the `API Key Name`. The API Key properties display on a new page.
3. For every API Key, ensure the section `Key restrictions` parameter `API restrictions` is not set to `None`.

Or,

Ensure API restrictions is not set to Google Cloud APIs

**Note:** Google Cloud APIs represents the API collection of all cloud services/APIs offered by Google cloud.

**From Google Cloud CLI**

1. List all API Keys.

```
gcloud services api-keys list
```

Each key should have a line that says `restrictions:` followed by varying parameters and NOT have a line saying `- service: cloudapis.googleapis.com` as shown here

```
restrictions:
apiTargets:
- service: cloudapis.googleapis.com
```

**Remediation:**

**From Console:**

1. Go to APIs & Services\Credentials using <https://console.cloud.google.com/apis/credentials>
2. In the section API Keys, Click the API Key Name. The API Key properties display on a new page.
3. In the Key restrictions section go to API restrictions.
4. Click the Select API drop-down to choose an API.
5. Click Save.
6. Repeat steps 2,3,4,5 for every unrestricted API key

**Note:** Do not set API restrictions to Google Cloud APIs, as this option allows access to all services offered by Google cloud.

**From Google Cloud CLI**

1. List all API keys.

```
gcloud services api-keys list
```

2. Note the `UID` of the key to add restrictions to.
3. Run the update command with the appropriate flags to add the required restrictions.

```
gcloud alpha services api-keys update <UID> <restriction_flags>
```

Note- Flags can be found by running

```
gcloud alpha services api-keys update --help
```

or in this documentation

<https://cloud.google.com/sdk/gcloud/reference/alpha/services/api-keys/update>

## Default Value:

By default, API restrictions are set to None.



## References:

1. <https://cloud.google.com/docs/authentication/api-keys>
2. <https://cloud.google.com/apis/docs/overview>

## Additional Information:

Some of the gcloud commands listed are currently in alpha and might change without notice.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>16.10 <u>Apply Secure Design Principles in Application Architectures</u></b> Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.			
v7	<b>0.0 <u>Explicitly Not Mapped</u></b> Explicitly Not Mapped			

## 1.15 Ensure API Keys Are Rotated Every 90 Days (Automated)

### Profile Applicability:

- Level 2

### Description:

API Keys should only be used for services in cases where other authentication methods are unavailable. If they are in use it is recommended to rotate API keys every 90 days.

### Rationale:

Security risks involved in using API-Keys are listed below:

- API keys are simple encrypted strings
- API keys do not identify the user or the application making the API request
- API keys are typically accessible to clients, making it easy to discover and steal an API key

Because of these potential risks, Google recommends using the standard authentication flow instead of API Keys. However, there are limited cases where API keys are more appropriate. For example, if there is a mobile application that needs to use the Google Cloud Translation API, but doesn't otherwise need a backend server, API keys are the simplest way to authenticate to that API.

Once a key is stolen, it has no expiration, meaning it may be used indefinitely unless the project owner revokes or regenerates the key. Rotating API keys will reduce the window of opportunity for an access key that is associated with a compromised or terminated account to be used.

API keys should be rotated to ensure that data cannot be accessed with an old key that might have been lost, cracked, or stolen.

### Impact:

Regenerating Key may break existing client connectivity as the client will try to connect with older API keys they have stored on devices.

### Audit:

#### From Google Cloud Console

1. Go to APIs & Services\Credentials using <https://console.cloud.google.com/apis/credentials>
2. In the section API Keys, for every key ensure the creation date is less than 90 days.



## From Google Cloud CLI

To list keys, use the command

```
gcloud services api-keys list
```

Ensure the date in `createTime` is within 90 days.

## Remediation:

### From Google Cloud Console

1. Go to APIs & Services\Credentials using <https://console.cloud.google.com/apis/credentials>
2. In the section API Keys, Click the API Key Name. The API Key properties display on a new page.
3. Click REGENERATE KEY to rotate API key.
4. Click Save.
5. Repeat steps 2,3,4 for every API key that has not been rotated in the last 90 days.

**Note:** Do not set `HTTP referrers` to wild-cards (\* or \*.`[TLD]` or `.[TLD]/`) allowing access to any/wide HTTP referrer(s)

Do not set `IP addresses` and `referrer` to any host (`0.0.0.0` or `0.0.0.0/0` or `::0`)

## From Google Cloud CLI

There is not currently a way to regenerate and API key using `gcloud` commands. To 'regenerate' a key you will need to create a new one, duplicate the restrictions from the key being rotated, and delete the old key.

1. List existing keys.

```
gcloud services api-keys list
```

2. Note the `UID` and restrictions of the key to regenerate.
3. Run this command to create a new API key. `<key_name>` is the display name of the new key.

```
gcloud alpha services api-keys create --display-name="<key_name>"
```

Note the `UID` of the newly created key

4. Run the update command to add required restrictions.

Note - the restriction may vary for each key. Refer to this documentation for the appropriate flags.

<https://cloud.google.com/sdk/gcloud/reference/alpha/services/api-keys/update>

```
gcloud alpha services api-keys update <UID of new key>
```

5. Delete the old key.

```
gcloud alpha services api-keys delete <UID of old key>
```



## References:

1. <https://developers.google.com/maps/api-security-best-practices#regenerate-apikey>
2. <https://cloud.google.com/sdk/gcloud/reference/alpha/services/api-keys>

## Additional Information:

There is no option to automatically regenerate (rotate) API keys periodically.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>16.10 Apply Secure Design Principles in Application Architectures</b> Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.			
v7	<b>0.0 Explicitly Not Mapped</b> Explicitly Not Mapped			

## 1.16 Ensure Essential Contacts is Configured for Organization (Automated)

### Profile Applicability:

- Level 1

### Description:

It is recommended that Essential Contacts is configured to designate email addresses for Google Cloud services to notify of important technical or security information.

### Rationale:

Many Google Cloud services, such as Cloud Billing, send out notifications to share important information with Google Cloud users. By default, these notifications are sent to members with certain Identity and Access Management (IAM) roles. With Essential Contacts, you can customize who receives notifications by providing your own list of contacts.

### Impact:

There is no charge for Essential Contacts except for the 'Technical Incidents' category that is only available to premium support customers.

### Audit:

#### From Google Cloud Console

1. Go to `Essential Contacts` by visiting <https://console.cloud.google.com/iam-admin/essential-contacts>
2. Make sure the organization appears in the resource selector at the top of the page. The resource selector tells you what project, folder, or organization you are currently managing contacts for.
3. Ensure that appropriate email addresses are configured for each of the following notification categories:
  - Legal
  - Security
  - Suspension
  - Technical

Alternatively, appropriate email addresses can be configured for the `All` notification category to receive all possible important notifications.

#### From Google Cloud CLI

1. To list all configured organization Essential Contacts run a command:

```
gcloud essential-contacts list --organization=<ORGANIZATION_ID>
```

2. Ensure at least one appropriate email address is configured for each of the following notification categories:

- LEGAL
- SECURITY
- SUSPENSION
- TECHNICAL

Alternatively, appropriate email addresses can be configured for the `ALL` notification category to receive all possible important notifications.

### Remediation:

#### From Google Cloud Console

1. Go to `Essential Contacts` by visiting <https://console.cloud.google.com/iam-admin/essential-contacts>
2. Make sure the organization appears in the resource selector at the top of the page. The resource selector tells you what project, folder, or organization you are currently managing contacts for.
3. Click `+Add contact`
4. In the `Email` and `Confirm Email` fields, enter the email address of the contact.
5. From the `Notification categories` drop-down menu, select the notification categories that you want the contact to receive communications for.
6. Click `Save`

#### From Google Cloud CLI

1. To add an organization Essential Contacts run a command:

```
gcloud essential-contacts create --email="<EMAIL>" \
--notification-categories="<NOTIFICATION_CATEGORIES>" \
--organization=<ORGANIZATION_ID>
```

### Default Value:

By default, there are no Essential Contacts configured.







In the absence of an Essential Contact, the following IAM roles are used to identify users to notify for the following categories:

- **Legal:** `roles/billing.admin`
- **Security:** `roles/resourcemanager.organizationAdmin`
- **Suspension:** `roles/owner`
- **Technical:** `roles/owner`
- **Technical Incidents:** `roles/owner`

## References:

1. <https://cloud.google.com/resource-manager/docs/managing-notification-contacts>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>17.2 Establish and Maintain Contact Information for Reporting Security Incidents</u></b></p> <p>Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.</p>			
v7	<p><b><u>19.5 Maintain Contact Information For Reporting Security Incidents</u></b></p> <p>Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.</p>			

## *1.17 Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager (Manual)*

### **Profile Applicability:**

- Level 1

### **Description:**

Google Cloud Functions allow you to host serverless code that is executed when an event is triggered, without the requiring the management a host operating system. These functions can also store environment variables to be used by the code that may contain authentication or other information that needs to remain confidential.

### **Rationale:**

It is recommended to use the Secret Manager, because environment variables are stored unencrypted, and accessible for all users who have access to the code.

### **Impact:**

There should be no impact on the Cloud Function. There are minor costs after 10,000 requests a month to the Secret Manager API as well for a high use of other functions. Modifying the Cloud Function to use the Secret Manager may prevent it running to completion.

### **Audit:**

Determine if Confidential Information is Stored in your Functions in Cleartext

#### **From Google Cloud Console**

1. Within the project you wish to audit, select the Navigation hamburger menu in the top left. Scroll down to under the heading 'Serverless', then select 'Cloud Functions'
2. Click on a function name from the list
3. Open the Variables tab and you will see both buildEnvironmentVariables and environmentVariables
4. Review the variables whether they are secrets
5. Repeat step 3-5 until all functions are reviewed

#### **From Google Cloud CLI**

1. To view a list of your cloud functions run

```
gcloud functions list
```

2. For each cloud function in the list run the following command.

```
gcloud functions describe <function_name>
```

3. Review the settings of the buildEnvironmentVariables and environmentVariables. Determine if this is data that should not be publicly accessible.

Determine if Secret Manager API is 'Enabled' for your Project

#### **From Google Cloud Console**

1. Within the project you wish to audit, select the Navigation hamburger menu in the top left. Hover over 'APIs & Services' to under the heading 'Serverless', then select 'Enabled APIs & Services' in the menu that opens up.
2. Click the button '+ Enable APIs and Services'
3. In the Search bar, search for 'Secret Manager API' and select it.
4. If it is enabled, the blue box that normally says 'Enable' will instead say 'Manage'.

#### **From Google Cloud CLI**

1. Within the project you wish to audit, run the following command.

```
gcloud services list
```

2. If 'Secret Manager API' is in the list, it is enabled.

#### **Remediation:**

Enable Secret Manager API for your Project

#### **From Google Cloud Console**

1. Within the project you wish to enable, select the Navigation hamburger menu in the top left. Hover over 'APIs & Services' to under the heading 'Serverless', then select 'Enabled APIs & Services' in the menu that opens up.
2. Click the button '+ Enable APIs and Services'
3. In the Search bar, search for 'Secret Manager API' and select it.
4. Click the blue box that says 'Enable'.

#### **From Google Cloud CLI**

1. Within the project you wish to enable the API in, run the following command.

```
gcloud services enable Secret Manager API
```

Reviewing Environment Variables That Should Be Migrated to Secret Manager

#### **From Google Cloud Console**

1. Log in to the Google Cloud Web Portal (<https://console.cloud.google.com/>)
2. Go to Cloud Functions
3. Click on a function name from the list

4. Click on Edit and review the Runtime environment for variables that should be secrets. Leave this list open for the next step.

### From Google Cloud CLI

1. To view a list of your cloud functions run

```
gcloud functions list
```

2. For each cloud function run the following command.

```
gcloud functions describe <function_name>
```

3. Review the settings of the buildEnvironmentVariables and environmentVariables. Keep this information for the next step.

### Migrating Environment Variables to Secrets within the Secret Manager

#### From Google Cloud Console

1. Go to the Secret Manager page in the Cloud Console.
2. On the Secret Manager page, click Create Secret.
3. On the Create secret page, under Name, enter the name of the Environment Variable you are replacing. This will then be the Secret Variable you will reference in your code.
4. You will also need to add a version. This is the actual value of the variable that will be referenced from the code. To add a secret version when creating the initial secret, in the Secret value field, enter the value from the Environment Variable you are replacing.
5. Leave the Regions section unchanged.
6. Click the Create secret button.
7. Repeat for all Environment Variables

### From Google Cloud CLI

1. Run the following command with the Environment Variable name you are replacing in the <secret-id>. It is most secure to point this command to a file with the Environment Variable value located in it, as if you entered it via command line it would show up in your shell's command history.

```
gcloud secrets create <secret-id> --data-file="/path/to/file.txt"
```

### Granting your Runtime's Service Account Access to Secrets

#### From Google Cloud Console

1. Within the project containing your runtime login with account that has the 'roles/secretmanager.secretAccessor' permission.



2. Select the Navigation hamburger menu in the top left. Hover over 'Security' to under the then select 'Secret Manager' in the menu that opens up.
3. Click the name of a secret listed in this screen.
4. If it is not already open, click Show Info Panel in this screen to open the panel.
5. In the info panel, click Add principal.
6. In the New principals field, enter the service account your function uses for its identity. (If you need help locating or updating your runtime's service account, please see the '[docs/securing/function-identity#runtime\\_service\\_account](#)' reference.)
5. In the Select a role dropdown, choose Secret Manager and then Secret Manager Secret Accessor.

### From Google Cloud CLI

As of the time of writing, using Google CLI to list Runtime variables is only in beta. Because this is likely to change we are not including it here.

Modifying the Code to use the Secrets in Secret Manager

### From Google Cloud Console

This depends heavily on which language your runtime is in. For the sake of the brevity of this recommendation, please see the '[/docs/creating-and-accessing-secrets#access](#)' reference for language specific instructions.

### From Google Cloud CLI

This depends heavily on which language your runtime is in. For the sake of the brevity of this recommendation, please see the '[/docs/creating-and-accessing-secrets#access](#)' reference for language specific instructions.

Deleting the Insecure Environment Variables

**Be certain to do this step last.** Removing variables from code actively referencing them will prevent it from completing successfully.

### From Google Cloud Console

1. Select the Navigation hamburger menu in the top left. Hover over 'Security' then select 'Secret Manager' in the menu that opens up.
2. Click the name of a function. Click Edit.
3. Click Runtime, build and connections settings to expand the advanced configuration options.
4. Click 'Security'. Hover over the secret you want to remove, then click 'Delete'.
5. Click Next. Click Deploy. The latest version of the runtime will now reference the secrets in Secret Manager.

### From Google Cloud CLI

```
gcloud functions deploy <Function name>--remove-env-vars <env vars>
```

If you need to find the env vars to remove, they are from the step where 'gcloud functions describe <function\_name>' was run.

### Default Value:

By default Secret Manager is not enabled.






## References:

1. [https://cloud.google.com/functions/docs/configuring/env-var#managing\\_secrets](https://cloud.google.com/functions/docs/configuring/env-var#managing_secrets)
2. <https://cloud.google.com/secret-manager/docs/overview>

## Additional Information:

There are slight additional costs to using the Secret Manager API. Review the documentation to determine your organizations' needs.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	<b>14.8 <u>Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			
v7	<b>16.4 <u>Encrypt or Hash all Authentication Credentials</u></b> Encrypt or hash with a salt all authentication credentials when stored.			

## 2 Logging and Monitoring

This section covers recommendations addressing Logging and Monitoring on Google Cloud Platform.

## *2.1 Ensure That Cloud Audit Logging Is Configured Properly (Automated)*

### **Profile Applicability:**

- Level 1

### **Description:**

It is recommended that Cloud Audit Logging is configured to track all admin activities and read, write access to user data.

### **Rationale:**

Cloud Audit Logging maintains two audit logs for each project, folder, and organization: Admin Activity and Data Access.

1. Admin Activity logs contain log entries for API calls or other administrative actions that modify the configuration or metadata of resources. Admin Activity audit logs are enabled for all services and cannot be configured.
2. Data Access audit logs record API calls that create, modify, or read user-provided data. These are disabled by default and should be enabled.

There are three kinds of Data Access audit log information:

- Admin read: Records operations that read metadata or configuration information. Admin Activity audit logs record writes of metadata and configuration information that cannot be disabled.
- Data read: Records operations that read user-provided data.
- Data write: Records operations that write user-provided data.

It is recommended to have an effective default audit config configured in such a way that:

1. logtype is set to DATA\_READ (to log user activity tracking) and DATA\_WRITES (to log changes/tampering to user data).
2. audit config is enabled for all the services supported by the Data Access audit logs feature.
3. Logs should be captured for all users, i.e., there are no exempted users in any of the audit config sections. This will ensure overriding the audit config will not contradict the requirement.

### **Impact:**

There is no charge for Admin Activity audit logs. Enabling the Data Access audit logs might result in your project being charged for the additional logs usage.

## Audit:

### From Google Cloud Console

1. Go to `Audit Logs` by visiting <https://console.cloud.google.com/iam-admin/audit>.
2. Ensure that Admin Read, Data Write, and Data Read are enabled for all Google Cloud services and that no exemptions are allowed.

### From Google Cloud CLI

1. List the Identity and Access Management (IAM) policies for the project, folder, or organization:

```
gcloud organizations get-iam-policy ORGANIZATION_ID
gcloud resource-manager folders get-iam-policy FOLDER_ID
gcloud projects get-iam-policy PROJECT_ID
```

2. Policy should have a default `auditConfigs` section which has the logtype set to `DATA_WRITES` and `DATA_READ` for all services. Note that projects inherit settings from folders, which in turn inherit settings from the organization. When called, `projects get-iam-policy`, the result shows only the policies set in the project, not the policies inherited from the parent folder or organization. Nevertheless, if the parent folder has Cloud Audit Logging enabled, the project does as well.

Sample output for default audit configs may look like this:

```
auditConfigs:
- auditLogConfigs:
- logType: ADMIN_READ
- logType: DATA_WRITE
- logType: DATA_READ
service: allServices
```

3. Any of the `auditConfigs` sections should not have parameter `"exemptedMembers:"` set, which will ensure that Logging is enabled for all users and no user is exempted.

## Remediation:

### From Google Cloud Console

1. Go to `Audit Logs` by visiting <https://console.cloud.google.com/iam-admin/audit>.
2. Follow the steps at <https://cloud.google.com/logging/docs/audit/configure-data-access> to enable audit logs for all Google Cloud services. Ensure that no exemptions are allowed.

## From Google Cloud CLI

1. To read the project's IAM policy and store it in a file run a command:

```
gcloud projects get-iam-policy PROJECT_ID > /tmp/project_policy.yaml
```

Alternatively, the policy can be set at the organization or folder level. If setting the policy at the organization level, it is not necessary to also set it for each folder or project.

```
gcloud organizations get-iam-policy ORGANIZATION_ID > /tmp/org_policy.yaml
gcloud resource-manager folders get-iam-policy FOLDER_ID >
/tmp/folder_policy.yaml
```

2. Edit policy in /tmp/policy.yaml, adding or changing only the audit logs configuration to:

**Note: Admin Activity Logs are enabled by default, and cannot be disabled. So they are not listed in these configuration changes.**

```
auditConfigs:
- auditLogConfigs:
  - logType: DATA_WRITE
  - logType: DATA_READ
  service: allServices
```

**Note:** `exemptedMembers:` is not set as audit logging should be enabled for all the users

3. To write new IAM policy run command:

```
gcloud organizations set-iam-policy ORGANIZATION_ID /tmp/org_policy.yaml
gcloud resource-manager folders set-iam-policy FOLDER_ID
/tmp/folder_policy.yaml
gcloud projects set-iam-policy PROJECT_ID /tmp/project_policy.yaml
```

If the preceding command reports a conflict with another change, then repeat these steps, starting with the first step.

### Default Value:

Admin Activity logs are always enabled. They cannot be disabled. Data Access audit logs are disabled by default because they can be quite large.

### References:











1. <https://cloud.google.com/logging/docs/audit/>
2. <https://cloud.google.com/logging/docs/audit/configure-data-access>

### Additional Information:

- Log type `DATA_READ` is equally important to that of `DATA_WRITE` to track detailed user activities.

- BigQuery Data Access logs are handled differently from other data access logs. BigQuery logs are enabled by default and cannot be disabled. They do not count against logs allotment and cannot result in extra logs charges.

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	<b>8.11 <u>Conduct Audit Log Reviews</u></b> Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.			
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			
v7	<b>6.7 <u>Regularly Review Logs</u></b> On a regular basis, review logs to identify anomalies or abnormal events.			

## 2.2 Ensure That Sinks Are Configured for All Log Entries (Automated)

### Profile Applicability:

- Level 1

### Description:

It is recommended to create a sink that will export copies of all the log entries. This can help aggregate logs from multiple projects and export them to a Security Information and Event Management (SIEM).

### Rationale:

Log entries are held in Cloud Logging. To aggregate logs, export them to a SIEM. To keep them longer, it is recommended to set up a log sink. Exporting involves writing a filter that selects the log entries to export, and choosing a destination in Cloud Storage, BigQuery, or Cloud Pub/Sub. The filter and destination are held in an object called a sink. To ensure all log entries are exported to sinks, ensure that there is no filter configured for a sink. Sinks can be created in projects, organizations, folders, and billing accounts.

### Impact:

There are no costs or limitations in Cloud Logging for exporting logs, but the export destinations charge for storing or transmitting the log data.

### Audit:

#### From Google Cloud Console

1. Go to `Logs Router` by visiting <https://console.cloud.google.com/logs/router>.
2. For every sink, click the 3-dot button for Menu options and select `View sink details`.
3. Ensure there is at least one sink with an `empty` Inclusion filter.
4. Additionally, ensure that the resource configured as `Destination` exists.

#### From Google Cloud CLI

1. Ensure that a sink with an `empty filter` exists. List the sinks for the project, folder or organization. If sinks are configured at a folder or organization level, they do not need to be configured for each project:

```
gcloud logging sinks list --folder=FOLDER_ID | --organization=ORGANIZATION_ID  
| --project=PROJECT_ID
```

The output should list at least one sink with an `empty filter`.



2. Additionally, ensure that the resource configured as `Destination` exists.

See <https://cloud.google.com/sdk/gcloud/reference/beta/logging/sinks/list> for more information.

## Remediation:

### From Google Cloud Console

1. Go to `Logs Router` by visiting <https://console.cloud.google.com/logs/router>.
2. Click on the arrow symbol with `CREATE SINK` text.
3. Fill out the fields for `Sink` details.
4. Choose Cloud Logging bucket in the Select sink destination drop down menu.
5. Choose a log bucket in the next drop down menu.
6. If an inclusion filter is not provided for this sink, all ingested logs will be routed to the destination provided above. This may result in higher than expected resource usage.
7. Click `Create Sink`.

For more information, see

[https://cloud.google.com/logging/docs/export/configure\\_export\\_v2#dest-create](https://cloud.google.com/logging/docs/export/configure_export_v2#dest-create).

### From Google Cloud CLI

To create a sink to export all log entries in a Google Cloud Storage bucket:

```
gcloud logging sinks create <sink-name>
storage.googleapis.com/DESTINATION_BUCKET_NAME
```

Sinks can be created for a folder or organization, which will include all projects.

```
gcloud logging sinks create <sink-name>
storage.googleapis.com/DESTINATION_BUCKET_NAME --include-children --
folder=FOLDER_ID | --organization=ORGANIZATION_ID
```

## Note:

1. A sink created by the command-line above will export logs in storage buckets. However, sinks can be configured to export logs into BigQuery, or Cloud Pub/Sub, or `Custom Destination`.
2. While creating a sink, the sink option `--log-filter` is not used to ensure the sink exports all log entries.
3. A sink can be created at a folder or organization level that collects the logs of all the projects underneath bypassing the option `--include-children` in the `gcloud` command.

## Default Value:

By default, there are no sinks configured.

## References:












1. <https://cloud.google.com/logging/docs/reference/tools/gcloud-logging>

2. <https://cloud.google.com/logging/quotas>
3. <https://cloud.google.com/logging/docs/routing/overview>
4. [https://cloud.google.com/logging/docs/export/using\\_exported\\_logs](https://cloud.google.com/logging/docs/export/using_exported_logs)
5. [https://cloud.google.com/logging/docs/export/configure\\_export\\_v2](https://cloud.google.com/logging/docs/export/configure_export_v2)
6. [https://cloud.google.com/logging/docs/export/aggregated\\_exports](https://cloud.google.com/logging/docs/export/aggregated_exports)
7. <https://cloud.google.com/sdk/gcloud/reference/beta/logging/sinks/list>

### Additional Information:

For Command-Line Audit and Remediation, the sink destination of type `Cloud Storage Bucket` is considered. However, the destination could be configured to `Cloud Storage Bucket` or `BigQuery` or `Cloud Pub/Sub` or `Custom Destination`. `Command Line Interface` commands would change accordingly.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	<b>8.3 <u>Ensure Adequate Audit Log Storage</u></b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			
v7	<b>6.4 <u>Ensure adequate storage for logs</u></b> Ensure that all systems that store logs have adequate storage space for the logs generated.			

## *2.3 Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket Lock (Automated)*

### **Profile Applicability:**

- Level 2

### **Description:**

Enabling retention policies on log buckets will protect logs stored in cloud storage buckets from being overwritten or accidentally deleted. It is recommended to set up retention policies and configure Bucket Lock on all storage buckets that are used as log sinks.

### **Rationale:**

Logs can be exported by creating one or more sinks that include a log filter and a destination. As Cloud Logging receives new log entries, they are compared against each sink. If a log entry matches a sink's filter, then a copy of the log entry is written to the destination.

Sinks can be configured to export logs in storage buckets. It is recommended to configure a data retention policy for these cloud storage buckets and to lock the data retention policy; thus permanently preventing the policy from being reduced or removed. This way, if the system is ever compromised by an attacker or a malicious insider who wants to cover their tracks, the activity logs are definitely preserved for forensics and security investigations.

### **Impact:**

Locking a bucket is an irreversible action. Once you lock a bucket, you cannot remove the retention policy from the bucket or decrease the retention period for the policy. You will then have to wait for the retention period for all items within the bucket before you can delete them, and then the bucket.

### **Audit:**

#### **From Google Cloud Console**

1. Open the Cloud Storage browser in the Google Cloud Console by visiting <https://console.cloud.google.com/storage/browser>.
2. In the Column display options menu, make sure `Retention policy` is checked.
3. In the list of buckets, the retention period of each bucket is found in the `Retention policy` column. If the retention policy is locked, an image of a lock appears directly to the left of the retention period.

#### **From Google Cloud CLI**

1. To list all sinks destined to storage buckets:

```
gcloud logging sinks list --folder=FOLDER_ID | --organization=ORGANIZATION_ID  
| --project=PROJECT_ID
```

2. For every storage bucket listed above, verify that retention policies and Bucket Lock are enabled:

```
gsutil retention get gs://BUCKET_NAME
```

For more information, see <https://cloud.google.com/storage/docs/using-bucket-lock#view-policy>.

### Remediation:

#### From Google Cloud Console

1. If sinks are **not** configured, first follow the instructions in the recommendation:  
Ensure that sinks are configured for all Log entries.
2. For each storage bucket configured as a sink, go to the Cloud Storage browser at [https://console.cloud.google.com/storage/browser/<BUCKET\\_NAME>](https://console.cloud.google.com/storage/browser/<BUCKET_NAME>).
3. Select the Bucket Lock tab near the top of the page.
4. In the Retention policy entry, click the Add Duration link. The Set a retention policy dialog box appears.
5. Enter the desired length of time for the retention period and click Save policy.
6. Set the Lock status for this retention policy to Locked.

#### From Google Cloud CLI

1. To list all sinks destined to storage buckets:

```
gcloud logging sinks list --folder=FOLDER_ID | --organization=ORGANIZATION_ID  
| --project=PROJECT_ID
```

2. For each storage bucket listed above, set a retention policy and lock it:

```
gsutil retention set [TIME_DURATION] gs://[BUCKET_NAME]  
gsutil retention lock gs://[BUCKET_NAME]
```

For more information, visit <https://cloud.google.com/storage/docs/using-bucket-lock#set-policy>.

### Default Value:

By default, storage buckets used as log sinks do not have retention policies and Bucket Lock configured.







## References:

1. <https://cloud.google.com/storage/docs/bucket-lock>
2. <https://cloud.google.com/storage/docs/using-bucket-lock>
3. <https://cloud.google.com/storage/docs/bucket-lock>

## Additional Information:

Caution: Locking a retention policy is an irreversible action. Once locked, you must delete the entire bucket in order to "remove" the bucket's retention policy. However, before you can delete the bucket, you must be able to delete all the objects in the bucket, which itself is only possible if all the objects have reached the retention period set by the retention policy.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

## 2.4 Ensure Log Metric Filter and Alerts Exist for Project Ownership Assignments/Changes (Automated)

### Profile Applicability:

- Level 1

### Description:

In order to prevent unnecessary project ownership assignments to users/service-accounts and further misuses of projects and resources, all `roles/Owner` assignments should be monitored.

Members (users/Service-Accounts) with a role assignment to primitive role `roles/Owner` are project owners.

The project owner has all the privileges on the project the role belongs to. These are summarized below:

- All viewer permissions on all GCP Services within the project
- Permissions for actions that modify the state of all GCP services within the project
- Manage roles and permissions for a project and all resources within the project
- Set up billing for a project

Granting the owner role to a member (user/Service-Account) will allow that member to modify the Identity and Access Management (IAM) policy. Therefore, grant the owner role only if the member has a legitimate purpose to manage the IAM policy. This is because the project IAM policy contains sensitive access control data. Having a minimal set of users allowed to manage IAM policy will simplify any auditing that may be necessary.

### Rationale:

Project ownership has the highest level of privileges on a project. To avoid misuse of project resources, the project ownership assignment/change actions mentioned above should be monitored and alerted to concerned recipients.

- Sending project ownership invites
- Acceptance/Rejection of project ownership invite by user
- Adding `role\Owner` to a user/service-account
- Removing a user/Service account from `role\Owner`

### Impact:

Enabling of logging may result in your project being charged for the additional logs usage.

## Audit:

### From Google Cloud Console

Ensure that the prescribed log metric is present:

1. Go to Logging/Log-based Metrics by visiting <https://console.cloud.google.com/logs/metrics>.
2. In the User-defined Metrics section, ensure that at least one metric `<Log_Metric_Name>` is present with filter text:

```
(protoPayload.serviceName="cloudresourcemanager.googleapis.com")
AND (ProjectOwnership OR projectOwnerInvitee)
OR (protoPayload.serviceData.policyDelta.bindingDeltas.action="REMOVE"
AND protoPayload.serviceData.policyDelta.bindingDeltas.role="roles/owner")
OR (protoPayload.serviceData.policyDelta.bindingDeltas.action="ADD"
AND protoPayload.serviceData.policyDelta.bindingDeltas.role="roles/owner")
```

Ensure that the prescribed Alerting Policy is present:

3. Go to Alerting by visiting <https://console.cloud.google.com/monitoring/alerting>.
4. Under the Policies section, ensure that at least one alert policy exists for the log metric above. Clicking on the policy should show that it is configured with a condition. For example, Violates when: Any logging.googleapis.com/user/<Log Metric Name> stream is above a threshold of zero(0) for greater than zero(0) seconds means that the alert will trigger for any new owner change. Verify that the chosen alerting thresholds make sense for your organization.
5. Ensure that the appropriate notifications channels have been set up.

### From Google Cloud CLI

Ensure that the prescribed log metric is present:

1. List the log metrics:

```
gcloud logging metrics list --format json
```

2. Ensure that the output contains at least one metric with filter set to:

```
(protoPayload.serviceName="cloudresourcemanager.googleapis.com")
AND (ProjectOwnership OR projectOwnerInvitee)
OR (protoPayload.serviceData.policyDelta.bindingDeltas.action="REMOVE"
AND protoPayload.serviceData.policyDelta.bindingDeltas.role="roles/owner")
OR (protoPayload.serviceData.policyDelta.bindingDeltas.action="ADD"
AND protoPayload.serviceData.policyDelta.bindingDeltas.role="roles/owner")
```

3. Note the value of the property `metricDescriptor.type` for the identified metric, in the format `logging.googleapis.com/user/<Log Metric Name>`.

Ensure that the prescribed alerting policy is present:

#### 4. List the alerting policies:

```
gcloud alpha monitoring policies list --format json
```

#### 5. Ensure that the output contains an least one alert policy where:

- `conditions.conditionThreshold.filter` is set to `metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"`
- `AND enabled` is set to `true`

### Remediation:

#### From Google Cloud Console

#### Create the prescribed log metric:

1. Go to `Logging/Logs-based Metrics` by visiting <https://console.cloud.google.com/logs/metrics> and click "CREATE METRIC".
2. Click the down arrow symbol on the `Filter Bar` at the rightmost corner and select `Convert to Advanced Filter`.
3. Clear any text and add:

```
(protoPayload.serviceName="cloudresourcemanager.googleapis.com")
AND (ProjectOwnership OR projectOwnerInvitee)
OR (protoPayload.serviceData.policyDelta.bindingDeltas.action="REMOVE"
AND protoPayload.serviceData.policyDelta.bindingDeltas.role="roles/owner")
OR (protoPayload.serviceData.policyDelta.bindingDeltas.action="ADD"
AND protoPayload.serviceData.policyDelta.bindingDeltas.role="roles/owner")
```

4. Click `Submit Filter`. The logs display based on the filter text entered by the user.
5. In the `Metric Editor` menu on the right, fill out the name field. Set `Units` to `1` (default) and the `Type` to `Counter`. This ensures that the log metric counts the number of log entries matching the advanced logs query.
6. Click `Create Metric`.

#### Create the display prescribed Alert Policy:

1. Identify the newly created metric under the section `User-defined Metrics` at <https://console.cloud.google.com/logs/metrics>.
2. Click the 3-dot icon in the rightmost column for the desired metric and select `Create alert from Metric`. A new page opens.
3. Fill out the alert policy configuration and click `Save`. Choose the alerting threshold and configuration that makes sense for the user's organization. For example, a



threshold of zero(0) for the most recent value will ensure that a notification is triggered for every owner change in the project:

```
Set `Aggregator` to `Count`  
  
Set `Configuration`:  
  
- Condition: above  
  
- Threshold: 0  
  
- For: most recent value
```

4. Configure the desired notifications channels in the section `Notifications`.
5. Name the policy and click `Save`.

### From Google Cloud CLI

Create a prescribed Log Metric:

- Use the command: `gcloud beta logging metrics create`
- Reference for Command Usage:  
<https://cloud.google.com/sdk/gcloud/reference/beta/logging/metrics/create>

Create prescribed Alert Policy

- Use the command: `gcloud alpha monitoring policies create`
- Reference for Command Usage:  
<https://cloud.google.com/sdk/gcloud/reference/alpha/monitoring/policies/create>







### References:

1. <https://cloud.google.com/logging/docs/logs-based-metrics/>
2. <https://cloud.google.com/monitoring/custom-metrics/>
3. <https://cloud.google.com/monitoring/alerts/>
4. <https://cloud.google.com/logging/docs/reference/tools/gcloud-logging>

### Additional Information:

1. Project ownership assignments for a user cannot be done using the `gcloud` utility as assigning project ownership to a user requires sending, and the user accepting, an invitation.
2. Project Ownership assignment to a service account does not send any invites. Set IAM Policy to `role/owner` is directly performed on service accounts.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			

## 2.5 Ensure That the Log Metric Filter and Alerts Exist for Audit Configuration Changes (Automated)

### Profile Applicability:

- Level 1

### Description:

Google Cloud Platform (GCP) services write audit log entries to the Admin Activity and Data Access logs to help answer the questions of, "who did what, where, and when?" within GCP projects.

Cloud audit logging records information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by GCP services. Cloud audit logging provides a history of GCP API calls for an account, including API calls made via the console, SDKs, command-line tools, and other GCP services.

### Rationale:

Admin activity and data access logs produced by cloud audit logging enable security analysis, resource change tracking, and compliance auditing.

Configuring the metric filter and alerts for audit configuration changes ensures the recommended state of audit configuration is maintained so that all activities in the project are audit-able at any point in time.

### Impact:

Enabling of logging may result in your project being charged for the additional logs usage.

### Audit:

#### From Google Cloud Console

#### Ensure the prescribed log metric is present:

1. Go to `Logging/Logs-based Metrics` by visiting <https://console.cloud.google.com/logs/metrics>.
2. In the `User-defined Metrics` section, ensure that at least one metric `<Log_Metric_Name>` is present with the filter text:

```
protoPayload.methodName="SetIamPolicy" AND  
protoPayload.serviceData.policyDelta.auditConfigDeltas:*
```

#### Ensure that the prescribed alerting policy is present:

3. Go to **Alerting** by visiting <https://console.cloud.google.com/monitoring/alerting>.
4. Under the **Policies** section, ensure that at least one alert policy exists for the log metric above. Clicking on the policy should show that it is configured with a condition. For example, **Violates when: Any**  
`logging.googleapis.com/user/<Log Metric Name> stream is above a threshold of 0 for greater than zero(0) seconds`, means that the alert will trigger for any new owner change. Verify that the chosen alerting thresholds make sense for the user's organization.
5. Ensure that appropriate notifications channels have been set up.

## From Google Cloud CLI

### Ensure that the prescribed log metric is present:

1. List the log metrics:

```
gcloud beta logging metrics list --format json
```

2. Ensure that the output contains at least one metric with the filter set to:

```
protoPayload.methodName="SetIamPolicy" AND  
protoPayload.serviceData.policyDelta.auditConfigDeltas:*
```

3. Note the value of the property `metricDescriptor.type` for the identified metric, in the format `logging.googleapis.com/user/<Log Metric Name>`.

### Ensure that the prescribed alerting policy is present:

4. List the alerting policies:

```
gcloud alpha monitoring policies list --format json
```

5. Ensure that the output contains at least one alert policy where:
  - `conditions.conditionThreshold.filter` is set to  
`metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"`
  - **AND** `enabled` is set to `true`

## Remediation:

### From Google Cloud Console

#### Create the prescribed log metric:

1. Go to **Logging/Logs-based Metrics** by visiting <https://console.cloud.google.com/logs/metrics> and click "CREATE METRIC".
2. Click the down arrow symbol on the **Filter Bar** at the rightmost corner and select **Convert to Advanced Filter**.
3. Clear any text and add:

```
protoPayload.methodName="SetIamPolicy" AND  
protoPayload.serviceData.policyDelta.auditConfigDeltas:*
```

4. Click `Submit Filter`. Display logs appear based on the filter text entered by the user.
5. In the `Metric Editor` menu on the right, fill out the name field. Set `Units` to 1 (default) and `Type` to `Counter`. This will ensure that the log metric counts the number of log entries matching the user's advanced logs query.
6. Click `Create Metric`.

### Create a prescribed Alert Policy:

1. Identify the new metric the user just created, under the section `User-defined Metrics` at <https://console.cloud.google.com/logs/metrics>.
2. Click the 3-dot icon in the rightmost column for the new metric and select `Create alert` from `Metric`. A new page opens.
3. Fill out the alert policy configuration and click `Save`. Choose the alerting threshold and configuration that makes sense for the organization. For example, a threshold of zero(0) for the most recent value will ensure that a notification is triggered for every owner change in the project:

```
Set `Aggregator` to `Count`  
  
Set `Configuration`:  
  
- Condition: above  
  
- Threshold: 0  
  
- For: most recent value
```

4. Configure the desired notifications channels in the section `Notifications`.
5. Name the policy and click `Save`.

### From Google Cloud CLI

Create a prescribed Log Metric:

- Use the command: `gcloud beta logging metrics create`
- Reference for command usage:  
<https://cloud.google.com/sdk/gcloud/reference/beta/logging/metrics/create>











Create prescribed Alert Policy

- Use the command: `gcloud alpha monitoring policies create`
- Reference for command usage:  
<https://cloud.google.com/sdk/gcloud/reference/alpha/monitoring/policies/create>

## References:

1. <https://cloud.google.com/logging/docs/logs-based-metrics/>
2. <https://cloud.google.com/monitoring/custom-metrics/>
3. <https://cloud.google.com/monitoring/alerts/>
4. <https://cloud.google.com/logging/docs/reference/tools/gcloud-logging>
5. <https://cloud.google.com/logging/docs/audit/configure-data-access#getiampolicy-setiampolicy>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	<b>8.5 Collect Detailed Audit Logs</b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.			
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 2.6 Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes (Automated)

### Profile Applicability:

- Level 1

### Description:

It is recommended that a metric filter and alarm be established for changes to Identity and Access Management (IAM) role creation, deletion and updating activities.

### Rationale:

Google Cloud IAM provides predefined roles that give granular access to specific Google Cloud Platform resources and prevent unwanted access to other resources. However, to cater to organization-specific needs, Cloud IAM also provides the ability to create custom roles. Project owners and administrators with the Organization Role Administrator role or the IAM Role Administrator role can create custom roles. Monitoring role creation, deletion and updating activities will help in identifying any over-privileged role at early stages.

### Impact:

Enabling of logging may result in your project being charged for the additional logs usage.

### Audit:

#### From Console:

#### Ensure that the prescribed log metric is present:

1. Go to `Logging/Logs-based Metrics` by visiting <https://console.cloud.google.com/logs/metrics>.
2. In the `User-defined Metrics` section, ensure that at least one metric `<Log_Metric_Name>` is present with filter text:

```
resource.type="iam_role"
AND (protoPayload.methodName="google.iam.admin.v1.CreateRole"
OR protoPayload.methodName="google.iam.admin.v1.DeleteRole"
OR protoPayload.methodName="google.iam.admin.v1.UpdateRole")
```

#### Ensure that the prescribed alerting policy is present:

3. Go to `Alerting` by visiting <https://console.cloud.google.com/monitoring/alerting>.
4. Under the `Policies` section, ensure that at least one alert policy exists for the log metric above. Clicking on the policy should show that it is configured with a condition. For example, `Violates when: Any logging.googleapis.com/user/<Log Metric Name> stream is above a`

threshold of zero(0) for greater than zero(0) seconds means that the alert will trigger for any new owner change. Verify that the chosen alerting thresholds make sense for the user's organization.

5. Ensure that the appropriate notifications channels have been set up.

### From Google Cloud CLI

Ensure that the prescribed log metric is present:

1. List the log metrics:

```
gcloud logging metrics list --format json
```

2. Ensure that the output contains at least one metric with the filter set to:

```
resource.type="iam_role"  
AND (protoPayload.methodName = "google.iam.admin.v1.CreateRole" OR  
protoPayload.methodName="google.iam.admin.v1.DeleteRole" OR  
protoPayload.methodName="google.iam.admin.v1.UpdateRole")
```

3. Note the value of the property `metricDescriptor.type` for the identified metric, in the format `logging.googleapis.com/user/<Log Metric Name>`.

**Ensure that the prescribed alerting policy is present:**

4. List the alerting policies:

```
gcloud alpha monitoring policies list --format json
```

5. Ensure that the output contains an least one alert policy where:

- `conditions.conditionThreshold.filter` is set to `metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"`
- `AND enabled` is set to `true`.

### Remediation:

#### From Console:

**Create the prescribed log metric:**

1. Go to `Logging/Logs-based Metrics` by visiting <https://console.cloud.google.com/logs/metrics> and click "CREATE METRIC".
2. Click the down arrow symbol on the `Filter Bar` at the rightmost corner and select `Convert to Advanced Filter`.
3. Clear any text and add:



```
resource.type="iam_role"
AND (protoPayload.methodName = "google.iam.admin.v1.CreateRole"
OR protoPayload.methodName="google.iam.admin.v1.DeleteRole"
OR protoPayload.methodName="google.iam.admin.v1.UpdateRole")
```

1. Click `Submit Filter`. Display logs appear based on the filter text entered by the user.
2. In the `Metric Editor` menu on the right, fill out the name field. Set `Units` to `1` (default) and `Type` to `Counter`. This ensures that the log metric counts the number of log entries matching the advanced logs query.
3. Click `Create Metric`.

### Create a prescribed Alert Policy:

1. Identify the new metric that was just created under the section `User-defined Metrics` at <https://console.cloud.google.com/logs/metrics>.
2. Click the 3-dot icon in the rightmost column for the metric and select `Create alert from Metric`. A new page displays.
3. Fill out the alert policy configuration and click `Save`. Choose the alerting threshold and configuration that makes sense for the user's organization. For example, a threshold of zero(0) for the most recent value ensures that a notification is triggered for every owner change in the project:

```
Set `Aggregator` to `Count`

Set `Configuration`:

- Condition: above

- Threshold: 0

- For: most recent value
```

1. Configure the desired notification channels in the section `Notifications`.
2. Name the policy and click `Save`.

### From Google Cloud CLI

Create the prescribed Log Metric:

- Use the command: `gcloud logging metrics create`

Create the prescribed Alert Policy:











- Use the command: `gcloud alpha monitoring policies create`

### References:

1. <https://cloud.google.com/logging/docs/logs-based-metrics/>

2. <https://cloud.google.com/monitoring/custom-metrics/>
3. <https://cloud.google.com/monitoring/alerts/>
4. <https://cloud.google.com/logging/docs/reference/tools/gcloud-logging>
5. <https://cloud.google.com/iam/docs/understanding-custom-roles>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 2.7 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes (Automated)

### Profile Applicability:

- Level 2

### Description:

It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) Network Firewall rule changes.

### Rationale:

Monitoring for Create or Update Firewall rule events gives insight to network access changes and may reduce the time it takes to detect suspicious activity.

### Impact:

Enabling of logging may result in your project being charged for the additional logs usage. These charges could be significant depending on the size of the organization.

### Audit:

#### From Google Cloud Console

#### Ensure that the prescribed log metric is present:

1. Go to `Logging/Logs-based Metrics` by visiting <https://console.cloud.google.com/logs/metrics>.
2. In the `User-defined Metrics` section, ensure at least one metric `<Log_Metric_Name>` is present with this filter text:

```
resource.type="gce_firewall_rule"
AND (protoPayload.methodName:"compute.firewalls.patch"
OR protoPayload.methodName:"compute.firewalls.insert"
OR protoPayload.methodName:"compute.firewalls.delete")
```

#### Ensure that the prescribed alerting policy is present:

3. Go to `Alerting` by visiting <https://console.cloud.google.com/monitoring/alerting>.
4. Under the `Policies` section, ensure that at least one alert policy exists for the log metric above. Clicking on the policy should show that it is configured with a condition. For example, `Violates when: Any logging.googleapis.com/user/<Log Metric Name> stream is above a threshold of zero(0) for greater than zero(0) seconds` means that the alert will trigger for any new owner change. Verify that the chosen alerting thresholds make sense for the user's organization.
5. Ensure that appropriate notification channels have been set up.

## From Google Cloud CLI

### Ensure that the prescribed log metric is present:

1. List the log metrics:

```
gcloud logging metrics list --format json
```

2. Ensure that the output contains at least one metric with the filter set to:

```
resource.type="gce_firewall_rule"  
AND (protoPayload.methodName:"compute.firewalls.patch"  
OR protoPayload.methodName:"compute.firewalls.insert"  
OR protoPayload.methodName:"compute.firewalls.delete")
```

3. Note the value of the property `metricDescriptor.type` for the identified metric, in the format `logging.googleapis.com/user/<Log Metric Name>`.

### Ensure that the prescribed alerting policy is present:

4. List the alerting policies:

```
gcloud alpha monitoring policies list --format json
```

5. Ensure that the output contains an least one alert policy where:

- `conditions.conditionThreshold.filter` is set to `metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"`
- `AND enabled` is set to `true`

## Remediation:

### From Google Cloud Console

#### Create the prescribed log metric:

1. Go to `Logging/Logs-based Metrics` by visiting <https://console.cloud.google.com/logs/metrics> and click "CREATE METRIC".
2. Click the down arrow symbol on the `Filter Bar` at the rightmost corner and select `Convert to Advanced Filter`.
3. Clear any text and add:

```
resource.type="gce_firewall_rule"  
AND (protoPayload.methodName:"compute.firewalls.patch"  
OR protoPayload.methodName:"compute.firewalls.insert"  
OR protoPayload.methodName:"compute.firewalls.delete")
```

4. Click `Submit Filter`. Display logs appear based on the filter text entered by the user.
5. In the `Metric Editor` menu on the right, fill out the name field. Set `Units` to 1 (default) and `Type` to `Counter`. This ensures that the log metric counts the number of log entries matching the advanced logs query.
6. Click `Create Metric`.

### Create the prescribed Alert Policy:

1. Identify the newly created metric under the section `User-defined Metrics` at <https://console.cloud.google.com/logs/metrics>.
2. Click the 3-dot icon in the rightmost column for the new metric and select `Create alert from Metric`. A new page displays.
3. Fill out the alert policy configuration and click `Save`. Choose the alerting threshold and configuration that makes sense for the user's organization. For example, a threshold of zero(0) for the most recent value ensures that a notification is triggered for every owner change in the project:

```
Set `Aggregator` to `Count`  
Set `Configuration`:  
- Condition: above  
- Threshold: 0  
- For: most recent value
```

4. Configure the desired notifications channels in the section `Notifications`.
5. Name the policy and click `Save`.

### From Google Cloud CLI

Create the prescribed Log Metric

- Use the command: `gcloud logging metrics create`

Create the prescribed alert policy:











- Use the command: `gcloud alpha monitoring policies create`

### References:

1. <https://cloud.google.com/logging/docs/logs-based-metrics/>
2. <https://cloud.google.com/monitoring/custom-metrics/>
3. <https://cloud.google.com/monitoring/alerts/>
4. <https://cloud.google.com/logging/docs/reference/tools/gcloud-logging>

5. <https://cloud.google.com/vpc/docs/firewalls>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 2.8 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes (Automated)

### Profile Applicability:

- Level 2

### Description:

It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) network route changes.

### Rationale:

Google Cloud Platform (GCP) routes define the paths network traffic takes from a VM instance to another destination. The other destination can be inside the organization VPC network (such as another VM) or outside of it. Every route consists of a destination and a next hop. Traffic whose destination IP is within the destination range is sent to the next hop for delivery.

Monitoring changes to route tables will help ensure that all VPC traffic flows through an expected path.

### Impact:

Enabling of logging may result in your project being charged for the additional logs usage. These charges could be significant depending on the size of the organization.

### Audit:

#### From Google Cloud Console

#### Ensure that the prescribed Log metric is present:

1. Go to `Logging/Logs-based Metrics` by visiting <https://console.cloud.google.com/logs/metrics>.
2. In the `User-defined Metrics` section, ensure that at least one metric `<Log_Metric_Name>` is present with the filter text:

```
resource.type="gce_route"
AND (protoPayload.methodName:"compute.routes.delete"
OR protoPayload.methodName:"compute.routes.insert")
```

#### Ensure the prescribed alerting policy is present:

3. Go to `Alerting` by visiting: <https://console.cloud.google.com/monitoring/alerting>.
4. Under the `Policies` section, ensure that at least one alert policy exists for the log metric above. Clicking on the policy should show that it is configured with a condition. For example, `Violates when: Any logging.googleapis.com/user/<Log Metric Name> stream is above a`

threshold of 0 for greater than zero(0) seconds means that the alert will trigger for any new owner change. Verify that the chosen alert thresholds make sense for the user's organization.

5. Ensure that the appropriate notification channels have been set up.

### From Google Cloud CLI

#### Ensure the prescribed log metric is present:

1. List the log metrics:

```
gcloud logging metrics list --format json
```

2. Ensure that the output contains at least one metric with the filter set to:

```
resource.type="gce_route"  
AND (protoPayload.methodName:"compute.routes.delete"  
OR protoPayload.methodName:"compute.routes.insert")
```

3. Note the value of the property `metricDescriptor.type` for the identified metric, in the format `logging.googleapis.com/user/<Log Metric Name>`.

#### Ensure that the prescribed alerting policy is present:

4. List the alerting policies:

```
gcloud alpha monitoring policies list --format json
```

5. Ensure that the output contains an least one alert policy where:

- `conditions.conditionThreshold.filter` is set to `metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"`
- `AND enabled` is set to `true`

### Remediation:

#### From Google Cloud Console

#### Create the prescribed Log Metric:

1. Go to `Logging/Logs-based Metrics` by visiting <https://console.cloud.google.com/logs/metrics> and click "CREATE METRIC".
2. Click the down arrow symbol on the `Filter Bar` at the rightmost corner and select `Convert to Advanced Filter`
3. Clear any text and add:



```
resource.type="gce_route"
AND (protoPayload.methodName:"compute.routes.delete"
OR protoPayload.methodName:"compute.routes.insert")
```

4. Click `Submit Filter`. Display logs appear based on the filter text entered by the user.
5. In the `Metric Editor` menu on the right, fill out the name field. Set `Units` to `1` (default) and `Type` to `Counter`. This ensures that the log metric counts the number of log entries matching the user's advanced logs query.
6. Click `Create Metric`.

### Create the prescribed alert policy:

1. Identify the newly created metric under the section `User-defined Metrics` at <https://console.cloud.google.com/logs/metrics>.
2. Click the 3-dot icon in the rightmost column for the new metric and select `Create alert from Metric`. A new page displays.
3. Fill out the alert policy configuration and click `Save`. Choose the alerting threshold and configuration that makes sense for the user's organization. For example, a threshold of zero(0) for the most recent value ensures that a notification is triggered for every owner change in the project:

```
Set `Aggregator` to `Count`

Set `Configuration`:

- Condition: above
- Threshold: 0
- For: most recent value
```

4. Configure the desired notification channels in the section `Notifications`.
5. Name the policy and click `Save`.

### From Google Cloud CLI

Create the prescribed Log Metric:

- Use the command: `gcloud logging metrics create`











Create the prescribed the alert policy:

- Use the command: `gcloud alpha monitoring policies create`

## References:

1. <https://cloud.google.com/logging/docs/logs-based-metrics/>
2. <https://cloud.google.com/monitoring/custom-metrics/>
3. <https://cloud.google.com/monitoring/alerts/>
4. <https://cloud.google.com/logging/docs/reference/tools/gcloud-logging>
5. <https://cloud.google.com/storage/docs/access-control/iam>
6. <https://cloud.google.com/sdk/gcloud/reference/beta/logging/metrics/create>
7. <https://cloud.google.com/sdk/gcloud/reference/alpha/monitoring/policies/create>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	<b>8.5 Collect Detailed Audit Logs</b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.			
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 2.9 Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes (Automated)

### Profile Applicability:

- Level 2

### Description:

It is recommended that a metric filter and alarm be established for Virtual Private Cloud (VPC) network changes.

### Rationale:

It is possible to have more than one VPC within a project. In addition, it is also possible to create a peer connection between two VPCs enabling network traffic to route between VPCs.

Monitoring changes to a VPC will help ensure VPC traffic flow is not getting impacted.

### Impact:

Enabling of logging may result in your project being charged for the additional logs usage. These charges could be significant depending on the size of the organization.

### Audit:

#### From Google Cloud Console

#### Ensure the prescribed log metric is present:

1. Go to `Logging/Logs-based Metrics` by visiting <https://console.cloud.google.com/logs/metrics>.
2. In the `User-defined Metrics` section, ensure at least one metric `<Log_Metric_Name>` is present with filter text:

```
resource.type="gce_network"
AND (protoPayload.methodName:"compute.networks.insert"
OR protoPayload.methodName:"compute.networks.patch"
OR protoPayload.methodName:"compute.networks.delete"
OR protoPayload.methodName:"compute.networks.removePeering"
OR protoPayload.methodName:"compute.networks.addPeering")
```

#### Ensure the prescribed alerting policy is present:

3. Go to `Alerting` by visiting <https://console.cloud.google.com/monitoring/alerting>.
4. Under the `Policies` section, ensure that at least one alert policy exists for the log metric above. Clicking on the policy should show that it is configured with a condition. For example, `Violates when: Any logging.googleapis.com/user/<Log Metric Name> stream is above a threshold of 0 for greater than 0 seconds` means that the alert will trigger for

any new owner change. Verify that the chosen alerting thresholds make sense for the user's organization.

5. Ensure that appropriate notification channels have been set up.

### From Google Cloud CLI

#### Ensure the log metric is present:

1. List the log metrics:

```
gcloud logging metrics list --format json
```

2. Ensure that the output contains at least one metric with filter set to:

```
resource.type="gce_network"
AND protoPayload.methodName="beta.compute.networks.insert"
OR protoPayload.methodName="beta.compute.networks.patch"
OR protoPayload.methodName="v1.compute.networks.delete"
OR protoPayload.methodName="v1.compute.networks.removePeering"
OR protoPayload.methodName="v1.compute.networks.addPeering"
```

3. Note the value of the property `metricDescriptor.type` for the identified metric, in the format `logging.googleapis.com/user/<Log Metric Name>`.

#### Ensure the prescribed alerting policy is present:

4. List the alerting policies:

```
gcloud alpha monitoring policies list --format json
```

5. Ensure that the output contains at least one alert policy where:

- `conditions.conditionThreshold.filter` is set to `metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"`
- AND `enabled` is set to `true`

### Remediation:

#### From Google Cloud Console

#### Create the prescribed log metric:

1. Go to `Logging/Logs-based Metrics` by visiting <https://console.cloud.google.com/logs/metrics> and click "CREATE METRIC".
2. Click the down arrow symbol on `Filter Bar` at the rightmost corner and select `Convert to Advanced Filter`.
3. Clear any text and add:

```
resource.type="gce_network"
AND (protoPayload.methodName:"compute.networks.insert"
OR protoPayload.methodName:"compute.networks.patch"
OR protoPayload.methodName:"compute.networks.delete"
OR protoPayload.methodName:"compute.networks.removePeering"
OR protoPayload.methodName:"compute.networks.addPeering")
```

4. Click `Submit Filter`. Display logs appear based on the filter text entered by the user.
5. In the `Metric Editor` menu on the right, fill out the name field. Set `Units` to 1 (default) and `Type` to `Counter`. This ensures that the log metric counts the number of log entries matching the user's advanced logs query.
6. Click `Create Metric`.

### Create the prescribed alert policy:

1. Identify the newly created metric under the section `User-defined Metrics` at <https://console.cloud.google.com/logs/metrics>.
2. Click the 3-dot icon in the rightmost column for the new metric and select `Create alert from Metric`. A new page appears.
3. Fill out the alert policy configuration and click `Save`. Choose the alerting threshold and configuration that makes sense for the user's organization. For example, a threshold of 0 for the most recent value will ensure that a notification is triggered for every owner change in the project:

```
Set `Aggregator` to `Count`

Set `Configuration`:

- Condition: above
- Threshold: 0
- For: most recent value
```

4. Configure the desired notification channels in the section `Notifications`.
5. Name the policy and click `Save`.

### From Google Cloud CLI

Create the prescribed Log Metric:

- Use the command: `gcloud logging metrics create`











Create the prescribed alert policy:

- Use the command: `gcloud alpha monitoring policies create`

## References:

1. <https://cloud.google.com/logging/docs/logs-based-metrics/>
2. <https://cloud.google.com/monitoring/custom-metrics/>
3. <https://cloud.google.com/monitoring/alerts/>
4. <https://cloud.google.com/logging/docs/reference/tools/gcloud-logging>
5. <https://cloud.google.com/vpc/docs/overview>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	<b>8.5 Collect Detailed Audit Logs</b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.			
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 2.10 Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes (Automated)

### Profile Applicability:

- Level 2

### Description:

It is recommended that a metric filter and alarm be established for Cloud Storage Bucket IAM changes.

### Rationale:

Monitoring changes to cloud storage bucket permissions may reduce the time needed to detect and correct permissions on sensitive cloud storage buckets and objects inside the bucket.

### Impact:

Enabling of logging may result in your project being charged for the additional logs usage. These charges could be significant depending on the size of the organization.

### Audit:

#### From Google Cloud Console

#### Ensure the prescribed log metric is present:

1. For each project that contains cloud storage buckets, go to `Logging/Logs-based Metrics` by visiting <https://console.cloud.google.com/logs/metrics>.
2. In the `User-defined Metrics` section, ensure at least one metric `<Log_Metric_Name>` is present with the filter text:

```
resource.type="gcs_bucket"
AND protoPayload.methodName="storage.setIamPermissions"
```

#### Ensure that the prescribed alerting policy is present:

3. Go to `Alerting` by visiting <https://console.cloud.google.com/monitoring/alerting>.
4. Under the `Policies` section, ensure that at least one alert policy exists for the log metric above. Clicking on the policy should show that it is configured with a condition. For example, `Violates when: Any logging.googleapis.com/user/<Log Metric Name> stream is above a threshold of 0 for greater than 0 seconds` means that the alert will trigger for any new owner change. Verify that the chosen alerting thresholds make sense for the user's organization.
5. Ensure that the appropriate notifications channels have been set up.

## From Google Cloud CLI

### Ensure that the prescribed log metric is present:

1. List the log metrics:

```
gcloud logging metrics list --format json
```

2. Ensure that the output contains at least one metric with the filter set to:

```
resource.type=gcs_bucket  
AND protoPayload.methodName="storage.setIamPermissions"
```

3. Note the value of the property `metricDescriptor.type` for the identified metric, in the format `logging.googleapis.com/user/<Log Metric Name>`.

### Ensure the prescribed alerting policy is present:

4. List the alerting policies:

```
gcloud alpha monitoring policies list --format json
```

5. Ensure that the output contains an least one alert policy where:

- `conditions.conditionThreshold.filter` is set to `metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"`
- `AND enabled` is set to `true`

## Remediation:

### From Google Cloud Console

#### Create the prescribed log metric:

1. Go to `Logging/Logs-based Metrics` by visiting <https://console.cloud.google.com/logs/metrics> and click "CREATE METRIC".
2. Click the down arrow symbol on the `Filter Bar` at the rightmost corner and select `Convert to Advanced Filter`.
3. Clear any text and add:

```
resource.type="gcs_bucket"  
AND protoPayload.methodName="storage.setIamPermissions"
```

4. Click `Submit Filter`. Display logs appear based on the filter text entered by the user.



5. In the `Metric Editor` menu on right, fill out the name field. Set `Units` to 1 (default) and `Type` to `Counter`. This ensures that the log metric counts the number of log entries matching the user's advanced logs query.
6. Click `Create Metric`.

### Create the prescribed Alert Policy:

1. Identify the newly created metric under the section `User-defined Metrics` at <https://console.cloud.google.com/logs/metrics>.
2. Click the 3-dot icon in the rightmost column for the new metric and select `Create alert from Metric`. A new page appears.
3. Fill out the alert policy configuration and click `Save`. Choose the alerting threshold and configuration that makes sense for the user's organization. For example, a threshold of zero(0) for the most recent value will ensure that a notification is triggered for every owner change in the project:

```
Set `Aggregator` to `Count`  
  
Set `Configuration`:  
- Condition: above  
- Threshold: 0  
- For: most recent value
```

4. Configure the desired notifications channels in the section `Notifications`.
5. Name the policy and click `Save`.

### From Google Cloud CLI

Create the prescribed Log Metric:

- Use the command: `gcloud beta logging metrics create`











Create the prescribed alert policy:

- Use the command: `gcloud alpha monitoring policies create`

### References:

1. <https://cloud.google.com/logging/docs/logs-based-metrics/>
2. <https://cloud.google.com/monitoring/custom-metrics/>
3. <https://cloud.google.com/monitoring/alerts/>
4. <https://cloud.google.com/logging/docs/reference/tools/gcloud-logging>
5. <https://cloud.google.com/storage/docs/overview>
6. <https://cloud.google.com/storage/docs/access-control/iam-roles>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 2.11 Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes (Automated)

### Profile Applicability:

- Level 2

### Description:

It is recommended that a metric filter and alarm be established for SQL instance configuration changes.

### Rationale:

Monitoring changes to SQL instance configuration changes may reduce the time needed to detect and correct misconfigurations done on the SQL server.

Below are a few of the configurable options which may the impact security posture of an SQL instance:

- Enable auto backups and high availability: Misconfiguration may adversely impact business continuity, disaster recovery, and high availability
- Authorize networks: Misconfiguration may increase exposure to untrusted networks

### Impact:

Enabling of logging may result in your project being charged for the additional logs usage. These charges could be significant depending on the size of the organization.

### Audit:

#### From Google Cloud Console

#### Ensure the prescribed log metric is present:

1. For each project that contains Cloud SQL instances, go to `Logging/Logs-based Metrics` by visiting <https://console.cloud.google.com/logs/metrics>.
2. In the `User-defined Metrics` section, ensure that at least one metric `<Log_Metric_Name>` is present with the filter text:

```
protoPayload.methodName="cloudsql.instances.update"
```

#### Ensure that the prescribed alerting policy is present:

3. Go to `Alerting` by visiting <https://console.cloud.google.com/monitoring/alerting>.
4. Under the `Policies` section, ensure that at least one alert policy exists for the log metric above. Clicking on the policy should show that it is configured with a condition. For example, `Violates when: Any logging.googleapis.com/user/<Log Metric Name> stream is above a`

threshold of zero(0) for greater than zero(0) seconds means that the alert will trigger for any new owner change. Verify that the chosen alerting thresholds make sense for the user's organization.

5. Ensure that the appropriate notifications channels have been set up.

### From Google Cloud CLI

#### Ensure that the prescribed log metric is present:

1. List the log metrics:

```
gcloud logging metrics list --format json
```

2. Ensure that the output contains at least one metric with the filter set to

```
protoPayload.methodName="cloudsql.instances.update"
```

3. Note the value of the property `metricDescriptor.type` for the identified metric, in the format `logging.googleapis.com/user/<Log Metric Name>`.

#### Ensure that the prescribed alerting policy is present:

4. List the alerting policies:

```
gcloud alpha monitoring policies list --format json
```

5. Ensure that the output contains at least one alert policy where:

- `conditions.conditionThreshold.filter` is set to `metric.type=\"logging.googleapis.com/user/<Log Metric Name>\"`
- **AND enabled** is set to `true`

### Remediation:

#### From Google Cloud Console

#### Create the prescribed Log Metric:

1. Go to `Logging/Logs-based Metrics` by visiting <https://console.cloud.google.com/logs/metrics> and click "CREATE METRIC".
2. Click the down arrow symbol on the `Filter Bar` at the rightmost corner and select `Convert to Advanced Filter`.
3. Clear any text and add:

```
protoPayload.methodName="cloudsql.instances.update"
```

4. Click `Submit Filter`. Display logs appear based on the filter text entered by the user.
5. In the `Metric Editor` menu on right, fill out the name field. Set `Units` to `1` (default) and `Type` to `Counter`. This ensures that the log metric counts the number of log entries matching the user's advanced logs query.
6. Click `Create Metric`.

### Create the prescribed alert policy:

1. Identify the newly created metric under the section `User-defined Metrics` at <https://console.cloud.google.com/logs/metrics>.
2. Click the 3-dot icon in the rightmost column for the new metric and select `Create alert from Metric`. A new page appears.
3. Fill out the alert policy configuration and click `Save`. Choose the alerting threshold and configuration that makes sense for the user's organization. For example, a threshold of zero(0) for the most recent value will ensure that a notification is triggered for every owner change in the user's project:

```
Set `Aggregator` to `Count`  
Set `Configuration`:  
- Condition: above  
- Threshold: 0  
- For: most recent value
```

4. Configure the desired notification channels in the section `Notifications`.
5. Name the policy and click `Save`.

### From Google Cloud CLI

Create the prescribed log metric:

- Use the command: `gcloud logging metrics create`

Create the prescribed alert policy:











- Use the command: `gcloud alpha monitoring policies create`
- Reference for command usage:  
<https://cloud.google.com/sdk/gcloud/reference/alpha/monitoring/policies/create>

### References:

1. <https://cloud.google.com/logging/docs/logs-based-metrics/>
2. <https://cloud.google.com/monitoring/custom-metrics/>
3. <https://cloud.google.com/monitoring/alerts/>

4. <https://cloud.google.com/logging/docs/reference/tools/gcloud-logging>
5. <https://cloud.google.com/storage/docs/overview>
6. <https://cloud.google.com/sql/docs/>
7. <https://cloud.google.com/sql/docs/mysql/>
8. <https://cloud.google.com/sql/docs/postgres/>

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 2.12 Ensure That Cloud DNS Logging Is Enabled for All VPC Networks (Automated)

### Profile Applicability:

- Level 1

### Description:

Cloud DNS logging records the queries from the name servers within your VPC to Stackdriver. Logged queries can come from Compute Engine VMs, GKE containers, or other GCP resources provisioned within the VPC.

### Rationale:

Security monitoring and forensics cannot depend solely on IP addresses from VPC flow logs, especially when considering the dynamic IP usage of cloud resources, HTTP virtual host routing, and other technology that can obscure the DNS name used by a client from the IP address. Monitoring of Cloud DNS logs provides visibility to DNS names requested by the clients within the VPC. These logs can be monitored for anomalous domain names, evaluated against threat intelligence, and

Note: For full capture of DNS, firewall must block egress UDP/53 (DNS) and TCP/443 (DNS over HTTPS) to prevent client from using external DNS name server for resolution.

### Impact:

Enabling of Cloud DNS logging might result in your project being charged for the additional logs usage.

### Audit:

#### From Google Cloud CLI

1. List all VPCs networks in a project:

```
gcloud compute networks list --format="table[box,title='All VPC Networks'] (name:label='VPC Network Name') "
```

2. List all DNS policies, logging enablement, and associated VPC networks:

```
gcloud dns policies list --flatten="networks[]" --  
format="table[box,title='All DNS Policies By VPC Network'] (name:label='Policy  
Name',enableLogging:label='Logging  
Enabled':align=center,networks.networkUrl.basename():label='VPC Network  
Name') "
```

Each VPC Network should be associated with a DNS policy with logging enabled.

## Remediation:

### From Google Cloud CLI

#### Add New DNS Policy With Logging Enabled

For each VPC network that needs a DNS policy with logging enabled:

```
gcloud dns policies create enable-dns-logging --enable-logging --  
description="Enable DNS Logging" --networks=VPC_NETWORK_NAME
```

The VPC\_NETWORK\_NAME can be one or more networks in comma-separated list

#### Enable Logging for Existing DNS Policy

For each VPC network that has an existing DNS policy that needs logging enabled:

```
gcloud dns policies update POLICY_NAME --enable-logging --  
networks=VPC_NETWORK_NAME
```

The VPC\_NETWORK\_NAME can be one or more networks in comma-separated list

## Default Value:

Cloud DNS logging is disabled by default on each network.

## References:








1. <https://cloud.google.com/dns/docs/monitoring>

## Additional Information:








### Additional Info

- Only queries that reach a name server are logged. Cloud DNS resolvers cache responses, queries answered from caches, or direct queries to an external DNS resolver outside the VPC are not logged.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	<b>8.6 Collect DNS Query Audit Logs</b> Collect DNS query audit logs on enterprise assets, where appropriate and supported.			
v8	<b>8.11 Conduct Audit Log Reviews</b> Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.			



Controls Version	Control	IG 1	IG 2	IG 3
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			
v7	<b>6.7 <u>Regularly Review Logs</u></b> On a regular basis, review logs to identify anomalies or abnormal events.			
v7	<b>8.7 <u>Enable DNS Query Logging</u></b> Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.			

## 2.13 Ensure Cloud Asset Inventory Is Enabled (Automated)

### Profile Applicability:

- Level 1

### Description:

GCP Cloud Asset Inventory is services that provides a historical view of GCP resources and IAM policies through a time-series database. The information recorded includes metadata on Google Cloud resources, metadata on policies set on Google Cloud projects or resources, and runtime information gathered within a Google Cloud resource.

Cloud Asset Inventory Service (CAIS) API enablement is not required for operation of the service, but rather enables the mechanism for searching/exporting CAIS asset data directly.

### Rationale:

The GCP resources and IAM policies captured by GCP Cloud Asset Inventory enables security analysis, resource change tracking, and compliance auditing.

It is recommended GCP Cloud Asset Inventory be enabled for all GCP projects.

### Audit:

#### From Google Cloud Console

Ensure that the Cloud Asset API is enabled:

1. Go to `API & Services/Library` by visiting <https://console.cloud.google.com/apis/library>
2. Search for `Cloud Asset API` and select the result for *Cloud Asset API*
3. Ensure that `API Enabled` is displayed.

#### From Google Cloud CLI

Ensure that the Cloud Asset API is enabled:

1. Query enabled services:

```
gcloud services list --enabled --filter=name:cloudasset.googleapis.com
```

If the API is listed, then it is enabled. If the response is `Listed 0 items` the API is not enabled.

### Remediation:

#### From Google Cloud Console

Enable the Cloud Asset API:

1. Go to `API & Services/Library` by visiting <https://console.cloud.google.com/apis/library>
2. Search for `Cloud Asset API` and select the result for *Cloud Asset API*
3. Click the `ENABLE` button.

### From Google Cloud CLI

Enable the Cloud Asset API:

1. Enable the Cloud Asset API through the services interface:

```
gcloud services enable cloudasset.googleapis.com
```

### Default Value:

The Cloud Asset Inventory API is disabled by default in each project.

### References:

1. <https://cloud.google.com/asset-inventory/docs>




### Additional Information:










Additional info

- Cloud Asset Inventory only keeps a five-week history of Google Cloud asset metadata. If a longer history is desired, automation to export the history to Cloud Storage or BigQuery should be evaluated.

Users need not enable CAI API if they don't have any plans to export.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>1.1 Establish and Maintain Detailed Enterprise Asset Inventory</b></p> <p>Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.</p>			

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>6.6 Establish and Maintain an Inventory of Authentication and Authorization Systems</u></b></p> <p>Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.</p>			
v7	<p><b><u>1.4 Maintain Detailed Asset Inventory</u></b></p> <p>Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.</p>			
v7	<p><b><u>11.2 Document Traffic Configuration Rules</u></b></p> <p>All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.</p>			
v7	<p><b><u>16.1 Maintain an Inventory of Authentication Systems</u></b></p> <p>Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.</p>			

## 2.14 Ensure 'Access Transparency' is 'Enabled' (Manual)

### Profile Applicability:

- Level 2

### Description:

GCP Access Transparency provides audit logs for all actions that Google personnel take in your Google Cloud resources.

### Rationale:

Controlling access to your information is one of the foundations of information security. Given that Google Employees do have access to your organizations' projects for support reasons, you should have logging in place to view who, when, and why your information is being accessed.

### Impact:

To use Access Transparency your organization will need to have at one of the following support level: Premium, Enterprise, Platinum, or Gold. There will be subscription costs associated with support, as well as increased storage costs for storing the logs. You will also not be able to turn Access Transparency off yourself, and you will need to submit a service request to Google Cloud Support.

### Audit:

#### From Google Cloud Console

#### Determine if Access Transparency is Enabled

1. From the Google Cloud Home, click on the Navigation hamburger menu in the top left. Hover over the IAM & Admin Menu. Select `settings` in the middle of the column that opens.
2. The status will be under the heading `Access Transparency`. Status should be `Enabled`

### Remediation:

#### From Google Cloud Console

#### Add privileges to enable Access Transparency

1. From the Google Cloud Home, within the project you wish to check, click on the Navigation hamburger menu in the top left. Hover over the 'IAM and Admin'. Select `IAM` in the top of the column that opens.
2. Click the blue button the says `+add` at the top of the screen.
3. In the `principals` field, select a user or group by typing in their associated email address.

4. Click on the `role` field to expand it. In the filter field enter `Access Transparency Admin` and select it.
5. Click `save`.

### **Verify that the Google Cloud project is associated with a billing account**

1. From the Google Cloud Home, click on the Navigation hamburger menu in the top left. Select `Billing`.
2. If you see `This project is not associated with a billing account` you will need to enter billing information or switch to a project with a billing account.

### **Enable Access Transparency**

1. From the Google Cloud Home, click on the Navigation hamburger menu in the top left. Hover over the IAM & Admin Menu. Select `settings` in the middle of the column that opens.
2. Click the blue button labeled `Enable Access Transparency for Organization`

### **Default Value:**

By default Access Transparency is not enabled.











### **References:**

1. <https://cloud.google.com/cloud-provider-access-management/access-transparency/docs/overview>
2. <https://cloud.google.com/cloud-provider-access-management/access-transparency/docs/enable>
3. <https://cloud.google.com/cloud-provider-access-management/access-transparency/docs/reading-logs>
4. [https://cloud.google.com/cloud-provider-access-management/access-transparency/docs/reading-logs#justification\\_reason\\_codes](https://cloud.google.com/cloud-provider-access-management/access-transparency/docs/reading-logs#justification_reason_codes)
5. <https://cloud.google.com/cloud-provider-access-management/access-transparency/docs/supported-services>

### **Additional Information:**

To enable Access Transparency for your Google Cloud organization, your Google Cloud organization must have one of the following customer support levels: Premium, Enterprise, Platinum, or Gold.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 2.15 Ensure 'Access Approval' is 'Enabled' (Automated)

### Profile Applicability:

- Level 2

### Description:

GCP Access Approval enables you to require your organizations' explicit approval whenever Google support try to access your projects. You can then select users within your organization who can approve these requests through giving them a security role in IAM. All access requests display which Google Employee requested them in an email or Pub/Sub message that you can choose to Approve. This adds an additional control and logging of who in your organization approved/denied these requests.

### Rationale:

Controlling access to your information is one of the foundations of information security. Google Employees do have access to your organizations' projects for support reasons. With Access Approval, organizations can then be certain that their information is accessed by only approved Google Personnel.

### Impact:

To use Access Approval your organization will need have enabled Access Transparency and have at one of the following support level: Enhanced or Premium. There will be subscription costs associated with these support levels, as well as increased storage costs for storing the logs. You will also not be able to turn the Access Transparency which Access Approval depends on, off yourself. To do so you will need to submit a service request to Google Cloud Support. There will also be additional overhead in managing user permissions. There may also be a potential delay in support times as Google Personnel will have to wait for their access to be approved.

### Audit:

#### From Google Cloud Console

#### Determine if Access Transparency is Enabled as it is a Dependency

1. From the Google Cloud Home inside the project you wish to audit, click on the Navigation hamburger menu in the top left. Hover over the `IAM & Admin Menu`. Select `settings` in the middle of the column that opens.
2. The status should be "Enabled" under the heading `Access Transparency`

#### Determine if Access Approval is Enabled

1. From the Google Cloud Home, within the project you wish to check, click on the Navigation hamburger menu in the top left. Hover over the `Security Menu`. Select `Access Approval` in the middle of the column that opens.



2. The status will be displayed here. If you see a screen saying you need to enroll in Access Approval, it is not enabled.

## From Google Cloud CLI

### Determine if Access Approval is Enabled

1. From within the project you wish to audit, run the following command.

```
gcloud access-approval settings get
```

2. The status will be displayed in the output.

IF Access Approval is not enabled you should get this output:

```
API [accessapproval.googleapis.com] not enabled on project [-----]. Would you like to enable and retry (this will take a few minutes)? (y/N)?
```

After entering `y` if you get the following output, it means that Access Transparency is not enabled:

```
ERROR: (gcloud.access-approval.settings.get) FAILED_PRECONDITION: Precondition check failed.
```

## Remediation:

### From Google Cloud Console

1. From the Google Cloud Home, within the project you wish to enable, click on the Navigation hamburger menu in the top left. Hover over the `Security` Menu. Select `Access Approval` in the middle of the column that opens.
2. The status will be displayed here. On this screen, there is an option to click `Enroll`. If it is greyed out and you see an error bar at the top of the screen that says `Access Transparency is not enabled` please view the corresponding reference within this section to enable it.
3. In the second screen click `Enroll`.

### Grant an IAM Group or User the role with permissions to Add Users to be Access Approval message Recipients

1. From the Google Cloud Home, within the project you wish to enable, click on the Navigation hamburger menu in the top left. Hover over the `IAM and Admin`. Select `IAM` in the middle of the column that opens.
2. Click the blue button the says `+ ADD` at the top of the screen.
3. In the `principals` field, select a user or group by typing in their associated email address.
4. Click on the role field to expand it. In the filter field enter `Access Approval Approver` and select it.
5. Click `save`.

## Add a Group or User as an Approver for Access Approval Requests

1. As a user with the `Access Approval Approver` permission, within the project where you wish to add an email address to which request will be sent, click on the Navigation hamburger menu in the top left. Hover over the `Security Menu`. Select `Access Approval` in the middle of the column that opens.
2. Click `Manage Settings`
3. Under `Set up approval notifications`, enter the email address associated with a Google Cloud User or Group you wish to send Access Approval requests to. All future access approvals will be sent as emails to this address.

## From Google Cloud CLI

1. To update all services in an entire project, run the following command from an account that has permissions as an 'Approver for Access Approval Requests'

```
gcloud access-approval settings update --project=<project name> --  
enrolled_services=all --notification_emails='<email recipient for access  
approval requests>@<domain name>'
```

## Default Value:

By default Access Approval and its dependency of Access Transparency are not enabled.







## References:

1. <https://cloud.google.com/cloud-provider-access-management/access-approval/docs>
2. <https://cloud.google.com/cloud-provider-access-management/access-approval/docs/overview>
3. <https://cloud.google.com/cloud-provider-access-management/access-approval/docs/quickstart-custom-key>
4. <https://cloud.google.com/cloud-provider-access-management/access-approval/docs/supported-services>
5. <https://cloud.google.com/cloud-provider-access-management/access-approval/docs/view-historical-requests>

## Additional Information:

The recipients of Access Requests will also need to be logged into a Google Cloud account associated with an email address in this list. To approve requests they can click approve within the email. Or they can view requests at the the Access Approval page within the Security submenu.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

## 2.16 Ensure Logging is enabled for HTTP(S) Load Balancer (Automated)

### Profile Applicability:

- Level 2

### Description:

Logging enabled on a HTTPS Load Balancer will show all network traffic and its destination.

### Rationale:

Logging will allow you to view HTTPS network traffic to your web applications.

### Impact:

On high use systems with a high percentage sample rate, the logging file may grow to high capacity in a short amount of time. Ensure that the sample rate is set appropriately so that storage costs are not exorbitant.

### Audit:

#### From Google Cloud Console

1. From Google Cloud home open the Navigation Menu in the top left.
2. Under the `Networking` heading select `Network services`.
3. Select the HTTPS load-balancer you wish to audit.
4. Select `Edit` then `Backend Configuration`.
5. Select `Edit` on the corresponding backend service.
6. Ensure that `Enable Logging` is selected. Also ensure that `Sample Rate` is set to an appropriate level for your needs.

#### From Google Cloud CLI

1. Run the following command

```
gcloud compute backend-services describe <serviceName>
```

1. Ensure that `enable-logging` is enabled and `sample rate` is set to your desired level.

### Remediation:

#### From Google Cloud Console

1. From Google Cloud home open the Navigation Menu in the top left.

2. Under the `Networking` heading select `Network services`.
3. Select the HTTPS load-balancer you wish to audit.
4. Select `Edit` then `Backend Configuration`.
5. Select `Edit` on the corresponding backend service.
6. Click `Enable Logging`.
7. Set `Sample Rate` to a desired value. This is a percentage as a decimal point. 1.0 is 100%.

## From Google Cloud CLI

1. Run the following command

```
gcloud compute backend-services update <serviceName> --region=REGION --enable-logging --logging-sample-rate=<percentageAsADecimal>
```







## Default Value:

By default logging for https load balancing is disabled. When logging is enabled it sets the default sample rate as 1.0 or 100%. Ensure this value fits the need of your organization to avoid high storage costs.

## References:

1. <https://cloud.google.com/load-balancing/>
2. <https://cloud.google.com/load-balancing/docs/https/https-logging-monitoring#gcloud:-global-mode>
3. <https://cloud.google.com/sdk/gcloud/reference/compute/backend-services/>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			

## 3 Networking

This section covers recommendations addressing networking on Google Cloud Platform.

### 3.1 Ensure That the Default Network Does Not Exist in a Project (Automated)

#### Profile Applicability:

- Level 2

#### Description:

To prevent use of `default` network, a project should not have a `default` network.

#### Rationale:

The `default` network has a preconfigured network configuration and automatically generates the following insecure firewall rules:

- `default-allow-internal`: Allows ingress connections for all protocols and ports among instances in the network.
- `default-allow-ssh`: Allows ingress connections on TCP port 22(SSH) from any source to any instance in the network.
- `default-allow-rdp`: Allows ingress connections on TCP port 3389(RDP) from any source to any instance in the network.
- `default-allow-icmp`: Allows ingress ICMP traffic from any source to any instance in the network.

These automatically created firewall rules do not get audit logged by default.

Furthermore, the default network is an auto mode network, which means that its subnets use the same predefined range of IP addresses, and as a result, it's not possible to use Cloud VPN or VPC Network Peering with the default network.

Based on organization security and networking requirements, the organization should create a new network and delete the `default` network.

#### Impact:

When an organization deletes the default network, it will need to remove all assets from that network and migrate them to a new network.

#### Audit:

##### From Google Cloud Console

1. Go to the `VPC networks` page by visiting:  
<https://console.cloud.google.com/networking/networks/list>.
2. Ensure that a network with the name `default` is not present.

##### From Google Cloud CLI

1. Set the project name in the Google Cloud Shell:

```
gcloud config set project PROJECT_ID
```

2. List the networks configured in that project:

```
gcloud compute networks list
```

It should not list `default` as one of the available networks in that project.

### Remediation:

#### From Google Cloud Console

1. Go to the `VPC networks` page by visiting:  
<https://console.cloud.google.com/networking/networks/list>.
2. Click the network named `default`.
3. On the network detail page, click `EDIT`.
4. Click `DELETE VPC NETWORK`.
5. If needed, create a new network to replace the default network.

#### From Google Cloud CLI

For each Google Cloud Platform project,

1. Delete the default network:

```
gcloud compute networks delete default
```

2. If needed, create a new network to replace it:

```
gcloud compute networks create NETWORK_NAME
```

### Prevention:

The user can prevent the default network and its insecure default firewall rules from being created by setting up an Organization Policy to `Skip default network creation` at <https://console.cloud.google.com/iam-admin/orgpolicies/compute-skipDefaultNetworkCreation>.

### Default Value:

By default, for each project, a `default` network is created.






### References:

1. [https://cloud.google.com/compute/docs/networking#firewall\\_rules](https://cloud.google.com/compute/docs/networking#firewall_rules)
2. <https://cloud.google.com/compute/docs/reference/latest/networks/insert>
3. <https://cloud.google.com/compute/docs/reference/latest/networks/delete>
4. <https://cloud.google.com/vpc/docs/firewall-rules-logging>



5. <https://cloud.google.com/vpc/docs/vpc#default-network>
6. <https://cloud.google.com/sdk/gcloud/reference/compute/networks/delete>

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</u></b></p> <p>Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v7	<p><b><u>11.1 Maintain Standard Security Configurations for Network Devices</u></b></p> <p>Maintain standard, documented security configuration standards for all authorized network devices.</p>			

## 3.2 Ensure Legacy Networks Do Not Exist for Older Projects (Automated)

### Profile Applicability:

- Level 1

### Description:

In order to prevent use of legacy networks, a project should not have a legacy network configured. As of now, Legacy Networks are gradually being phased out, and you can no longer create projects with them. This recommendation is to check older projects to ensure that they are not using Legacy Networks.

### Rationale:

Legacy networks have a single network IPv4 prefix range and a single gateway IP address for the whole network. The network is global in scope and spans all cloud regions. Subnetworks cannot be created in a legacy network and are unable to switch from legacy to auto or custom subnet networks. Legacy networks can have an impact for high network traffic projects and are subject to a single point of contention or failure.

### Impact:

None.

### Audit:

#### From Google Cloud CLI

For each Google Cloud Platform project,

1. Set the project name in the Google Cloud Shell:

```
gcloud config set project <Project-ID>
```

2. List the networks configured in that project:

```
gcloud compute networks list
```

None of the listed networks should be in the `legacy` mode.

### Remediation:

#### From Google Cloud CLI

For each Google Cloud Platform project,

1. Follow the documentation and create a non-legacy network suitable for the organization's requirements.

2. Follow the documentation and delete the networks in the `legacy` mode.






**Default Value:**

By default, networks are not created in the `legacy` mode.

**References:**

1. [https://cloud.google.com/vpc/docs/using-legacy#creating\\_a\\_legacy\\_network](https://cloud.google.com/vpc/docs/using-legacy#creating_a_legacy_network)
2. [https://cloud.google.com/vpc/docs/using-legacy#deleting\\_a\\_legacy\\_network](https://cloud.google.com/vpc/docs/using-legacy#deleting_a_legacy_network)

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</u></b> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b><u>11.1 Maintain Standard Security Configurations for Network Devices</u></b> Maintain standard, documented security configuration standards for all authorized network devices.			

### 3.3 Ensure That DNSSEC Is Enabled for Cloud DNS (Automated)

#### Profile Applicability:

- Level 1

#### Description:

Cloud Domain Name System (DNS) is a fast, reliable and cost-effective domain name system that powers millions of domains on the internet. Domain Name System Security Extensions (DNSSEC) in Cloud DNS enables domain owners to take easy steps to protect their domains against DNS hijacking and man-in-the-middle and other attacks.

#### Rationale:

Domain Name System Security Extensions (DNSSEC) adds security to the DNS protocol by enabling DNS responses to be validated. Having a trustworthy DNS that translates a domain name like [www.example.com](http://www.example.com) into its associated IP address is an increasingly important building block of today's web-based applications. Attackers can hijack this process of domain/IP lookup and redirect users to a malicious site through DNS hijacking and man-in-the-middle attacks. DNSSEC helps mitigate the risk of such attacks by cryptographically signing DNS records. As a result, it prevents attackers from issuing fake DNS responses that may misdirect browsers to nefarious websites.

#### Audit:

##### From Google Cloud Console

1. Go to Cloud DNS by visiting <https://console.cloud.google.com/net-services/dns/zones>.
2. For each zone of Type Public, ensure that DNSSEC is set to On.

##### From Google Cloud CLI

1. List all the Managed Zones in a project:

```
gcloud dns managed-zones list
```

2. For each zone of VISIBILITY public, get its metadata:

```
gcloud dns managed-zones describe ZONE_NAME
```

3. Ensure that `dnssecConfig.state` property is on.

#### Remediation:

##### From Google Cloud Console

1. Go to Cloud DNS by visiting <https://console.cloud.google.com/net-services/dns/zones>.
2. For each zone of Type Public, set DNSSEC to On.

### From Google Cloud CLI

Use the below command to enable DNSSEC for Cloud DNS Zone Name.

```
gcloud dns managed-zones update ZONE_NAME --dnssec-state on
```






### Default Value:

By default DNSSEC is not enabled.

### References:

1. <https://cloudplatform.googleblog.com/2017/11/DNSSEC-now-available-in-Cloud-DNS.html>
2. <https://cloud.google.com/dns/dnssec-config#enabling>
3. <https://cloud.google.com/dns/dnssec>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</b> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b>11.1 Maintain Standard Security Configurations for Network Devices</b> Maintain standard, documented security configuration standards for all authorized network devices.			

### *3.4 Ensure That RSASHA1 Is Not Used for the Key-Signing Key in Cloud DNS DNSSEC (Automated)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

NOTE: Currently, the SHA1 algorithm has been removed from general use by Google, and, if being used, needs to be whitelisted on a project basis by Google and will also, therefore, require a Google Cloud support contract.

DNSSEC algorithm numbers in this registry may be used in CERT RRs. Zone signing (DNSSEC) and transaction security mechanisms (SIG(0) and TSIG) make use of particular subsets of these algorithms. The algorithm used for key signing should be a recommended one and it should be strong.

#### **Rationale:**

Domain Name System Security Extensions (DNSSEC) algorithm numbers in this registry may be used in CERT RRs. Zonesigning (DNSSEC) and transaction security mechanisms (SIG(0) and TSIG) make use of particular subsets of these algorithms.

The algorithm used for key signing should be a recommended one and it should be strong. When enabling DNSSEC for a managed zone, or creating a managed zone with DNSSEC, the user can select the DNSSEC signing algorithms and the denial-of-existence type. Changing the DNSSEC settings is only effective for a managed zone if DNSSEC is not already enabled. If there is a need to change the settings for a managed zone where it has been enabled, turn DNSSEC off and then re-enable it with different settings.

#### **Audit:**

##### **From Google Cloud CLI**

Ensure the property algorithm for keyType keySigning is not using RSASHA1.

```
gcloud dns managed-zones describe ZONENAME --  
format="json(dnsName,dnssecConfig.state,dnssecConfig.defaultKeySpecs) "
```

#### **Remediation:**

##### **From Google Cloud CLI**

1. If it is necessary to change the settings for a managed zone where it has been enabled, DNSSEC must be turned off and re-enabled with different settings. To turn off DNSSEC, run the following command:

```
gcloud dns managed-zones update ZONE_NAME --dnssec-state off
```

2. To update key-signing for a reported managed DNS Zone, run the following command:

```
gcloud dns managed-zones update ZONE_NAME --dnssec-state on --ksk-algorithm KSK_ALGORITHM --ksk-key-length KSK_KEY_LENGTH --zsk-algorithm ZSK_ALGORITHM --zsk-key-length ZSK_KEY_LENGTH --denial-of-existence DENIAL_OF_EXISTENCE
```

Supported algorithm options and key lengths are as follows.

Algorithm	KSK Length	ZSK Length
-----	-----	-----
RSASHA1	1024,2048	1024,2048
RSASHA256	1024,2048	1024,2048
RSASHA512	1024,2048	1024,2048
ECDSAP256SHA256	256	256
ECDSAP384SHA384	384	384






## References:

1. [https://cloud.google.com/dns/dnssec-advanced#advanced\\_signing\\_options](https://cloud.google.com/dns/dnssec-advanced#advanced_signing_options)

## Additional Information:

1. RSASHA1 key-signing support may be required for compatibility reasons.
2. Remediation CLI works well with gcloud-cli version 221.0.0 and later.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</u></b> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b><u>11.1 Maintain Standard Security Configurations for Network Devices</u></b> Maintain standard, documented security configuration standards for all authorized network devices.			

### *3.5 Ensure That RSASHA1 Is Not Used for the Zone-Signing Key in Cloud DNS DNSSEC (Automated)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

NOTE: Currently, the SHA1 algorithm has been removed from general use by Google, and, if being used, needs to be whitelisted on a project basis by Google and will also, therefore, require a Google Cloud support contract.

DNSSEC algorithm numbers in this registry may be used in CERT RRs. Zone signing (DNSSEC) and transaction security mechanisms (SIG(0) and TSIG) make use of particular subsets of these algorithms. The algorithm used for key signing should be a recommended one and it should be strong.

#### **Rationale:**

DNSSEC algorithm numbers in this registry may be used in CERT RRs. Zone signing (DNSSEC) and transaction security mechanisms (SIG(0) and TSIG) make use of particular subsets of these algorithms.

The algorithm used for key signing should be a recommended one and it should be strong. When enabling DNSSEC for a managed zone, or creating a managed zone with DNSSEC, the DNSSEC signing algorithms and the denial-of-existence type can be selected. Changing the DNSSEC settings is only effective for a managed zone if DNSSEC is not already enabled. If the need exists to change the settings for a managed zone where it has been enabled, turn DNSSEC off and then re-enable it with different settings.

#### **Audit:**

##### **From Google Cloud CLI**

Ensure the property algorithm for keyType zone signing is not using RSASHA1.

```
gcloud dns managed-zones describe --  
format="json(dnsName,dnssecConfig.state,dnssecConfig.defaultKeySpecs)"
```

#### **Remediation:**

##### **From Google Cloud CLI**

1. If the need exists to change the settings for a managed zone where it has been enabled, DNSSEC must be turned off and then re-enabled with different settings. To turn off DNSSEC, run following command:



```
gcloud dns managed-zones update ZONE_NAME --dnssec-state off
```

2. To update zone-signing for a reported managed DNS Zone, run the following command:

```
gcloud dns managed-zones update ZONE_NAME --dnssec-state on --ksk-algorithm KSK_ALGORITHM --ksk-key-length KSK_KEY_LENGTH --zsk-algorithm ZSK_ALGORITHM --zsk-key-length ZSK_KEY_LENGTH --denial-of-existence DENIAL_OF_EXISTENCE
```

Supported algorithm options and key lengths are as follows.

Algorithm	KSK Length	ZSK Length
-----	-----	-----
RSASHA1	1024,2048	1024,2048
RSASHA256	1024,2048	1024,2048
RSASHA512	1024,2048	1024,2048
ECDSAP256SHA256	256	384
ECDSAP384SHA384	384	384






## References:

1. [https://cloud.google.com/dns/dnssec-advanced#advanced\\_signing\\_options](https://cloud.google.com/dns/dnssec-advanced#advanced_signing_options)

## Additional Information:

1. RSASHA1 zone-signing support may be required for compatibility reasons.
2. The remediation CLI works well with gcloud-cli version 221.0.0 and later.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</u></b> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b><u>11.1 Maintain Standard Security Configurations for Network Devices</u></b> Maintain standard, documented security configuration standards for all authorized network devices.			

## 3.6 Ensure That SSH Access Is Restricted From the Internet (Automated)

### Profile Applicability:

- Level 2

### Description:

GCP Firewall Rules are specific to a VPC Network. Each rule either allows or denies traffic when its conditions are met. Its conditions allow the user to specify the type of traffic, such as ports and protocols, and the source or destination of the traffic, including IP addresses, subnets, and instances.

Firewall rules are defined at the VPC network level and are specific to the network in which they are defined. The rules themselves cannot be shared among networks. Firewall rules only support IPv4 traffic. When specifying a source for an ingress rule or a destination for an egress rule by address, only an IPv4 address or IPv4 block in CIDR notation can be used. Generic (0.0.0.0/0) incoming traffic from the internet to VPC or VM instance using SSH on Port 22 can be avoided.

### Rationale:

GCP Firewall Rules within a VPC Network apply to outgoing (egress) traffic from instances and incoming (ingress) traffic to instances in the network. Egress and ingress traffic flows are controlled even if the traffic stays within the network (for example, instance-to-instance communication). For an instance to have outgoing Internet access, the network must have a valid Internet gateway route or custom route whose destination IP is specified. This route simply defines the path to the Internet, to avoid the most general (0.0.0.0/0) destination IP Range specified from the Internet through SSH with the default Port 22. Generic access from the Internet to a specific IP Range needs to be restricted.

### Impact:

All Secure Shell (SSH) connections from outside of the network to the concerned VPC(s) will be blocked. There could be a business need where SSH access is required from outside of the network to access resources associated with the VPC. In that case, specific source IP(s) should be mentioned in firewall rules to white-list access to SSH port for the concerned VPC(s).

### Audit:

#### From Google Cloud Console

1. Go to VPC network.
2. Go to the Firewall Rules.
3. Ensure that Port is not equal to 22 and Action is not set to Allow.

4. Ensure IP Ranges is not equal to 0.0.0.0/0 under Source filters.

### From Google Cloud CLI

```
gcloud compute firewall-rules list --  
format=table ' (name,direction,sourceRanges,allowed) '
```

Ensure that there is no rule matching the below criteria:

- SOURCE\_RANGES is 0.0.0.0/0
- AND DIRECTION is INGRESS
- AND IPProtocol is tcp or ALL
- AND PORTS is set to 22 or range containing 22 or Null (not set)

Note:

- When ALL TCP ports are allowed in a rule, PORT does not have any value set (NULL)
- When ALL Protocols are allowed in a rule, PORT does not have any value set (NULL)

### Remediation:

#### From Google Cloud Console

1. Go to VPC Network.
2. Go to the Firewall Rules.
3. Click the Firewall Rule you want to modify.
4. Click Edit.
5. Modify Source IP ranges to specific IP.
6. Click Save.

### From Google Cloud CLI

1. Update the Firewall rule with the new SOURCE\_RANGE from the below command:

```
gcloud compute firewall-rules update FirewallName --allow=[PROTOCOL[:PORT[-  
PORT]],...] --source-ranges=[CIDR_RANGE,...]
```












### References:

1. <https://cloud.google.com/vpc/docs/firewalls#blockedtraffic>
2. <https://cloud.google.com/blog/products/identity-security/cloud-iap-enables-context-aware-access-to-vms-via-ssh-and-rdp-without-bastion-hosts>

### Additional Information:

Currently, GCP VPC only supports IPV4; however, Google is already working on adding IPV6 support for VPC. In that case along with source IP range 0.0.0.0, the rule should be checked for IPV6 equivalent ::/0 as well.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 <u>Implement and Manage a Firewall on Servers</u></b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	<b>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	<b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	<b>12.4 <u>Deny Communication over Unauthorized Ports</u></b> Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.			

## 3.7 Ensure That RDP Access Is Restricted From the Internet (Automated)

### Profile Applicability:

- Level 2

### Description:

GCP Firewall Rules are specific to a VPC Network. Each rule either allows or denies traffic when its conditions are met. Its conditions allow users to specify the type of traffic, such as ports and protocols, and the source or destination of the traffic, including IP addresses, subnets, and instances.

Firewall rules are defined at the VPC network level and are specific to the network in which they are defined. The rules themselves cannot be shared among networks. Firewall rules only support IPv4 traffic. When specifying a source for an ingress rule or a destination for an egress rule by address, an IPv4 address or IPv4 block in CIDR notation can be used. Generic (0.0.0.0/0) incoming traffic from the Internet to a VPC or VM instance using RDP on Port 3389 can be avoided.

### Rationale:

GCP Firewall Rules within a VPC Network. These rules apply to outgoing (egress) traffic from instances and incoming (ingress) traffic to instances in the network. Egress and ingress traffic flows are controlled even if the traffic stays within the network (for example, instance-to-instance communication). For an instance to have outgoing Internet access, the network must have a valid Internet gateway route or custom route whose destination IP is specified. This route simply defines the path to the Internet, to avoid the most general (0.0.0.0/0) destination IP Range specified from the Internet through RDP with the default Port 3389. Generic access from the Internet to a specific IP Range should be restricted.

### Impact:

All Remote Desktop Protocol (RDP) connections from outside of the network to the concerned VPC(s) will be blocked. There could be a business need where secure shell access is required from outside of the network to access resources associated with the VPC. In that case, specific source IP(s) should be mentioned in firewall rules to white-list access to RDP port for the concerned VPC(s).

### Audit:

#### From Google Cloud Console

1. Go to VPC network.
2. Go to the Firewall Rules.
3. Ensure Port is not equal to 3389 and Action is not Allow.

4. Ensure IP Ranges is not equal to 0.0.0.0/0 under Source filters.

### From Google Cloud CLI

```
gcloud compute firewall-rules list --  
format=table ' (name,direction,sourceRanges,allowed.ports) '
```

Ensure that there is no rule matching the below criteria:

- SOURCE\_RANGES is 0.0.0.0/0
- AND DIRECTION is INGRESS
- AND IPProtocol is TCP or ALL
- AND PORTS is set to 3389 or range containing 3389 or Null (not set)

Note:

- When ALL TCP ports are allowed in a rule, PORT does not have any value set (NULL)
- When ALL Protocols are allowed in a rule, PORT does not have any value set (NULL)

### Remediation:

#### From Google Cloud Console

1. Go to VPC Network.
2. Go to the Firewall Rules.
3. Click the Firewall Rule to be modified.
4. Click Edit.
5. Modify Source IP ranges to specific IP.
6. Click Save.

### From Google Cloud CLI

1.Update RDP Firewall rule with new SOURCE\_RANGE from the below command:

```
gcloud compute firewall-rules update FirewallName --allow=[PROTOCOL[:PORT[-  
PORT]],...] --source-ranges=[CIDR_RANGE,...]
```












### References:

1. <https://cloud.google.com/vpc/docs/firewalls#blockedtraffic>
2. <https://cloud.google.com/blog/products/identity-security/cloud-iap-enables-context-aware-access-to-vms-via-ssh-and-rdp-without-bastion-hosts>

### Additional Information:

Currently, GCP VPC only supports IPV4; however, Google is already working on adding IPV6 support for VPC. In that case along with source IP range 0.0.0.0, the rule should be checked for IPv6 equivalent ::/0 as well.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 <u>Implement and Manage a Firewall on Servers</u></b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	<b>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	<b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	<b>12.4 <u>Deny Communication over Unauthorized Ports</u></b> Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.			

### *3.8 Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network (Automated)*

#### **Profile Applicability:**

- Level 2

#### **Description:**

Flow Logs is a feature that enables users to capture information about the IP traffic going to and from network interfaces in the organization's VPC Subnets. Once a flow log is created, the user can view and retrieve its data in Stackdriver Logging. It is recommended that Flow Logs be enabled for every business-critical VPC subnet.

#### **Rationale:**

VPC networks and subnetworks not reserved for internal HTTP(S) load balancing provide logically isolated and secure network partitions where GCP resources can be launched. When Flow Logs are enabled for a subnet, VMs within that subnet start reporting on all Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) flows. Each VM samples the TCP and UDP flows it sees, inbound and outbound, whether the flow is to or from another VM, a host in the on-premises datacenter, a Google service, or a host on the Internet. If two GCP VMs are communicating, and both are in subnets that have VPC Flow Logs enabled, both VMs report the flows.

Flow Logs supports the following use cases:

- Network monitoring
- Understanding network usage and optimizing network traffic expenses
- Network forensics
- Real-time security analysis

Flow Logs provide visibility into network traffic for each VM inside the subnet and can be used to detect anomalous traffic or provide insight during security workflows.

The Flow Logs must be configured such that all network traffic is logged, the interval of logging is granular to provide detailed information on the connections, no logs are filtered, and metadata to facilitate investigations are included.

**Note:** Subnets reserved for use by internal HTTP(S) load balancers do not support VPC flow logs.

#### **Impact:**

Standard pricing for Stackdriver Logging, BigQuery, or Cloud Pub/Sub applies. VPC Flow Logs generation will be charged starting in GA as described in reference:

<https://cloud.google.com/vpc/>



## Audit:

### From Google Cloud Console

1. Go to the VPC network GCP Console visiting  
<https://console.cloud.google.com/networking/networks/list>
2. From the list of network subnets, make sure for each subnet:
  - Flow Logs is set to On
  - Aggregation Interval is set to 5 sec
  - Include metadata checkbox is checked
  - Sample rate is set to 100%

**Note:** It is not possible to determine if a Log filter has been defined from the console.

### From Google Cloud CLI

```
gcloud compute networks subnets list --format json | \
jq -r
'(["Subnet","Purpose","Flow_Logs","Aggregation_Interval","Flow_Sampling","Met
adata","Logs_Filtered"] | (., map(length*"-")),
  (.[0] |
    [
      .name,
      .purpose,
      (if has("enableFlowLogs") and .enableFlowLogs == true then
"Enabled" else "Disabled" end),
      (if has("logConfig") then .logConfig.aggregationInterval else
"N/A" end),
      (if has("logConfig") then .logConfig.flowSampling else "N/A"
end),
      (if has("logConfig") then .logConfig.metadata else "N/A" end),
      (if has("logConfig") then (.logConfig | has("filterExpr")) else
"N/A" end)
    ]
  ) |
  @tsv' | \
column -t
```

The output of the above command will list:

- each subnet
- the subnet's purpose
- a Enabled or Disabled value if Flow Logs are enabled
- the value for Aggregation Interval or N/A if disabled, the value for Flow Sampling or N/A if disabled
- the value for Metadata or N/A if disabled
- 'true' or 'false' if a Logging Filter is configured or 'N/A' if disabled.

If the subnet's purpose is PRIVATE then Flow Logs should be Enabled.

If Flow Logs is enabled then:

- `Aggregation_Interval` should be `INTERVAL_5_SEC`
- `Flow_Sampling` should be `1`
- `Metadata` should be `INCLUDE_ALL_METADATA`
- `Logs_Filtered` should be `false`.

## Remediation:

### From Google Cloud Console

1. Go to the VPC network GCP Console visiting <https://console.cloud.google.com/networking/networks/list>
2. Click the name of a subnet, The Subnet details page displays.
3. Click the `EDIT` button.
4. Set Flow Logs to On.
5. Expand the Configure Logs section.
6. Set Aggregation Interval to 5 SEC.
7. Check the box beside Include metadata.
8. Set Sample rate to 100.
9. Click Save.

**Note:** It is not possible to configure a Log filter from the console.

### From Google Cloud CLI

To enable VPC Flow Logs for a network subnet, run the following command:

```
gcloud compute networks subnets update [SUBNET_NAME] --region [REGION] --enable-flow-logs --logging-aggregation-interval=interval-5-sec --logging-flow-sampling=1 --logging-metadata=include-all
```






## Default Value:






By default, Flow Logs is set to Off when a new VPC network subnet is created.

## References:

1. [https://cloud.google.com/vpc/docs/using-flow-logs#enabling\\_vpc\\_flow\\_logging](https://cloud.google.com/vpc/docs/using-flow-logs#enabling_vpc_flow_logging)
2. <https://cloud.google.com/vpc/>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	<b>13.6 Collect Network Traffic Flow Logs</b> Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			
v7	<b>12.8 <u>Deploy NetFlow Collection on Networking Boundary Devices</u></b> Enable the collection of NetFlow and logging data on all network boundary devices.			

### 3.9 Ensure No HTTPS or SSL Proxy Load Balancers Permit SSL Policies With Weak Cipher Suites (Manual)

#### Profile Applicability:

- Level 1

#### Description:

Secure Sockets Layer (SSL) policies determine what port Transport Layer Security (TLS) features clients are permitted to use when connecting to load balancers. To prevent usage of insecure features, SSL policies should use (a) at least TLS 1.2 with the MODERN profile; or (b) the RESTRICTED profile, because it effectively requires clients to use TLS 1.2 regardless of the chosen minimum TLS version; or (3) a CUSTOM profile that does not support any of the following features:

```
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

#### Rationale:

Load balancers are used to efficiently distribute traffic across multiple servers. Both SSL proxy and HTTPS load balancers are external load balancers, meaning they distribute traffic from the Internet to a GCP network. GCP customers can configure load balancer SSL policies with a minimum TLS version (1.0, 1.1, or 1.2) that clients can use to establish a connection, along with a profile (Compatible, Modern, Restricted, or Custom) that specifies permissible cipher suites. To comply with users using outdated protocols, GCP load balancers can be configured to permit insecure cipher suites. In fact, the GCP default SSL policy uses a minimum TLS version of 1.0 and a Compatible profile, which allows the widest range of insecure cipher suites. As a result, it is easy for customers to configure a load balancer without even knowing that they are permitting outdated cipher suites.

#### Impact:

Creating more secure SSL policies can prevent clients using older TLS versions from establishing a connection.

#### Audit:

##### From Google Cloud Console

1. See all load balancers by visiting <https://console.cloud.google.com/net-services/loadbalancing/loadBalancers/list>.
2. For each load balancer for SSL (Proxy) or HTTPS, click on its name to go the Load balancer details page.

3. Ensure that each target proxy entry in the `Frontend` table has an `SSL Policy` configured.
4. Click on each SSL policy to go to its `SSL policy details` page.
5. Ensure that the SSL policy satisfies one of the following conditions:
  - has a `Min TLS` set to `TLS 1.2` and `Profile` set to `Modern profile`, or
  - has `Profile` set to `Restricted`. Note that a `Restricted` profile effectively requires clients to use `TLS 1.2` regardless of the chosen minimum TLS version, or
  - has `Profile` set to `Custom` and the following features are all disabled:

```
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

### From Google Cloud CLI

1. List all `TargetHttpsProxies` and `TargetSslProxies`.

```
gcloud compute target-https-proxies list
gcloud compute target-ssl-proxies list
```

2. For each target proxy, list its properties:

```
gcloud compute target-https-proxies describe TARGET_HTTPS_PROXY_NAME
gcloud compute target-ssl-proxies describe TARGET_SSL_PROXY_NAME
```

3. Ensure that the `sslPolicy` field is present and identifies the name of the SSL policy:

```
sslPolicy:
https://www.googleapis.com/compute/v1/projects/PROJECT_ID/global/sslPolicies/
SSL_POLICY_NAME
```

If the `sslPolicy` field is missing from the configuration, it means that the GCP default policy is used, which is insecure.

4. Describe the SSL policy:

```
gcloud compute ssl-policies describe SSL_POLICY_NAME
```

5. Ensure that the policy satisfies one of the following conditions:
  - has `Profile` set to `Modern` and `minTlsVersion` set to `TLS_1_2`, or
  - has `Profile` set to `Restricted`, or
  - has `Profile` set to `Custom` and `enabledFeatures` does not contain any of the following values:

```
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

## Remediation:

### From Google Cloud Console

If the TargetSSLProxy or TargetHttpsProxy does not have an SSL policy configured, create a new SSL policy. Otherwise, modify the existing insecure policy.

1. Navigate to the `SSL Policies` page by visiting:  
<https://console.cloud.google.com/net-security/sslpolicies>
2. Click on the name of the insecure policy to go to its `SSL policy details` page.
3. Click `EDIT`.
4. Set `Minimum TLS version` to `TLS 1.2`.
5. Set `Profile` to `Modern` or `Restricted`.
6. Alternatively, if the user selects the profile `Custom`, make sure that the following features are disabled:

```
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

### From Google Cloud CLI

1. For each insecure SSL policy, update it to use secure cyphers:

```
gcloud compute ssl-policies update NAME [--profile
COMPATIBLE|MODERN|RESTRICTED|CUSTOM] --min-tls-version 1.2 [--custom-features
FEATURES]
```

2. If the target proxy has a GCP default SSL policy, use the following command corresponding to the proxy type to update it.

```
gcloud compute target-ssl-proxies update TARGET_SSL_PROXY_NAME --ssl-policy
SSL_POLICY_NAME
gcloud compute target-https-proxies update TARGET_HTTPS_POLICY_NAME --ssl-
policy SSL_POLICY_NAME
```





### Default Value:

The GCP default SSL policy is the least secure setting: Min TLS 1.0 and Compatible profile

## References:

1. <https://cloud.google.com/load-balancing/docs/use-ssl-policies>
2. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.			

### *3.10 Use Identity Aware Proxy (IAP) to Ensure Only Traffic From Google IP Addresses are 'Allowed' (Manual)*

#### **Profile Applicability:**

- Level 2

#### **Description:**

IAP authenticates the user requests to your apps via a Google single sign in. You can then manage these users with permissions to control access. It is recommended to use both IAP permissions and firewalls to restrict this access to your apps with sensitive information.

#### **Rationale:**

IAP ensure that access to VMs is controlled by authenticating incoming requests. Access to your apps and the VMs should be restricted by firewall rules that allow only the proxy IAP IP addresses contained in the 35.235.240.0/20 subnet. Otherwise, unauthenticated requests can be made to your apps. To ensure that load balancing works correctly health checks should also be allowed.

#### **Impact:**

If firewall rules are not configured correctly, legitimate business services could be negatively impacted. It is recommended to make these changes during a time of low usage.

#### **Audit:**

#### **From Google Cloud Console**

1. For each of your apps that have IAP enabled go to the Cloud Console VPC network > Firewall rules.
2. Verify that the only rules correspond to the following values:
  - Targets: All instances in the network
  - Source IP ranges:
    - IAP Proxy Addresses 35.235.240.0/20
    - Google Health Check 130.211.0.0/22
    - Google Health Check 35.191.0.0/16
  - Protocols and ports:
    - Specified protocols and ports required for access and management of your app. For example most health check connection protocols would be covered by;
      - tcp:80 (Default HTTP Health Check port)
      - tcp:443 (Default HTTPS Health Check port)



**Note: if you have custom ports used by your load balancers, you will need to list them here**

## Remediation:

### From Google Cloud Console

1. Go to the Cloud Console [VPC network > Firewall rules](#).
2. Select the checkbox next to the following rules:
  - default-allow-http
  - default-allow-https
  - default-allow-internal
3. Click `Delete`.
4. Click `Create firewall rule` and set the following values:
  - Name: allow-iap-traffic
  - Targets: All instances in the network
  - Source IP ranges (press Enter after you paste each value in the box, copy each full CIDR IP address):
    - IAP Proxy Addresses 35.235.240.0/20
    - Google Health Check 130.211.0.0/22
    - Google Health Check 35.191.0.0/16
  - Protocols and ports:
    - Specified protocols and ports required for access and management of your app. For example most health check connection protocols would be covered by;
    - tcp:80 (Default HTTP Health Check port)
    - tcp:443 (Default HTTPS Health Check port)

**Note: if you have custom ports used by your load balancers, you will need to list them here**
5. When you're finished updating values, click `Create`.





## Default Value:

By default all traffic is allowed.

## References:

1. <https://cloud.google.com/iap/docs/concepts-overview>
2. <https://cloud.google.com/iap/docs/load-balancer-howto>
3. <https://cloud.google.com/load-balancing/docs/health-checks>
4. <https://cloud.google.com/blog/products/identity-security/cloud-iap-enables-context-aware-access-to-vms-via-ssh-and-rdp-without-bastion-hosts>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.6 <u>Centralize Account Management</u></b> Centralize account management through a directory or identity service.			
v7	<b>16.2 <u>Configure Centralized Point of Authentication</u></b> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			

## 4 Virtual Machines

This section covers recommendations addressing virtual machines on Google Cloud Platform.

## 4.1 Ensure That Instances Are Not Configured To Use the Default Service Account (Automated)

### Profile Applicability:

- Level 1

### Description:

It is recommended to configure your instance to not use the default Compute Engine service account because it has the Editor role on the project.

### Rationale:

When a default Compute Engine service account is created, it is automatically granted the Editor role (roles/editor) on your project which allows read and write access to most Google Cloud Services. This role includes a very large number of permissions. To defend against privilege escalations if your VM is compromised and prevent an attacker from gaining access to all of your project, you should either revoke the Editor role from the default Compute Engine service account or create a new service account and assign only the permissions needed by your instance. To mitigate this at scale, we strongly recommend that you disable the automatic role grant by adding a constraint to your organization policy.

The default Compute Engine service account is named `[PROJECT_NUMBER]-compute@developer.gserviceaccount.com`.

### Audit:

#### From Google Cloud Console

1. Go to the `VM instances` page by visiting:  
<https://console.cloud.google.com/compute/instances>.
2. Click on each instance name to go to its `VM instance details` page.
3. Under the section `API and identity management`, ensure that the default Compute Engine service account is not used. This account is named `[PROJECT_NUMBER]-compute@developer.gserviceaccount.com`.

#### From Google Cloud CLI

1. List the instances in your project and get details on each instance:

```
gcloud compute instances list --format=json | jq -r '. | "SA: \n([.[]].serviceAccounts[[]].email) Name: \n([.[]].name) "'
```

2. Ensure that the service account section has an email that does not match the pattern `[PROJECT_NUMBER]-compute@developer.gserviceaccount.com`.

**Exception:**

VMs created by GKE should be excluded. These VMs have names that start with `gke-` and are labeled `goog-gke-node`.

**Remediation:****From Google Cloud Console**

1. Go to the VM instances page by visiting:  
<https://console.cloud.google.com/compute/instances>.
2. Click on the instance name to go to its VM instance details page.
3. Click `STOP` and then click `EDIT`.
4. Under the section `API and identity management`, select a service account other than the default Compute Engine service account. You may first need to create a new service account.
5. Click `Save` and then click `START`.

**From Google Cloud CLI**

1. Stop the instance:

```
gcloud compute instances stop <INSTANCE_NAME>
```

2. Update the instance:

```
gcloud compute instances set-service-account <INSTANCE_NAME> --service-account=<SERVICE_ACCOUNT>
```

3. Restart the instance:

```
gcloud compute instances start <INSTANCE_NAME>
```






**Default Value:**

By default, Compute instances are configured to use the default Compute Engine service account.

**References:**

1. <https://cloud.google.com/compute/docs/access/service-accounts>
2. <https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances>
3. <https://cloud.google.com/sdk/gcloud/reference/compute/instances/set-service-account>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.7 Manage Default Accounts on Enterprise Assets and Software</u></b> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			
v7	<b><u>4.7 Limit Access to Script Tools</u></b> Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.			

## 4.2 Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs (Automated)

### Profile Applicability:

- Level 1

### Description:

To support principle of least privileges and prevent potential privilege escalation it is recommended that instances are not assigned to default service account `Compute Engine default service account` with `Scope Allow full access to all Cloud APIs`.

### Rationale:

Along with ability to optionally create, manage and use user managed custom service accounts, Google Compute Engine provides default service account `Compute Engine default service account` for an instances to access necessary cloud services. `Project Editor` role is assigned to `Compute Engine default service account` hence, This service account has almost all capabilities over all cloud services except billing. However, when `Compute Engine default service account` assigned to an instance it can operate in 3 scopes.

1. Allow default access: Allows only minimum access required to run an Instance (Least Privileges)
2. Allow full access to all Cloud APIs: Allow full access to all the cloud APIs/Services (Too much access)
3. Set access for each API: Allows Instance administrator to choose only those APIs that are needed to perform specific business functionality expected by instance

When an instance is configured with `Compute Engine default service account` with `Scope Allow full access to all Cloud APIs`, based on IAM roles assigned to the user(s) accessing Instance, it may allow user to perform cloud operations/API calls that user is not supposed to perform leading to successful privilege escalation.

### Impact:

In order to change service account or scope for an instance, it needs to be stopped.

### Audit:

#### From Google Cloud Console

1. Go to the `VM instances` page by visiting:  
<https://console.cloud.google.com/compute/instances>.
2. Click on each instance name to go to its `VM instance details` page.

3. Under the `API` and identity management, ensure that `Cloud API` access scopes is not set to `Allow full access to all Cloud APIs`.

## From Google Cloud CLI

1. List the instances in your project and get details on each instance:

```
gcloud compute instances list --format=json | jq -r ' . | "SA Scopes: \n([].serviceAccounts[].scopes) Name: \n([].name) Email: \n([].serviceAccounts[].email) "'
```

2. Ensure that the service account section has an email that does not match the pattern `[PROJECT_NUMBER]-compute@developer.gserviceaccount.com`.

### Exception:

VMs created by GKE should be excluded. These VMs have names that start with `gke-` and are labeled `goog-gke-node`

### Remediation:

## From Google Cloud Console

1. Go to the `VM instances` page by visiting:  
<https://console.cloud.google.com/compute/instances>.
2. Click on the impacted VM instance.
3. If the instance is not stopped, click the `Stop` button. Wait for the instance to be stopped.
4. Next, click the `Edit` button.
5. Scroll down to the `Service Account` section.
6. Select a different service account or ensure that `Allow full access to all Cloud APIs` is not selected.
7. Click the `Save` button to save your changes and then click `START`.

## From Google Cloud CLI

1. Stop the instance:

```
gcloud compute instances stop <INSTANCE_NAME>
```

2. Update the instance:

```
gcloud compute instances set-service-account <INSTANCE_NAME> --service-account=<SERVICE_ACCOUNT> --scopes [SCOPE1, SCOPE2...]
```

3. Restart the instance:



```
gcloud compute instances start <INSTANCE_NAME>
```

### Default Value:

While creating an VM instance, default service account is used with scope `Allow default access`.






### References:

1. <https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances>
2. <https://cloud.google.com/compute/docs/access/service-accounts>

### Additional Information:

- User IAM roles will override service account scope but configuring minimal scope ensures defense in depth
- Non-default service accounts do not offer selection of access scopes like default service account. IAM roles with non-default service accounts should be used to control VM access.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.7 Manage Default Accounts on Enterprise Assets and Software</u></b> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			
v7	<b><u>4.7 Limit Access to Script Tools</u></b> Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.			

## 4.3 Ensure “Block Project-Wide SSH Keys” Is Enabled for VM Instances (Automated)

### Profile Applicability:

- Level 1

### Description:

It is recommended to use Instance specific SSH key(s) instead of using common/shared project-wide SSH key(s) to access Instances.

### Rationale:

Project-wide SSH keys are stored in Compute/Project-meta-data. Project wide SSH keys can be used to login into all the instances within project. Using project-wide SSH keys eases the SSH key management but if compromised, poses the security risk which can impact all the instances within project. It is recommended to use Instance specific SSH keys which can limit the attack surface if the SSH keys are compromised.

### Impact:

Users already having Project-wide ssh key pairs and using third party SSH clients will lose access to the impacted Instances. For Project users using gcloud or GCP Console based SSH option, no manual key creation and distribution is required and will be handled by GCE (Google Compute Engine) itself. To access Instance using third party SSH clients Instance specific SSH key pairs need to be created and distributed to the required users.

### Audit:

#### From Google Cloud Console

1. Go to the `VM instances` page by visiting <https://console.cloud.google.com/compute/instances>. It will list all the instances in your project.
2. For every instance, click on the name of the instance.
3. Under `SSH Keys`, ensure `Block project-wide SSH keys` is selected.

#### From Google Cloud CLI

1. List the instances in your project and get details on each instance:

```
gcloud compute instances list --format=json
```

2. Ensure `key: block-project-ssh-keys` is set to value: `'true'`.

## Remediation:

### From Google Cloud Console

1. Go to the VM instances page by visiting: <https://console.cloud.google.com/compute/instances>. It will list all the instances in your project.
2. Click on the name of the Impacted instance
3. Click **Edit** in the toolbar
4. Under SSH Keys, go to the **Block project-wide SSH keys** checkbox
5. To block users with project-wide SSH keys from connecting to this instance, select **Block project-wide SSH keys**
6. Click **Save** at the bottom of the page
7. Repeat steps for every impacted Instance

### From Google Cloud CLI

To block project-wide public SSH keys, set the metadata value to `TRUE`:

```
gcloud compute instances add-metadata <INSTANCE_NAME> --metadata block-project-ssh-keys=TRUE
```

### Default Value:

By Default **Block Project-wide SSH keys** is not enabled.






### References:





1. <https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys>
2. <https://cloud.google.com/sdk/gcloud/reference/topic/formats>

### Additional Information:

If OS Login is enabled, SSH keys in instance metadata are ignored, and therefore blocking project-wide SSH keys is not necessary.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 Encrypt Sensitive Data in Transit</b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<b>4.4 <u>Use Unique Passwords</u></b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			
v7	<b>16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u></b> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

## 4.4 Ensure Oslogin Is Enabled for a Project (Automated)

### Profile Applicability:

- Level 1

### Description:

Enabling OS login binds SSH certificates to IAM users and facilitates effective SSH certificate management.

### Rationale:

Enabling osLogin ensures that SSH keys used to connect to instances are mapped with IAM users. Revoking access to IAM user will revoke all the SSH keys associated with that particular user. It facilitates centralized and automated SSH key pair management which is useful in handling cases like response to compromised SSH key pairs and/or revocation of external/third-party/Vendor users.

### Impact:

Enabling OS Login on project disables metadata-based SSH key configurations on all instances from a project. Disabling OS Login restores SSH keys that you have configured in project or instance meta-data.

### Audit:

#### From Google Cloud Console

1. Go to the VM compute metadata page by visiting <https://console.cloud.google.com/compute/metadata>.
2. Ensure that key `enable-oslogin` is present with value set to `TRUE`.
3. Because instances can override project settings, ensure that no instance has custom metadata with key `enable-oslogin` and value `FALSE`.

#### From Google Cloud CLI

1. List the instances in your project and get details on each instance:

```
gcloud compute instances list --format=json
```

2. Verify that the section `commonInstanceMetadata` has a key `enable-oslogin` set to value `TRUE`.

#### Exception:

VMs created by GKE should be excluded. These VMs have names that start with `gke-` and are labeled `goog-gke-node`

## Remediation:

### From Google Cloud Console

1. Go to the VM compute metadata page by visiting:  
<https://console.cloud.google.com/compute/metadata>.
2. Click `Edit`.
3. Add a metadata entry where the key is `enable-oslogin` and the value is `TRUE`.
4. Click `Save` to apply the changes.
5. For every instance that overrides the project setting, go to the `VM Instances` page at <https://console.cloud.google.com/compute/instances>.
6. Click the name of the instance on which you want to remove the metadata value.
7. At the top of the instance details page, click `Edit` to edit the instance settings.
8. Under `Custom metadata`, remove any entry with key `enable-oslogin` and the value is `FALSE`.
9. At the bottom of the instance details page, click `Save` to apply your changes to the instance.

### From Google Cloud CLI

1. Configure oslogin on the project:

```
gcloud compute project-info add-metadata --metadata enable-oslogin=TRUE
```

2. Remove instance metadata that overrides the project setting.

```
gcloud compute instances remove-metadata <INSTANCE_NAME> --keys=enable-oslogin
```

Optionally, you can enable two factor authentication for OS login. For more information, see: <https://cloud.google.com/compute/docs/oslogin/setup-two-factor-authentication>.

### Default Value:

By default, parameter `enable-oslogin` is not set, which is equivalent to setting it to `FALSE`.

### References:

1. <https://cloud.google.com/compute/docs/instances/managing-instance-access>
2. [https://cloud.google.com/compute/docs/instances/managing-instance-access#enable\\_oslogin](https://cloud.google.com/compute/docs/instances/managing-instance-access#enable_oslogin)
3. <https://cloud.google.com/sdk/gcloud/reference/compute/instances/remove-metadata>
4. <https://cloud.google.com/compute/docs/oslogin/setup-two-factor-authentication>

### Additional Information:

1. In order to use osLogin, instance using Custom Images must have the latest version of the Linux Guest Environment installed. The following image families do not yet support OS Login:

Project cos-cloud (Container-Optimized OS) image family cos-stable.







All project coreos-cloud (CoreOS) image families

Project suse-cloud (SLES) image family sles-11

All Windows Server and SQL Server image families

2. Project enable-oslogin can be over-riden by setting enable-oslogin parameter to an instance metadata individually.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.6 Centralize Account Management</b> Centralize account management through a directory or identity service.			
v8	<b>6.7 Centralize Access Control</b> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.			
v7	<b>16.2 Configure Centralized Point of Authentication</b> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			

## 4.5 Ensure 'Enable Connecting to Serial Ports' Is Not Enabled for VM Instance (Automated)

### Profile Applicability:

- Level 1

### Description:

Interacting with a serial port is often referred to as the serial console, which is similar to using a terminal window, in that input and output is entirely in text mode and there is no graphical interface or mouse support.

If you enable the interactive serial console on an instance, clients can attempt to connect to that instance from any IP address. Therefore interactive serial console support should be disabled.

### Rationale:

A virtual machine instance has four virtual serial ports. Interacting with a serial port is similar to using a terminal window, in that input and output is entirely in text mode and there is no graphical interface or mouse support. The instance's operating system, BIOS, and other system-level entities often write output to the serial ports, and can accept input such as commands or answers to prompts. Typically, these system-level entities use the first serial port (port 1) and serial port 1 is often referred to as the serial console.

The interactive serial console does not support IP-based access restrictions such as IP whitelists. If you enable the interactive serial console on an instance, clients can attempt to connect to that instance from any IP address. This allows anybody to connect to that instance if they know the correct SSH key, username, project ID, zone, and instance name.

Therefore interactive serial console support should be disabled.

### Audit:

#### From Google Cloud CLI

1. Login to Google Cloud console
2. Go to Compute Engine
3. Go to VM instances
4. Click on the Specific VM
5. Ensure the statement `Connecting to serial serial ports is disabled` is displayed at the top of the details tab, just below the `Connect to serial console` drop-down..

#### From Google Cloud Console

Ensure the below command's output shows `null`:



```
gcloud compute instances describe <vmName> --zone=<region> --format="json(metadata.items[0].key,metadata.items[0].value) "
```

or key and value properties from below command's json response are equal to serial-port-enable and 0 or false respectively.

```
{
  "metadata": {
    "items": [
      {
        "key": "serial-port-enable",
        "value": "0"
      }
    ]
  }
}
```

## Remediation:

### From Google Cloud CLI

1. Login to Google Cloud console
2. Go to Computer Engine
3. Go to VM instances
4. Click on the Specific VM
5. Click `EDIT`
6. Unselect `Enable connecting to serial ports` below `Remote access` block.
7. Click `Save`

### From Google Cloud Console

Use the below command to disable

```
gcloud compute instances add-metadata <INSTANCE_NAME> --zone=<ZONE> --metadata=serial-port-enable=false
```

or

```
gcloud compute instances add-metadata <INSTANCE_NAME> --zone=<ZONE> --metadata=serial-port-enable=0
```

## Prevention:

You can prevent VMs from having serial port access enable by `Disable VM serial port access` organization policy:

<https://console.cloud.google.com/iam-admin/orgpolicies/compute-disableSerialPortAccess>.





## Default Value:

By default, connecting to serial ports is not enabled.

## References:

1. <https://cloud.google.com/compute/docs/instances/interacting-with-serial-console>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

## 4.6 Ensure That IP Forwarding Is Not Enabled on Instances (Automated)

### Profile Applicability:

- Level 1

### Description:

Compute Engine instance cannot forward a packet unless the source IP address of the packet matches the IP address of the instance. Similarly, GCP won't deliver a packet whose destination IP address is different than the IP address of the instance receiving the packet. However, both capabilities are required if you want to use instances to help route packets.

Forwarding of data packets should be disabled to prevent data loss or information disclosure.

### Rationale:

Compute Engine instance cannot forward a packet unless the source IP address of the packet matches the IP address of the instance. Similarly, GCP won't deliver a packet whose destination IP address is different than the IP address of the instance receiving the packet. However, both capabilities are required if you want to use instances to help route packets. To enable this source and destination IP check, disable the `canIpForward` field, which allows an instance to send and receive packets with non-matching destination or source IPs.

### Impact:

Deleting instance(s) acting as routers/packet forwarders may break the network connectivity.

### Audit:

#### From Google Cloud Console

1. Go to the `VM Instances` page by visiting:  
<https://console.cloud.google.com/compute/instances>.
2. For every instance, click on its name to go to the `VM instance details` page.
3. Under the `Network interfaces` section, ensure that `IP forwarding` is set to `Off` for every network interface.

#### From Google Cloud CLI

1. List all instances:

```
gcloud compute instances list --format='table(name,canIpForward) '
```

2. Ensure that `CAN_IP_FORWARD` column in the output of above command does not contain `True` for any VM instance.

**Exception:**

Instances created by GKE should be excluded because they need to have IP forwarding enabled and cannot be changed. Instances created by GKE have names that start with "gke-".

**Remediation:**

You only edit the `canIpForward` setting at instance creation time. Therefore, you need to delete the instance and create a new one where `canIpForward` is set to `false`.

**From Google Cloud Console**

1. Go to the VM Instances page by visiting:  
<https://console.cloud.google.com/compute/instances>.
2. Select the VM Instance you want to remediate.
3. Click the Delete button.
4. On the 'VM Instances' page, click 'CREATE INSTANCE'.
5. Create a new instance with the desired configuration. By default, the instance is configured to not allow IP forwarding.

**From Google Cloud CLI**

1. Delete the instance:

```
gcloud compute instances delete INSTANCE_NAME
```

2. Create a new instance to replace it, with IP forwarding set to Off

```
gcloud compute instances create
```

**Default Value:**

By default, instances are not configured to allow IP forwarding.











**References:**

1. <https://cloud.google.com/vpc/docs/using-routes#canipforward>

**Additional Information:**

You can only set the `canIpForward` field at instance creation time. After an instance is created, the field becomes read-only.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 <u>Implement and Manage a Firewall on Servers</u></b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	<b>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	<b>11.1 <u>Maintain Standard Security Configurations for Network Devices</u></b> Maintain standard, documented security configuration standards for all authorized network devices.			
v7	<b>11.2 <u>Document Traffic Configuration Rules</u></b> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.			

## *4.7 Ensure VM Disks for Critical VMs Are Encrypted With Customer-Supplied Encryption Keys (CSEK) (Automated)*

### **Profile Applicability:**

- Level 2

### **Description:**

Customer-Supplied Encryption Keys (CSEK) are a feature in Google Cloud Storage and Google Compute Engine. If you supply your own encryption keys, Google uses your key to protect the Google-generated keys used to encrypt and decrypt your data. By default, Google Compute Engine encrypts all data at rest. Compute Engine handles and manages this encryption for you without any additional actions on your part. However, if you wanted to control and manage this encryption yourself, you can provide your own encryption keys.

### **Rationale:**

By default, Google Compute Engine encrypts all data at rest. Compute Engine handles and manages this encryption for you without any additional actions on your part. However, if you wanted to control and manage this encryption yourself, you can provide your own encryption keys.

If you provide your own encryption keys, Compute Engine uses your key to protect the Google-generated keys used to encrypt and decrypt your data. Only users who can provide the correct key can use resources protected by a customer-supplied encryption key.

Google does not store your keys on its servers and cannot access your protected data unless you provide the key. This also means that if you forget or lose your key, there is no way for Google to recover the key or to recover any data encrypted with the lost key.

At least business critical VMs should have VM disks encrypted with CSEK.

### **Impact:**

If you lose your encryption key, you will not be able to recover the data.

### **Audit:**

#### **From Google Cloud Console**

1. Go to Compute Engine `Disks` by visiting:  
<https://console.cloud.google.com/compute/disks>.
2. Click on the disk for your critical VMs to see its configuration details.
3. Ensure that `Encryption type` is set to `Customer supplied`.

## From Google Cloud CLI

Ensure `diskEncryptionKey` property in the below command's response is not null, and contains key `sha256` with corresponding value

```
gcloud compute disks describe <DISK_NAME> --zone <ZONE> --format="json(diskEncryptionKey,name)"
```

## Remediation:

Currently there is no way to update the encryption of an existing disk. Therefore you should create a new disk with `Encryption` set to `Customer supplied`.

## From Google Cloud Console

1. Go to Compute Engine `Disks` by visiting:  
<https://console.cloud.google.com/compute/disks>.
2. Click `CREATE DISK`.
3. Set `Encryption` type to `Customer supplied`,
4. Provide the `Key` in the box.
5. Select `Wrapped key`.
6. Click `Create`.

## From Google Cloud CLI

In the `gcloud compute` tool, encrypt a disk using the `--csek-key-file` flag during instance creation. If you are using an RSA-wrapped key, use the `gcloud beta` component:

```
gcloud compute instances create <INSTANCE_NAME> --csek-key-file <example-file.json>
```

To encrypt a standalone persistent disk:

```
gcloud compute disks create <DISK_NAME> --csek-key-file <example-file.json>
```

## Default Value:

By default, VM disks are encrypted with Google-managed keys. They are not encrypted with Customer-Supplied Encryption Keys.

## References:

1. [https://cloud.google.com/compute/docs/disks/customer-supplied-encryption#encrypt\\_a\\_new\\_persistent\\_disk\\_with\\_your\\_own\\_keys](https://cloud.google.com/compute/docs/disks/customer-supplied-encryption#encrypt_a_new_persistent_disk_with_your_own_keys)
2. <https://cloud.google.com/compute/docs/reference/rest/v1/disks/get>
3. [https://cloud.google.com/compute/docs/disks/customer-supplied-encryption#key\\_file](https://cloud.google.com/compute/docs/disks/customer-supplied-encryption#key_file)

## Additional Information:




**Note 1:** When you delete a persistent disk, Google discards the cipher keys, rendering the data irretrievable. This process is irreversible.

Note 2: It is up to you to generate and manage your key. You must provide a key that is a 256-bit string encoded in RFC 4648 standard base64 to Compute Engine.

Note 3: An example key file looks like this.

```
[
  {
    "uri": "https://www.googleapis.com/compute/v1/projects/myproject/zones/us-central1-a/disks/example-disk",
    "key": "acXTX3rxrKAFTF0tYVLvydU1riRZTvUNC4g5I11NY-c=",
    "key-type": "raw"
  },
  {
    "uri":
"https://www.googleapis.com/compute/v1/projects/myproject/global/snapshots/my-private-snapshot",
    "key":
"ieCx/NcW06PcT7Ep1X6LUTc/hLvUDYyzSZPPVCVPTVEohpeHASqC8uw5TzyO9U+Fka9JFHZ0mBibXUInrC/jEk014kCK/NPjYgEMOyssZ4ZINPKxlUh2zn1bV+MCaTICrdmuSBTWlUUiFoDD6PYznLwh8ZNdaheCeZ8ewEXgFQ8V+sDroLaN3Xs3MDTXQEMMoNuxMCZEIpg9Vtp9x2oeQ5lAbtt7bYAAHf5l+gJWw3sUfs0/Glw5fpdjT8Uggr+RMZezGr1tJEF293rvTIjWOEB3z5OHyHwQkvdrPDFcTqsLfh+8Hr8g+mf+7zVPEC8nEbqpd13GPv3A7AwPp7MA=="
    "key-type": "rsa-encrypted"
  }
]
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	<b>14.8 <u>Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			



## 4.8 Ensure Compute Instances Are Launched With Shielded VM Enabled (Automated)

### Profile Applicability:

- Level 2

### Description:

To defend against advanced threats and ensure that the boot loader and firmware on your VMs are signed and untampered, it is recommended that Compute instances are launched with Shielded VM enabled.

### Rationale:

Shielded VMs are virtual machines (VMs) on Google Cloud Platform hardened by a set of security controls that help defend against rootkits and bootkits.

Shielded VM offers verifiable integrity of your Compute Engine VM instances, so you can be confident your instances haven't been compromised by boot- or kernel-level malware or rootkits. Shielded VM's verifiable integrity is achieved through the use of Secure Boot, virtual trusted platform module (vTPM)-enabled Measured Boot, and integrity monitoring.

Shielded VM instances run firmware which is signed and verified using Google's Certificate Authority, ensuring that the instance's firmware is unmodified and establishing the root of trust for Secure Boot.

Integrity monitoring helps you understand and make decisions about the state of your VM instances and the Shielded VM vTPM enables Measured Boot by performing the measurements needed to create a known good boot baseline, called the integrity policy baseline. The integrity policy baseline is used for comparison with measurements from subsequent VM boots to determine if anything has changed.

Secure Boot helps ensure that the system only runs authentic software by verifying the digital signature of all boot components, and halting the boot process if signature verification fails.

### Audit:

#### From Google Cloud Console

1. Go to the `VM instances` page by visiting:  
<https://console.cloud.google.com/compute/instances>.
2. Click on the instance name to see its `VM instance details` page.
3. Under the section `Shielded VM`, ensure that `vTPM` and `Integrity Monitoring` are on.

## From Google Cloud CLI

1. For each instance in your project, get its metadata:

```
gcloud compute instances list --format=json | jq -r '. | "vTPM: \
(.[].shieldedInstanceConfig.enableVtpm) IntegrityMonitoring: \
(.[].shieldedInstanceConfig.enableIntegrityMonitoring) Name: \
(.[].name) "'
```

2. Ensure that there is a `shieldedInstanceConfig` configuration and that configuration has the `enableIntegrityMonitoring` and `enableVtpm` set to `true`. If the VM is not a Shield VM image, you will not see a `shieldedInstanceConfig` in the output.

## Remediation:

To be able turn on `Shielded VM` on an instance, your instance must use an image with `Shielded VM` support.

## From Google Cloud Console

1. Go to the `VM instances` page by visiting: <https://console.cloud.google.com/compute/instances>.
2. Click on the instance name to see its `VM instance details` page.
3. Click `STOP` to stop the instance.
4. When the instance has stopped, click `EDIT`.
5. In the `Shielded VM` section, select `Turn on vTPM` and `Turn on Integrity Monitoring`.
6. Optionally, if you do not use any custom or unsigned drivers on the instance, also select `Turn on Secure Boot`.
7. Click the `Save` button to modify the instance and then click `START` to restart it.

## From Google Cloud CLI

You can only enable `Shielded VM` options on instances that have `Shielded VM` support. For a list of `Shielded VM` public images, run the `gcloud compute images list` command with the following flags:

```
gcloud compute images list --project gce-uefi-images --no-standard-images
```

1. Stop the instance:

```
gcloud compute instances stop <INSTANCE_NAME>
```

2. Update the instance:

```
gcloud compute instances update <INSTANCE_NAME> --shielded-vtpm --shielded-vm-integrity-monitoring
```

3. Optionally, if you do not use any custom or unsigned drivers on the instance, also turn on secure boot.

```
gcloud compute instances update <INSTANCE_NAME> --shielded-vm-secure-boot
```

4. Restart the instance:

```
gcloud compute instances start <INSTANCE_NAME>
```

### Prevention:

You can ensure that all new VMs will be created with Shielded VM enabled by setting up an Organization Policy to for `Shielded VM` at <https://console.cloud.google.com/iam-admin/orgpolicies/compute-requireShieldedVm>. Learn more at: <https://cloud.google.com/security/shielded-cloud/shielded-vm#organization-policy-constraint>.

### Default Value:

By default, Compute Instances do not have Shielded VM enabled.



### References:

1. <https://cloud.google.com/compute/docs/instances/modifying-shielded-vm>
2. <https://cloud.google.com/shielded-vm>
3. <https://cloud.google.com/security/shielded-cloud/shielded-vm#organization-policy-constraint>

### Additional Information:

If you do use custom or unsigned drivers on the instance, enabling Secure Boot will cause the machine to no longer boot. Turn on Secure Boot only on instances that have been verified to not have any custom drivers installed.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	5.2 <u>Maintain Secure Images</u> Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.			

## 4.9 Ensure That Compute Instances Do Not Have Public IP Addresses (Automated)

### Profile Applicability:

- Level 2

### Description:

Compute instances should not be configured to have external IP addresses.

### Rationale:

To reduce your attack surface, Compute instances should not have public IP addresses. Instead, instances should be configured behind load balancers, to minimize the instance's exposure to the internet.

### Impact:

Removing the external IP address from your Compute instance may cause some applications to stop working.

### Audit:

#### From Google Cloud Console

1. Go to the `VM instances` page by visiting:  
<https://console.cloud.google.com/compute/instances>.
2. For every VM, ensure that there is no `External IP` configured.

#### From Google Cloud CLI

```
gcloud compute instances list --format=json
```

1. The output should not contain an `accessConfigs` section under `networkInterfaces`. Note that the `natIP` value is present only for instances that are running or for instances that are stopped but have a static IP address. For instances that are stopped and are configured to have an ephemeral public IP address, the `natIP` field will not be present. Example output:

```
networkInterfaces:
- accessConfigs:
  - kind: compute#accessConfig
    name: External NAT
    networkTier: STANDARD
    type: ONE_TO_ONE_NAT
```

### Exception:

Instances created by GKE should be excluded because some of them have external IP addresses and cannot be changed by editing the instance settings. Instances created by GKE should be excluded. These instances have names that start with "gke-" and are labeled "goog-gke-node".

### Remediation:

#### From Google Cloud Console

1. Go to the VM instances page by visiting:  
<https://console.cloud.google.com/compute/instances>.
2. Click on the instance name to go to the Instance detail page.
3. Click Edit.
4. For each Network interface, ensure that External IP is set to None.
5. Click Done and then click Save.

#### From Google Cloud CLI

1. Describe the instance properties:

```
gcloud compute instances describe <INSTANCE_NAME> --zone=<ZONE>
```

2. Identify the access config name that contains the external IP address. This access config appears in the following format:

```
networkInterfaces:
- accessConfigs:
  - kind: compute#accessConfig
    name: External NAT
    natIP: 130.211.181.55
    type: ONE_TO_ONE_NAT
```

3. Delete the access config.

```
gcloud compute instances delete-access-config <INSTANCE_NAME> --zone=<ZONE> -  
-access-config-name <ACCESS_CONFIG_NAME>
```

In the above example, the `ACCESS_CONFIG_NAME` is `External NAT`. The name of your access config might be different.

#### Prevention:

You can configure the `Define allowed external IPs for VM instances` Organization Policy to prevent VMs from being configured with public IP addresses. Learn more at: <https://console.cloud.google.com/orgpolicies/compute-vmExternallpAccess>

#### Default Value:

By default, Compute instances have a public IP address.

#### References:




1. [https://cloud.google.com/load-balancing/docs/backend-service#backends\\_and\\_external\\_ip\\_addresses](https://cloud.google.com/load-balancing/docs/backend-service#backends_and_external_ip_addresses)
2. <https://cloud.google.com/compute/docs/instances/connecting-advanced#sshbetweeninstances>
3. <https://cloud.google.com/compute/docs/instances/connecting-to-instance>
4. [https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address#unassign\\_ip](https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address#unassign_ip)
5. <https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints>




#### Additional Information:

You can connect to Linux VMs that do not have public IP addresses by using Identity-Aware Proxy for TCP forwarding. Learn more at <https://cloud.google.com/compute/docs/instances/connecting-advanced#sshbetweeninstances>

For Windows VMs, see <https://cloud.google.com/compute/docs/instances/connecting-to-instance>.

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><b>14.6 <u>Protect Information through Access Control Lists</u></b></p> <p>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.</p>			

## 4.10 Ensure That App Engine Applications Enforce HTTPS Connections (Manual)

### Profile Applicability:

- Level 2

### Description:

In order to maintain the highest level of security all connections to an application should be secure by default.

### Rationale:

Insecure HTTP connections maybe subject to eavesdropping which can expose sensitive data.

### Impact:

All connections to appengine will automatically be redirected to the HTTPS endpoint ensuring that all connections are secured by TLS.

### Audit:

Verify that the app.yaml file controlling the application contains a line which enforces secure connections. For example

```
handlers:
- url: /*
  secure: always
  redirect_http_response_code: 301
  script: auto
```

<https://cloud.google.com/appengine/docs/standard/python3/config/appref>

### Remediation:

Add a line to the app.yaml file controlling the application which enforces secure connections. For example

```
handlers:
- url: /*
  **secure: always**
  redirect_http_response_code: 301
  script: auto
```

[<https://cloud.google.com/appengine/docs/standard/python3/config/appref>]

### Default Value:







By default both HTTP and HTTPS are supported



## References:

1. <https://cloud.google.com/appengine/docs/standard/python3/config/appref>
2. <https://cloud.google.com/appengine/docs/flexible/nodejs/configuring-your-app-with-yaml>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	<b>16.11 <u>Leverage Vetted Modules or Services for Application Security Components</u></b> Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.			
v7	<b>18.5 <u>Use Only Standardized and Extensively Reviewed Encryption Algorithms</u></b> Use only standardized and extensively reviewed encryption algorithms.			

## 4.11 Ensure That Compute Instances Have Confidential Computing Enabled (Automated)

### Profile Applicability:

- Level 2

### Description:

Google Cloud encrypts data at-rest and in-transit, but customer data must be decrypted for processing. Confidential Computing is a breakthrough technology which encrypts data in-use—while it is being processed. Confidential Computing environments keep data encrypted in memory and elsewhere outside the central processing unit (CPU).

Confidential VMs leverage the Secure Encrypted Virtualization (SEV) feature of AMD EPYC™ CPUs. Customer data will stay encrypted while it is used, indexed, queried, or trained on. Encryption keys are generated in hardware, per VM, and not exportable. Thanks to built-in hardware optimizations of both performance and security, there is no significant performance penalty to Confidential Computing workloads.

### Rationale:

Confidential Computing enables customers' sensitive code and other data encrypted in memory during processing. Google does not have access to the encryption keys. Confidential VM can help alleviate concerns about risk related to either dependency on Google infrastructure or Google insiders' access to customer data in the clear.

### Impact:

- Confidential Computing for Compute instances does not support live migration. Unlike regular Compute instances, Confidential VMs experience disruptions during maintenance events like a software or hardware update.
- Additional charges may be incurred when enabling this security feature. See <https://cloud.google.com/compute/confidential-vm/pricing> for more info.

### Audit:

Note: Confidential Computing is currently only supported on N2D and C2D machines. To learn more about features supported by types of machines, visit <https://cloud.google.com/compute/docs/machine-types>

### From Google Cloud Console

1. Go to the `VM instances` page by visiting: <https://console.cloud.google.com/compute/instances>.
2. Click on the instance name to see its VM instance details page.
3. Ensure that `Confidential VM service` is `Enabled`.

## From Google Cloud CLI

1. List the instances in your project and get details on each instance:

```
gcloud compute instances list --format=json
```

2. Ensure that `enableConfidentialCompute` is set to `true` for all instances with machine type starting with "n2d-".

```
confidentialInstanceConfig:  
  enableConfidentialCompute: true
```

### Remediation:

Confidential Computing can only be enabled when an instance is created. You must delete the current instance and create a new one.

## From Google Cloud Console

1. Go to the VM instances page by visiting:  
<https://console.cloud.google.com/compute/instances>.
2. Click `CREATE INSTANCE`.
3. Fill out the desired configuration for your instance.
4. Under the `Confidential VM service` section, check the option `Enable the Confidential Computing service on this VM instance`.
5. Click `Create`.

## From Google Cloud CLI

Create a new instance with Confidential Compute enabled.

```
gcloud compute instances create <INSTANCE_NAME> --zone <ZONE> --  
confidential-compute --maintenance-policy=TERMINATE
```




### Default Value:

By default, Confidential Computing is disabled for Compute instances.

### References:

1. <https://cloud.google.com/compute/confidential-vm/docs/creating-cvm-instance>
2. <https://cloud.google.com/compute/confidential-vm/docs/about-cvm>
3. <https://cloud.google.com/confidential-computing>
4. <https://cloud.google.com/blog/products/identity-security/introducing-google-cloud-confidential-computing-with-confidential-vms>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	<b>14.8 <u>Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

## 4.12 Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects (Manual)

### Profile Applicability:

- Level 2

### Description:

Google Cloud Virtual Machines have the ability via an OS Config agent API to periodically (about every 10 minutes) report OS inventory data. A patch compliance API periodically reads this data, and cross references metadata to determine if the latest updates are installed.

This is not the only Patch Management solution available to your organization and you should weigh your needs before committing to using this method.

### Rationale:

Keeping virtual machine operating systems up to date is a security best practice. Using this service will simplify this process.

### Impact:

Most Operating Systems require a restart or changing critical resources to apply the updates. Using the Google Cloud VM manager for its OS Patch management will incur additional costs for each VM managed by it. Please view the VM manager pricing reference for further information.

### Audit:

#### From Google Cloud Console

#### Determine if OS Config API is Enabled for the Project

1. Navigate into a project. In the expanded navigation menu located at the top left of the screen hover over `APIs & Services`. Then in the menu right of that select `API Libraries`
2. Search for "VM Manager (OS Config API) or scroll down in the left hand column and select the filter labeled "Compute" where it is the last listed. Open this API.
3. Verify the blue button at the top is enabled.

#### Determine if VM Instances have correct metadata tags for OSConfig parsing

1. From the main Google Cloud console, open the hamburger menu in the top left. Mouse over Computer Engine to expand the menu next to it.
2. Under the "Settings" heading, select "Metadata".
3. In this view there will be a list of the project wide metadata tags for VMs. Determine if the tag "enable-osconfig" is set to "true".

## **Determine if the Operating System of VM Instances have the local OS-Config Agent running**

There is no way to determine this from the Google Cloud console. The only way is to run operating specific commands locally inside the operating system via remote connection. For the sake of brevity of this recommendation please view the docs/troubleshooting/vm-manager/verify-setup reference at the bottom of the page. If you initialized your VM instance with a Google Supplied OS Image with a build date of later than v20200114 it will have the service installed. You should still determine its status for proper operation.

### **Verify the service account you have setup for the project in Recommendation 4.1 is running**

1. Go to the `VM instances` page by visiting:  
<https://console.cloud.google.com/compute/instances>.
2. Click on each instance name to go to its `VM instance details` page.
3. Under the section `Service Account`, take note of the service account
4. Run the commands locally for your operating system that are located at the docs/troubleshooting/vm-manager/verify-setup#service-account-enabled reference located at the bottom of this page. They should return the name of your service account.

## **Determine if Instances can connect to public update hosting**

Each type of operating system has its own update process. You will need to determine on each operating system that it can reach the update servers via its network connection. The VM Manager doesn't host the updates, it will only allow you to centrally issue a command to each VM to update.

### **Determine if OS Config API is Enabled for the Project**

1. In each project you wish to enable run the following command

```
gcloud services list
```

2. If `osconfig.googleapis.com` is in the left hand column it is enabled for this project.

## **Determine if VM Manager is Enabled for the Project**

1. Within the project run the following command:

```
gcloud compute instances os-inventory describe VM-NAME \
--zone=ZONE
```

The output will look like

INSTANCE_ID	INSTANCE_NAME	OS
OSCONFIG_AGENT_VERSION	UPDATE_TIME	
29255009728795105	centos7	CentOS Linux 7 (Core)
20210217.00-g1.e17	2021-04-12T22:19:36.559Z	
5138980234596718741	rhel-8	Red Hat Enterprise Linux 8.3 (Ootpa)
20210316.00-g1.e18	2021-09-16T17:19:24Z	
7127836223366142250	windows	Microsoft Windows Server 2019 Datacenter
20210316.00.0+win@1	2021-09-16T17:13:18Z	

### Determine if VM Instances have correct metadata tags for OSConfig parsing

1. Select the project you want to view tagging in.

### From Google Cloud Console

1. From the main Google Cloud console, open the hamburger menu in the top left. Mouse over Computer Engine to expand the menu next to it.
2. Under the "Settings" heading, select "Metadata".
3. In this view there will be a list of the project wide metadata tags for Vms. Verify a tag of 'enable-osconfig' is in this list and it is set to 'true'.

### From Command Line

Run the following command to view instance data

```
gcloud compute instances list --format="table(name,status,tags.list())"
```

On each instance it should have a tag of 'enable-osconfig' set to 'true'

### Determine if the Operating System of VM Instances have the local OS-Config Agent running

There is no way to determine this from the Google Cloud CLI. The best way is to run the the commands inside the operating system located at 'Check OS-Config agent is installed and running' at the /docs/troubleshooting/vm-manager/verify-setup reference at the bottom of the page. If you initialized your VM instance with a Google Supplied OS Image with a build date of later than v20200114 it will have the service installed. You should still determine its status.

### Verify the service account you have setup for the project in Recommendation 4.1 is running

1. Go to the VM instances page by visiting:  
<https://console.cloud.google.com/compute/instances>.
2. Click on each instance name to go to its VM instance details page.
3. Under the section Service Account, take note of the service account
4. View the compute/docs/troubleshooting/vm-manager/verify-setup#service-account-enabled resource at the bottom of the page for operating system specific commands to run locally.

## Determine if Instances can connect to public update hosting

Linux

Debian Based Operating Systems

```
sudo apt update
```

The output should have a numbered list of lines with Hit: URL of updates.

Redhat Based Operating Systems

```
yum check-update
```

The output should show a list of packages that have updates available.

Windows

```
ping http://windowsupdate.microsoft.com/
```

The ping should successfully be delivered and received.

### Remediation:

#### From Google Cloud Console

#### Enabling OS Patch Management on a Project by Project Basis

#### Install OS Config API for the Project

1. Navigate into a project. In the expanded portal menu located at the top left of the screen hover over "APIs & Services". Then in the menu right of that select "API Libraries"
2. Search for "VM Manager (OS Config API) or scroll down in the left hand column and select the filter labeled "Compute" where it is the last listed. Open this API.
3. Click the blue 'Enable' button.

#### Add MetaData Tags for OSConfig Parsing

1. From the main Google Cloud console, open the portal menu in the top left. Mouse over Computer Engine to expand the menu next to it.
2. Under the "Settings" heading, select "Metadata".
3. In this view there will be a list of the project wide metadata tags for VMs. Click edit and 'add item' in the key column type 'enable-osconfig' and in the value column set it to 'true'.

#### From Command Line

1. For project wide tagging, run the following command

```
gcloud compute project-info add-metadata \
  --project <PROJECT_ID>\
  --metadata=enable-osconfig=TRUE
```



Please see the reference [/compute/docs/troubleshooting/vm-manager/verify-setup#metadata-enabled](#) at the bottom for more options like instance specific tagging. Note: Adding a new tag via commandline may overwrite existing tags. You will need to do this at a time of low usage for the least impact.

### **Install and Start the Local OSConfig for Data Parsing**

There is no way to centrally manage or start the Local OSConfig agent. Please view the reference of [manage-os#agent-install](#) to view specific operating system commands.

### **Setup a project wide Service Account**

Please view Recommendation 4.1 to view how to setup a service account. Rerun the audit procedure to test if it has taken effect.

### **Enable NAT or Configure Private Google Access to allow Access to Public Update Hosting**

For the sake of brevity, please see the attached resources to enable NAT or Private Google Access. Rerun the audit procedure to test if it has taken effect.

From Command Line:

### **Install OS Config API for the Project**

1. In each project you wish to audit run `gcloud services enable osconfig.googleapis.com`

### **Install and Start the Local OSConfig for Data Parsing**

Please view the reference of [manage-os#agent-install](#) to view specific operating system commands.

### **Setup a project wide Service Account**

Please view Recommendation 4.1 to view how to setup a service account. Rerun the audit procedure to test if it has taken effect.

### **Enable NAT or Configure Private Google Access to allow Access to Public Update Hosting**

For the sake of brevity, please see the attached resources to enable NAT or Private Google Access. Rerun the audit procedure to test if it has taken effect.

Determine if Instances can connect to public update hosting

Linux

Debian Based Operating Systems

```
sudo apt update
```

The output should have a numbered list of lines with Hit: URL of updates.

Redhat Based Operating Systems

```
yum check-update
```

The output should show a list of packages that have updates available.

Windows

```
ping http://windowsupdate.microsoft.com/
```

The ping should successfully be delivered and received.

## Default Value:

By default most operating systems and programs do not update themselves. The Google Cloud VM Manager which is a dependency of the OS Patch management feature is installed on Google Built OS images with a build date of v20200114 or later. The VM manager is not enabled in a project by default and will need to be setup.

## References:







1. <https://cloud.google.com/compute/docs/manage-os>
2. <https://cloud.google.com/compute/docs/os-patch-management>
3. <https://cloud.google.com/compute/docs/vm-manager>
4. <https://cloud.google.com/compute/docs/images/os-details#vm-manager>
5. <https://cloud.google.com/compute/docs/vm-manager#pricing>
6. <https://cloud.google.com/compute/docs/troubleshooting/vm-manager/verify-setup>
7. <https://cloud.google.com/compute/docs/instances/view-os-details#view-data-tools>
8. <https://cloud.google.com/compute/docs/os-patch-management/create-patch-job>
9. <https://cloud.google.com/nat/docs/set-up-network-address-translation>
10. <https://cloud.google.com/vpc/docs/configure-private-google-access>
11. <https://workbench.cisecurity.org/sections/811638/recommendations/1334335>
12. <https://cloud.google.com/compute/docs/manage-os#agent-install>
13. <https://cloud.google.com/compute/docs/troubleshooting/vm-manager/verify-setup#service-account-enabled>
14. <https://cloud.google.com/compute/docs/os-patch-management#use-dashboard>
15. <https://cloud.google.com/compute/docs/troubleshooting/vm-manager/verify-setup#metadata-enabled>

## Additional Information:

This is not your only solution to handle updates. This is a Google Cloud specific recommendation to leverage a resource to solve the need for comprehensive update procedures and policy. If you have a solution already in place you do not need to make the switch.

There are also further resources that would be out of the scope of this recommendation. If you need to allow your VMs to access public hosted updates, please see the reference to setup NAT or Private Google Access.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>2.2 Ensure Authorized Software is Currently Supported</u></b> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	<b><u>2.2 Ensure Software is Supported by Vendor</u></b> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

## 5 Storage

This section covers recommendations addressing storage on Google Cloud Platform.

## 5.1 Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible (Automated)

### Profile Applicability:

- Level 1

### Description:

It is recommended that IAM policy on Cloud Storage bucket does not allow anonymous or public access.

### Rationale:

Allowing anonymous or public access grants permissions to anyone to access bucket content. Such access might not be desired if you are storing any sensitive data. Hence, ensure that anonymous or public access to a bucket is not allowed.

### Impact:

No storage buckets would be publicly accessible. You would have to explicitly administer bucket access.

### Audit:

#### From Google Cloud Console

1. Go to Storage browser by visiting <https://console.cloud.google.com/storage/browser>.
2. Click on each bucket name to go to its Bucket details page.
3. Click on the Permissions tab.
4. Ensure that `allUsers` and `allAuthenticatedUsers` are not in the Members list.

#### From Google Cloud CLI

1. List all buckets in a project

```
gsutil ls
```

2. Check the IAM Policy for each bucket:

```
gsutil iam get gs://BUCKET_NAME
```

No role should contain `allUsers` and/or `allAuthenticatedUsers` as a member.

#### Using Rest API

1. List all buckets in a project

```
Get https://www.googleapis.com/storage/v1/b?project=<ProjectName>
```

## 2. Check the IAM Policy for each bucket

```
GET https://www.googleapis.com/storage/v1/b/<bucketName>/iam
```

No role should contain `allUsers` and/or `allAuthenticatedUsers` as a member.

### Remediation:

#### From Google Cloud Console

1. Go to Storage browser by visiting <https://console.cloud.google.com/storage/browser>.
2. Click on the bucket name to go to its Bucket details page.
3. Click on the Permissions tab.
4. Click Delete button in front of `allUsers` and `allAuthenticatedUsers` to remove that particular role assignment.

#### From Google Cloud CLI

Remove `allUsers` and `allAuthenticatedUsers` access.

```
gsutil iam ch -d allUsers gs://BUCKET_NAME  
gsutil iam ch -d allAuthenticatedUsers gs://BUCKET_NAME
```

### Prevention:

You can prevent Storage buckets from becoming publicly accessible by setting up the Domain restricted sharing organization policy at:

<https://console.cloud.google.com/iam-admin/orgpolicies/iam-allowedPolicyMemberDomains>.

### Default Value:

By Default, Storage buckets are not publicly shared.







### References:

1. <https://cloud.google.com/storage/docs/access-control/iam-reference>
2. <https://cloud.google.com/storage/docs/access-control/making-data-public>
3. <https://cloud.google.com/storage/docs/gsutil/commands/iam>

### Additional Information:

To implement Access restrictions on buckets, configuring Bucket IAM is preferred way than configuring Bucket ACL. On GCP console, "Edit Permissions" for bucket exposes IAM configurations only. Bucket ACLs are configured automatically as per need in order to implement/support User enforced Bucket IAM policy. In-case administrator changes bucket ACL using command-line(gsutils)/API bucket IAM also gets updated automatically.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>12.4 <u>Deny Communication over Unauthorized Ports</u></b> Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.			

## *5.2 Ensure That Cloud Storage Buckets Have Uniform Bucket-Level Access Enabled (Automated)*

### **Profile Applicability:**

- Level 2

### **Description:**

It is recommended that uniform bucket-level access is enabled on Cloud Storage buckets.

### **Rationale:**

It is recommended to use uniform bucket-level access to unify and simplify how you grant access to your Cloud Storage resources.

Cloud Storage offers two systems for granting users permission to access your buckets and objects: Cloud Identity and Access Management (Cloud IAM) and Access Control Lists (ACLs). These systems act in parallel - in order for a user to access a Cloud Storage resource, only one of the systems needs to grant the user permission. Cloud IAM is used throughout Google Cloud and allows you to grant a variety of permissions at the bucket and project levels. ACLs are used only by Cloud Storage and have limited permission options, but they allow you to grant permissions on a per-object basis.

In order to support a uniform permissioning system, Cloud Storage has uniform bucket-level access. Using this feature disables ACLs for all Cloud Storage resources: access to Cloud Storage resources then is granted exclusively through Cloud IAM. Enabling uniform bucket-level access guarantees that if a Storage bucket is not publicly accessible, no object in the bucket is publicly accessible either.

### **Impact:**

If you enable uniform bucket-level access, you revoke access from users who gain their access solely through object ACLs.

Certain Google Cloud services, such as Stackdriver, Cloud Audit Logs, and Datastore, cannot export to Cloud Storage buckets that have uniform bucket-level access enabled.

### **Audit:**

#### **From Google Cloud Console**

1. Open the Cloud Storage browser in the Google Cloud Console by visiting:  
<https://console.cloud.google.com/storage/browser>
2. For each bucket, make sure that `Access control` column has the value `Uniform`.

#### **From Google Cloud CLI**



1. List all buckets in a project

```
gsutil ls
```

2. For each bucket, verify that uniform bucket-level access is enabled.

```
gsutil uniformbucketlevelaccess get gs://BUCKET_NAME/
```

If uniform bucket-level access is enabled, the response looks like:

```
Uniform bucket-level access setting for gs://BUCKET_NAME/:
  Enabled: True
  LockedTime: LOCK_DATE
```

## Remediation:

### From Google Cloud Console

1. Open the Cloud Storage browser in the Google Cloud Console by visiting:  
<https://console.cloud.google.com/storage/browser>
2. In the list of buckets, click on the name of the desired bucket.
3. Select the `Permissions` tab near the top of the page.
4. In the text box that starts with `This bucket uses fine-grained access control...`, click `Edit`.
5. In the pop-up menu that appears, select `Uniform`.
6. Click `Save`.

### From Google Cloud CLI

Use the `on` option in a `uniformbucketlevelaccess set` command:

```
gsutil uniformbucketlevelaccess set on gs://BUCKET_NAME/
```

## Prevention

You can set up an Organization Policy to enforce that any new bucket has uniform bucket level access enabled. Learn more at:

<https://cloud.google.com/storage/docs/setting-org-policies#uniform-bucket>

## Default Value:

By default, Cloud Storage buckets do not have uniform bucket-level access enabled.







## References:

1. <https://cloud.google.com/storage/docs/uniform-bucket-level-access>
2. <https://cloud.google.com/storage/docs/using-uniform-bucket-level-access>
3. <https://cloud.google.com/storage/docs/setting-org-policies#uniform-bucket>

## Additional Information:

Uniform bucket-level access can no longer be disabled if it has been active on a bucket for 90 consecutive days.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

## 6 Cloud SQL Database Services

This section covers security recommendations to follow to secure Cloud SQL database services.

The recommendations in this section on setting up database flags are also present in the [CIS Oracle MySQL Community Server 5.7 Benchmarks](#) and in the [CIS PostgreSQL 12 Benchmarks](#). We, nevertheless, include them here as well, the remediation instructions are different on Cloud SQL. Settings these flags require superuser privileges and can only be configured through GCP controls.

Learn more at: <https://cloud.google.com/sql/docs/postgres/users> and <https://cloud.google.com/sql/docs/mysql/flags>.

## 6.1 MySQL Database

This section covers recommendations addressing Cloud SQL for MySQL on Google Cloud Platform.

## 6.1.1 Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges (Manual)

### Profile Applicability:

- Level 1

### Description:

It is recommended to set a password for the administrative user (`root` by default) to prevent unauthorized access to the SQL database instances.

This recommendation is applicable only for MySQL Instances. PostgreSQL does not offer any setting for No Password from the cloud console.

### Rationale:

At the time of MySQL Instance creation, not providing an administrative password allows anyone to connect to the SQL database instance with administrative privileges. The root password should be set to ensure only authorized users have these privileges.

### Impact:

Connection strings for administrative clients need to be reconfigured to use a password.

### Audit:

#### From Google Cloud CLI

1. List All SQL database instances of type MySQL:

```
gcloud sql instances list --filter='DATABASE_VERSION:MYSQL*' --project <project_id> --format="(NAME,PRIMARY_ADDRESS)"
```

2. For every MySQL instance try to connect using the `PRIMARY_ADDRESS`, if available:

```
mysql -u root -h <mysql_instance_ip_address>
```

The command should return either an error message or a password prompt.

Sample Error message:

```
ERROR 1045 (28000): Access denied for user 'root'@'<Instance_IP>' (using password: NO)
```

If a command produces the `mysql>` prompt, the MySQL instance allows anyone to connect with administrative privileges without needing a password.

**Note:** The `No Password` setting is exposed only at the time of MySQL instance creation. Once the instance is created, the Google Cloud Platform Console does not expose the set to confirm whether a password for an administrative user is set to a MySQL instance.

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Platform Console using `https://console.cloud.google.com/sql/`
2. Select the instance to open its Overview page.
3. Select `Access Control > Users`.
4. Click the `More actions` icon for the user to be updated.
5. Select `Change password`, specify a `New password`, and click `OK`.

### From Google Cloud CLI

1. Set a password to a MySQL instance:

```
gcloud sql users set-password root --host=<host> --instance=<instance_name> -  
-prompt-for-password
```

2. A prompt will appear, requiring the user to enter a password:

```
Instance Password:
```

3. With a successful password configured, the following message should be seen:

```
Updating Cloud SQL user...done.
```




### Default Value:




From the Google Cloud Platform Console, the `Create Instance` workflow enforces the rule to enter the root password unless the option `No Password` is selected explicitly.

### References:

1. <https://cloud.google.com/sql/docs/mysql/create-manage-users>
2. <https://cloud.google.com/sql/docs/mysql/create-instance>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.7 Manage Default Accounts on Enterprise Assets and Software</u></b> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<b>4.2 Change Default Passwords</b> Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.			

## 6.1.2 Ensure 'Skip\_show\_database' Database Flag for Cloud SQL MySQL Instance Is Set to 'On' (Automated)

### Profile Applicability:

- Level 1

### Description:

It is recommended to set `skip_show_database` database flag for Cloud SQL MySQL instance to `on`

### Rationale:

`skip_show_database` database flag prevents people from using the `SHOW DATABASES` statement if they do not have the `SHOW DATABASES` privilege. This can improve security if you have concerns about users being able to see databases belonging to other users. Its effect depends on the `SHOW DATABASES` privilege: If the variable value is `ON`, the `SHOW DATABASES` statement is permitted only to users who have the `SHOW DATABASES` privilege, and the statement displays all database names. If the value is `OFF`, `SHOW DATABASES` is permitted to all users, but displays the names of only those databases for which the user has the `SHOW DATABASES` or other privilege. This recommendation is applicable to MySQL database instances.

### Audit:

#### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its `Instance Overview` page
3. Ensure the database flag `skip_show_database` that has been set is listed under the `Database flags` section.

#### From Google Cloud CLI

1. List all Cloud SQL database Instances

```
gcloud sql instances list
```

2. Ensure the below command returns `on` for every Cloud SQL MySQL database instance



```
gcloud sql instances describe <INSTANCE_NAME> --format=json | jq  
' .settings.databaseFlags[] | select(.name=="skip_show_database")|.value '
```

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the Mysql instance for which you want to enable to database flag.
3. Click `Edit`.
4. Scroll down to the `Flags` section.
5. To set a flag that has not been set on the instance before, click `Add a Database Flag`, choose the flag `skip_show_database` from the drop-down menu, and set its value to `on`.
6. Click `Save` to save your changes.
7. Confirm your changes under `Flags` on the Overview page.

### From Google Cloud CLI

1. List all Cloud SQL database Instances

```
gcloud sql instances list
```

2. Configure the `skip_show_database` database flag for every Cloud SQL Mysql database instance using the below command.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags  
skip_show_database=on
```

#### Note:

This command will overwrite all database flags previously set. To keep those and add new ones, include the values for all flags you want set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

#### References:

1. <https://cloud.google.com/sql/docs/mysql/flags>
2. [https://dev.mysql.com/doc/refman/5.7/en/server-system-variables.html#sysvar\\_skip\\_show\\_database](https://dev.mysql.com/doc/refman/5.7/en/server-system-variables.html#sysvar_skip_show_database)







#### Additional Information:

WARNING: This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags - <https://cloud.google.com/sql/docs/mysql/flags> - to see if your instance will be restarted when this patch is submitted.

**Note:** some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines."

**Note:** Configuring the above flag restarts the Cloud SQL instance.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

### 6.1.3 Ensure That the 'Local\_infile' Database Flag for a Cloud SQL MySQL Instance Is Set to 'Off' (Automated)

#### Profile Applicability:

- Level 1

#### Description:

It is recommended to set the `local_infile` database flag for a Cloud SQL MySQL instance to `off`.

#### Rationale:

The `local_infile` flag controls the server-side LOCAL capability for LOAD DATA statements. Depending on the `local_infile` setting, the server refuses or permits local data loading by clients that have LOCAL enabled on the client side.

To explicitly cause the server to refuse LOAD DATA LOCAL statements (regardless of how client programs and libraries are configured at build time or runtime), start `mysqld` with `local_infile` disabled. `local_infile` can also be set at runtime.

Due to security issues associated with the `local_infile` flag, it is recommended to disable it. This recommendation is applicable to MySQL database instances.

#### Impact:

Disabling `local_infile` makes the server refuse local data loading by clients that have LOCAL enabled on the client side.

#### Audit:

#### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its Instance Overview page
3. Ensure the database flag `local_infile` that has been set is listed under the Database flags section.

#### From Google Cloud CLI

1. List all Cloud SQL database instances:

```
gcloud sql instances list
```

2. Ensure the below command returns `off` for every Cloud SQL MySQL database instance.

```
gcloud sql instances describe <INSTANCE_NAME> --format=json | jq  
' .settings.databaseFlags[] | select(.name=="local_infile")|.value '
```

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the MySQL instance where the database flag needs to be enabled.
3. Click `Edit`.
4. Scroll down to the `Flags` section.
5. To set a flag that has not been set on the instance before, click `Add a Database Flag`, choose the flag `local_infile` from the drop-down menu, and set its value to `off`.
6. Click `Save`.
7. Confirm the changes under `Flags` on the Overview page.

### From Google Cloud CLI

1. List all Cloud SQL database instances using the following command:

```
gcloud sql instances list
```

2. Configure the `local_infile` database flag for every Cloud SQL MySQL database instance using the below command:

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags local_infile=off
```

## Note:

This command will overwrite all database flags that were previously set. To keep those and add new ones, include the values for all flags to be set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

## Default Value:

By default `local_infile` is `on`.

## References:

1. <https://cloud.google.com/sql/docs/mysql/flags>
2. [https://dev.mysql.com/doc/refman/5.7/en/server-system-variables.html#sysvar\\_local\\_infile](https://dev.mysql.com/doc/refman/5.7/en/server-system-variables.html#sysvar_local_infile)
3. <https://dev.mysql.com/doc/refman/5.7/en/load-data-local.html>

### Additional Information:



**WARNING:** This patch modifies database flag values, which may require the instance to be restarted. Check the list of supported flags -

<https://cloud.google.com/sql/docs/mysql/flags> - to see if your instance will be restarted when this patch is submitted.

**Note:** some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines."

**Note:** Configuring the above flag restarts the Cloud SQL instance.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>16.7 <u>Use Standard Hardening Configuration Templates for Application Infrastructure</u></b> Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.			
v7	<b>0.0 <u>Explicitly Not Mapped</u></b> Explicitly Not Mapped			

## 6.2 PostgreSQL Database

This section covers recommendations addressing Cloud SQL for PostgreSQL on Google Cloud Platform.

## 6.2.1 Ensure 'Log\_error\_verbosity' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'DEFAULT' or Stricter (Automated)

### Profile Applicability:

- Level 2

### Description:

The `log_error_verbosity` flag controls the verbosity/details of messages logged. Valid values are:

- `TERSE`
- `DEFAULT`
- `VERBOSE`

`TERSE` excludes the logging of `DETAIL`, `HINT`, `QUERY`, and `CONTEXT` error information.

`VERBOSE` output includes the `SQLSTATE` error code, source code file name, function name, and line number that generated the error.

Ensure an appropriate value is set to 'DEFAULT' or stricter.

### Rationale:

Auditing helps in troubleshooting operational problems and also permits forensic analysis. If `log_error_verbosity` is not set to the correct value, too many details or too few details may be logged. This flag should be configured with a value of 'DEFAULT' or stricter. This recommendation is applicable to PostgreSQL database instances.

### Impact:

Turning on logging will increase the required storage over time. Mismanaged logs may cause your storage costs to increase. Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

### Audit:

#### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its `Instance Overview` page
3. Go to `Configuration` card
4. Under `Database flags`, check the value of `log_error_verbosity` flag is set to 'DEFAULT' or stricter.

## From Google Cloud CLI

1. Use the below command for every Cloud SQL PostgreSQL database instance to verify the value of `log_error_verbosity`

```
gcloud sql instances describe [INSTANCE_NAME] --format=json | jq  
'settings.databaseFlags[] | select(.name=="log_error_verbosity")|.value'
```

In the output, database flags are listed under the settings as the collection `databaseFlags`.

### Remediation:

## From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the PostgreSQL instance for which you want to enable the database flag.
3. Click `Edit`.
4. Scroll down to the `Flags` section.
5. To set a flag that has not been set on the instance before, click `Add a Database Flag`, choose the flag `log_error_verbosity` from the drop-down menu and set appropriate value.
6. Click `Save` to save your changes.
7. Confirm your changes under `Flags` on the Overview page.

## From Google Cloud CLI

1. Configure the `log_error_verbosity` database flag for every Cloud SQL PostgreSQL database instance using the below command.

```
gcloud sql instances patch INSTANCE_NAME --database-flags  
log_error_verbosity=<TERSE|DEFAULT|VERBOSE>
```

**Note:** This command will overwrite all database flags previously set. To keep those and add new ones, include the values for all flags you want set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

### Default Value:

By default `log_error_verbosity` is `DEFAULT`.

### References:

1. <https://cloud.google.com/sql/docs/postgres/flags>
2. <https://www.postgresql.org/docs/current/runtime-config-logging.html#RUNTIME-CONFIG-LOGGING-WHAT>



### Additional Information:





**WARNING:** This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags -

<https://cloud.google.com/sql/docs/postgres/flags> - to see if your instance will be restarted when this patch is submitted.

**Note:** some database flag settings can affect instance availability or stability and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

**Note:** Configuring the above flag does not require restarting the Cloud SQL instance.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 6.2.2 Ensure That the 'Log\_connections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On' (Automated)

### Profile Applicability:

- Level 1

### Description:

Enabling the `log_connections` setting causes each attempted connection to the server to be logged, along with successful completion of client authentication. This parameter cannot be changed after the session starts.

### Rationale:

PostgreSQL does not log attempted connections by default. Enabling the `log_connections` setting will create log entries for each attempted connection as well as successful completion of client authentication which can be useful in troubleshooting issues and to determine any unusual connection attempts to the server. This recommendation is applicable to PostgreSQL database instances.

### Impact:

Turning on logging will increase the required storage over time. Mismanaged logs may cause your storage costs to increase. Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

### Audit:

#### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its `Instance Overview` page.
3. Go to the `Configuration` card.
4. Under `Database flags`, check the value of `log_connections` flag to determine if it is configured as expected.

#### From Google Cloud CLI

1. Ensure the below command returns `on` for every Cloud SQL PostgreSQL database instance:

```
gcloud sql instances describe [INSTANCE_NAME] --format=json | jq  
' .settings.databaseFlags[] | select(.name=="log_connections")|.value '
```

In the output, database flags are listed under the `settings` as the collection `databaseFlags`.

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the PostgreSQL instance for which you want to enable the database flag.
3. Click `Edit`.
4. Scroll down to the `Flags` section.
5. To set a flag that has not been set on the instance before, click `Add a Database Flag`, choose the flag `log_connections` from the drop-down menu and set the value as `on`.
6. Click `Save`.
7. Confirm the changes under `Flags` on the Overview page.

### From Google Cloud CLI

1. Configure the `log_connections` database flag for every Cloud SQL PostgreSQL database instance using the below command.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags  
"log_connections=on"
```

## Note:

This command will overwrite all previously set database flags. To keep those and add new ones, include the values for all flags to be set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

## Default Value:

By default `log_connections` is `off`.

## References:

1. <https://cloud.google.com/sql/docs/postgres/flags>
2. <https://www.postgresql.org/docs/9.6/runtime-config-logging.html#RUNTIME-CONFIG-LOGGING-WHAT>

### Additional Information:





**WARNING:** This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags -

<https://cloud.google.com/sql/docs/postgres/flags> - to see if your instance will be restarted when this patch is submitted.

**Note:** some database flag settings can affect instance availability or stability and remove the instance from the Cloud SQL SLA. For information about these flags, see the Operational Guidelines.

**Note:** Configuring the above flag does not require restarting the Cloud SQL instance.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 6.2.3 Ensure That the 'Log\_disconnections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On' (Automated)

### Profile Applicability:

- Level 1

### Description:

Enabling the `log_disconnections` setting logs the end of each session, including the session duration.

### Rationale:

PostgreSQL does not log session details such as duration and session end by default. Enabling the `log_disconnections` setting will create log entries at the end of each session which can be useful in troubleshooting issues and determine any unusual activity across a time period. The `log_disconnections` and `log_connections` work hand in hand and generally, the pair would be enabled/disabled together. This recommendation is applicable to PostgreSQL database instances.

### Impact:

Turning on logging will increase the required storage over time. Mismanaged logs may cause your storage costs to increase. Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

### Audit:

#### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its `Instance Overview` page
3. Go to the `Configuration` card.
4. Under `Database flags`, check the value of `log_disconnections` flag is configured as expected.

#### From Google Cloud CLI

1. Ensure the below command returns `on` for every Cloud SQL PostgreSQL database instance:

```
gcloud sql instances list --format=json | jq '.[].settings.databaseFlags[] | select(.name=="log_disconnections")|.value'
```

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the PostgreSQL instance where the database flag needs to be enabled.
3. Click Edit.
4. Scroll down to the `Flags` section.
5. To set a flag that has not been set on the instance before, click Add a Database Flag, choose the flag `log_disconnections` from the drop-down menu and set the value as `on`.
6. Click Save.
7. Confirm the changes under `Flags` on the Overview page.

### From Google Cloud CLI

1. Configure the `log_disconnections` database flag for every Cloud SQL PostgreSQL database instance using the below command:

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags log_disconnections=on
```

**Note:** This command will overwrite all previously set database flags. To keep those and add new ones, include the values for all flags to be set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

## Default Value:

By default `log_disconnections` is off.

## References:

1. <https://cloud.google.com/sql/docs/postgres/flags>
2. <https://www.postgresql.org/docs/9.6/runtime-config-logging.html#RUNTIME-CONFIG-LOGGING-WHAT>





## Additional Information:

WARNING: This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags - <https://cloud.google.com/sql/docs/postgres/flags> - to see if your instance will be restarted when this patch is submitted.

**Note:** some database flag settings can affect instance availability or stability and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

**Note:** Configuring the above flag does not require restarting the Cloud SQL instance.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 6.2.4 Ensure 'Log\_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set Appropriately (Automated)

### Profile Applicability:

- Level 2

### Description:

The value of `log_statement` flag determined the SQL statements that are logged. Valid values are:

- `none`
- `ddl`
- `mod`
- `all`

The value `ddl` logs all data definition statements. The value `mod` logs all ddl statements, plus data-modifying statements.

The statements are logged after a basic parsing is done and statement type is determined, thus this does not logs statements with errors. When using extended query protocol, logging occurs after an Execute message is received and values of the Bind parameters are included.

A value of 'ddl' is recommended unless otherwise directed by your organization's logging policy.

### Rationale:

Auditing helps in forensic analysis. If `log_statement` is not set to the correct value, too many statements may be logged leading to issues in finding the relevant information from the logs, or too few statements may be logged with relevant information missing from the logs. Setting `log_statement` to align with your organization's security and logging policies facilitates later auditing and review of database activities. This recommendation is applicable to PostgreSQL database instances.

### Impact:

Turning on logging will increase the required storage over time. Mismanaged logs may cause your storage costs to increase. Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.



## Audit:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its `Instance Overview` page
3. Go to `Configuration` card
4. Under `Database flags`, check the value of `log_statement` flag is set to appropriately.

### From Google Cloud CLI

1. Use the below command for every Cloud SQL PostgreSQL database instance to verify the value of `log_statement`

```
gcloud sql instances list --format=json | jq '[][.settings.databaseFlags[] | select(.name=="log_statement")|.value']
```

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the PostgreSQL instance for which you want to enable the database flag.
3. Click `Edit`.
4. Scroll down to the `Flags` section.
5. To set a flag that has not been set on the instance before, click `Add a Database Flag`, choose the flag `log_statement` from the drop-down menu and set appropriate value.
6. Click `Save` to save your changes.
7. Confirm your changes under `Flags` on the Overview page.

### From Google Cloud CLI

1. Configure the `log_statement` database flag for every Cloud SQL PostgreSQL database instance using the below command.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags log_statement=<ddl|mod|all|none>
```

**Note:** This command will overwrite all database flags previously set. To keep those and add new ones, include the values for all flags you want set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

## References:

1. <https://cloud.google.com/sql/docs/postgres/flags>
2. <https://www.postgresql.org/docs/current/runtime-config-logging.html#RUNTIME-CONFIG-LOGGING-WHAT>

## Additional Information:





**WARNING:** This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags -

<https://cloud.google.com/sql/docs/postgres/flags> - to see if your instance will be restarted when this patch is submitted.

**Note:** some database flag settings can affect instance availability or stability and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

**Note:** Configuring the above flag does not require restarting the Cloud SQL instance.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 6.2.5 Ensure that the 'Log\_min\_messages' Flag for a Cloud SQL PostgreSQL Instance is set at minimum to 'Warning' (Automated)

### Profile Applicability:

- Level 1

### Description:

The `log_min_messages` flag defines the minimum message severity level that is considered as an error statement. Messages for error statements are logged with the SQL statement. Valid values include (from lowest to highest severity) `DEBUG5`, `DEBUG4`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `LOG`, `FATAL`, and `PANIC`. Each severity level includes the subsequent levels mentioned above. `ERROR` is considered the best practice setting. Changes should only be made in accordance with the organization's logging policy.

### Rationale:

Auditing helps in troubleshooting operational problems and also permits forensic analysis. If `log_min_messages` is not set to the correct value, messages may not be classified as error messages appropriately. An organization will need to decide their own threshold for logging `log_min_messages` flag.

This recommendation is applicable to PostgreSQL database instances.

### Impact:

Setting the threshold too low will might result in increased log storage size and length, making it difficult to find actual errors. Setting the threshold to 'Warning' will log messages for the most needed error messages. Higher severity levels may cause errors needed to troubleshoot to not be logged.

**Note:** To effectively turn off logging failing statements, set this parameter to `PANIC`.

### Audit:

#### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its `Instance Overview` page.
3. Go to the `Configuration` card.
4. Under `Database flags`, check the value of `log_min_messages` flag is in accordance with the organization's logging policy.

## From Google Cloud CLI

1. Use the below command for every Cloud SQL PostgreSQL database instance to verify that the value of `log_min_messages` is in accordance with the organization's logging policy.

```
gcloud sql instances describe [INSTANCE_NAME] --format=json | jq  
' .settings.databaseFlags[] | select(.name=="log_min_messages") | .value '
```

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>
2. Select the PostgreSQL instance for which you want to enable the database flag.
3. Click `Edit`.
4. Scroll down to the `Flags` section.
5. To set a flag that has not been set on the instance before, click `Add a Database Flag`, choose the flag `log_min_messages` from the drop-down menu and set appropriate value.
6. Click `Save` to save the changes.
7. Confirm the changes under `Flags` on the Overview page.

### From Google Cloud CLI

1. Configure the `log_min_messages` database flag for every Cloud SQL PostgreSQL database instance using the below command.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags  
log_min_messages=<DEBUG5 | DEBUG4 | DEBUG3 | DEBUG2 | DEBUG1 | INFO | NOTICE | WARNING | ERRO  
R | LOG | FATAL | PANIC>
```

**Note:** This command will overwrite all database flags previously set. To keep those and add new ones, include the values for all flags to be set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

## Default Value:

By default `log_min_messages` is `ERROR`.

## References:

1. <https://cloud.google.com/sql/docs/postgres/flags>
2. <https://www.postgresql.org/docs/9.6/runtime-config-logging.html#RUNTIME-CONFIG-LOGGING-WHEN>

### Additional Information:





**WARNING:** This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags -

<https://cloud.google.com/sql/docs/postgres/flags> - to see if your instance will be restarted when this patch is submitted.

**Note:** Some database flag settings can affect instance availability or stability and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

**Note:** Configuring the above flag does not require restarting the Cloud SQL instance.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 6.2.6 Ensure 'Log\_min\_error\_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Error' or Stricter (Automated)

### Profile Applicability:

- Level 1

### Description:

The `log_min_error_statement` flag defines the minimum message severity level that are considered as an error statement. Messages for error statements are logged with the SQL statement. Valid values include (from lowest to highest severity) `DEBUG5`, `DEBUG4`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `LOG`, `FATAL`, and `PANIC`. Each severity level includes the subsequent levels mentioned above. Ensure a value of `ERROR` or stricter is set.

### Rationale:

Auditing helps in troubleshooting operational problems and also permits forensic analysis. If `log_min_error_statement` is not set to the correct value, messages may not be classified as error messages appropriately. Considering general log messages as error messages would make it difficult to find actual errors and considering only stricter severity levels as error messages may skip actual errors to log their SQL statements. The `log_min_error_statement` flag should be set to `ERROR` or stricter. This recommendation is applicable to PostgreSQL database instances.

### Impact:

Turning on logging will increase the required storage over time. Mismanaged logs may cause your storage costs to increase. Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

### Audit:

#### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its `Instance Overview` page
3. Go to `Configuration` card
4. Under `Database flags`, check the value of `log_min_error_statement` flag is configured as to `ERROR` or stricter.

## From Google Cloud CLI

1. Use the below command for every Cloud SQL PostgreSQL database instance to verify the value of `log_min_error_statement` is set to `ERROR` or stricter.

```
gcloud sql instances describe <INSTANCE_NAME> --format=json | jq  
'.[].settings.databaseFlags[] |  
select(.name=="log_min_error_statement")|.value'
```

In the output, database flags are listed under the `settings` as the collection `databaseFlags`.

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the PostgreSQL instance for which you want to enable the database flag.
3. Click `Edit`.
4. Scroll down to the `Flags` section.
5. To set a flag that has not been set on the instance before, click `Add item`, choose the flag `log_min_error_statement` from the drop-down menu and set appropriate value.
6. Click `Save` to save your changes.
7. Confirm your changes under `Flags` on the Overview page.

## From Google Cloud CLI

1. Configure the `log_min_error_statement` database flag for every Cloud SQL PostgreSQL database instance using the below command.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags  
log_min_error_statement=<DEBUG5 | DEBUG4 | DEBUG3 | DEBUG2 | DEBUG1 | INFO | NOTICE | WARNI  
NG | ERROR>
```

**Note:** This command will overwrite all database flags previously set. To keep those and add new ones, include the values for all flags you want set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("`=`").

## Default Value:

By default `log_min_error_statement` is `ERROR`.

## References:

1. <https://cloud.google.com/sql/docs/postgres/flags>

2. <https://www.postgresql.org/docs/9.6/runtime-config-logging.html#RUNTIME-CONFIG-LOGGING-WHEN>

### Additional Information:





**WARNING:** This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags -

<https://cloud.google.com/sql/docs/postgres/flags> - to see if your instance will be restarted when this patch is submitted.

**Note:** some database flag settings can affect instance availability or stability and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

**Note:** Configuring the above flag does not require restarting the Cloud SQL instance.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 Collect Detailed Audit Logs</b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			



## 6.2.7 Ensure That the 'Log\_min\_duration\_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to '-1' (Disabled) (Automated)

### Profile Applicability:

- Level 1

### Description:

The `log_min_duration_statement` flag defines the minimum amount of execution time of a statement in milliseconds where the total duration of the statement is logged. Ensure that `log_min_duration_statement` is disabled, i.e., a value of `-1` is set.

### Rationale:

Logging SQL statements may include sensitive information that should not be recorded in logs. This recommendation is applicable to PostgreSQL database instances.

### Impact:

Turning on logging will increase the required storage over time. Mismanaged logs may cause your storage costs to increase. Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

### Audit:

#### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its `Instance Overview` page.
3. Go to the `Configuration` card.
4. Under `Database flags`, check that the value of `log_min_duration_statement` flag is set to `-1`.

#### From Google Cloud CLI

1. Use the below command for every Cloud SQL PostgreSQL database instance to verify the value of `log_min_duration_statement` is set to `-1`.

```
gcloud sql instances describe <INSTANCE_NAME> --format=json | jq
'.settings.databaseFlags[] |
select(.name=="log_min_duration_statement")|.value'
```

In the output, database flags are listed under the `settings` as the collection `databaseFlags`.

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the PostgreSQL instance where the database flag needs to be enabled.
3. Click `Edit`.
4. Scroll down to the `Flags` section.
5. To set a flag that has not been set on the instance before, click `Add item`, choose the flag `log_min_duration_statement` from the drop-down menu and set a value of `-1`.
6. Click `Save`.
7. Confirm the changes under `Flags` on the Overview page.

### From Google Cloud CLI

1. List all Cloud SQL database instances using the following command:

```
gcloud sql instances list
```

2. Configure the `log_min_duration_statement` flag for every Cloud SQL PostgreSQL database instance using the below command:

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags
log_min_duration_statement=-1
```

**Note:** This command will overwrite all database flags previously set. To keep those and add new ones, include the values for all flags to be set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("`=`").

## Default Value:

By default `log_min_duration_statement` is `-1`.

## References:

1. <https://cloud.google.com/sql/docs/postgres/flags>
2. <https://www.postgresql.org/docs/current/runtime-config-logging.html#RUNTIME-CONFIG-LOGGING-WHAT>

### Additional Information:





**WARNING:** This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags -

<https://cloud.google.com/sql/docs/postgres/flags> - to see if your instance will be restarted when this patch is submitted.

**Note:** Some database flag settings can affect instance availability or stability and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

**Note:** Configuring the above flag does not require restarting the Cloud SQL instance.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

## 6.2.8 Ensure That 'cloudsql.enable\_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging (Automated)

### Profile Applicability:

- Level 1

### Description:

Ensure `cloudsql.enable_pgaudit` database flag for Cloud SQL PostgreSQL instance is set to `on` to allow for centralized logging.

### Rationale:

As numerous other recommendations in this section consist of turning on flags for logging purposes, your organization will need a way to manage these logs. You may have a solution already in place. If you do not, consider installing and enabling the open source `pgaudit` extension within PostgreSQL and enabling its corresponding flag of `cloudsql.enable_pgaudit`. This flag and installing the extension enables database auditing in PostgreSQL through the open-source `pgAudit` extension. This extension provides detailed session and object logging to comply with government, financial, & ISO standards and provides auditing capabilities to mitigate threats by monitoring security events on the instance. Enabling the flag and settings later in this recommendation will send these logs to Google Logs Explorer so that you can access them in a central location. This recommendation is applicable only to PostgreSQL database instances.

### Impact:

Enabling the `pgAudit` extension can lead to increased data storage requirements and to ensure durability of `pgAudit` log records in the event of unexpected storage issues, it is recommended to enable the `Enable automatic storage increases` setting on the instance. Enabling flags via the command line will also overwrite all existing flags, so you should apply all needed flags in the CLI command. Also flags may require a restart of the server to be implemented or will break existing functionality so update your servers at a time of low usage.

### Audit:

#### Determining if the `pgAudit` Flag is set to 'on' From Google Cloud Console

1. Go to <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its `Overview` page.
3. Click `Edit`.
4. Scroll down and expand `Flags`.

5. Ensure that `cloudsql.enable_pgaudit` flag is set to `on`.

### From Google Cloud CLI

Run the command by providing `<INSTANCE_NAME>`. Ensure the value of the flag is `on`.

```
gcloud sql instances describe <INSTANCE_NAME> --format="json" | jq  
'|.settings|.databaseFlags[]|select(.name=="cloudsql.enable_pgaudit")|.value  
,
```

### Determine if the pgAudit extension is installed

1. Connect to the the server running PostgreSQL or through a SQL client of your choice.
2. Via command line open the PostgreSQL shell by typing `psql`
3. Run the following command

```
SELECT *  
FROM pg_extension;
```

4. If pgAudit is in this list. If so, it is installed.

### Determine if Data Access Audit logs are enabled for your project and have sufficient privileges

1. From the homepage open the hamburger menu in the top left.
2. Scroll down to `IAM & Admin` and hover over it.
3. In the menu that opens up, select `Audit Logs`
4. In the middle of the page, in the search box next to `filter` search for `Cloud Composer API`
5. Select it, and ensure that both 'Admin Read' and 'Data Read' are checked.

### Determine if logs are being sent to Logs Explorer

1. From the Google Console home page, open the hamburger menu in the top left.
2. In the menu that pops open, scroll down to `Logs Explorer` under `Operations`.
3. In the query box, paste the following and search

```
resource.type="cloudsql_database"  
logName="projects/<your-project-  
name>/logs/cloudaudit.googleapis.com%2Fdata_access"  
protoPayload.request.@type="type.googleapis.com/google.cloud.sql.audit.v1.PgA  
uditEntry"
```

4. If it returns any log sources, they are correctly setup.

## Remediation:

### Initialize the pgAudit flag From Google Cloud Console

1. Go to <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its Overview page.
3. Click Edit.
4. Scroll down and expand Flags.
5. To set a flag that has not been set on the instance before, click Add item.
6. Enter `cloudsql.enable_pgaudit` for the flag name and set the flag to on.
7. Click Done.
8. Click Save to update the configuration.
9. Confirm your changes under Flags on the Overview page.

### From Google Cloud CLI

Run the below command by providing <INSTANCE\_NAME> to enable `cloudsql.enable_pgaudit` flag.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags
cloudsql.enable_pgaudit=on
```

Note: RESTART is required to get this configuration in effect.

### Creating the extension

1. Connect to the the server running PostgreSQL or through a SQL client of your choice.
2. If SSHing to the server in the command line open the PostgreSQL shell by typing `psql`
3. Run the following command as a superuser.

```
CREATE EXTENSION pgaudit;
```

### Updating the previously created pgaudit.log flag for your Logging Needs

#### From Console:

Note: there are multiple options here. This command will enable logging for all databases on a server. Please see the customizing database audit logging reference for more flag options.

1. Go to <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its Overview page.
3. Click Edit.
4. Scroll down and expand Flags.
5. To set a flag that has not been set on the instance before, click Add item.
6. Enter `pgaudit.log=all` for the flag name and set the flag to on.
7. Click Done.
8. Click Save to update the configuration.

9. Confirm your changes under `Flags` on the `Overview` page.

### From Command Line:

Run the command

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags \
cloudsql.enable_pgaudit=on,pgaudit.log=all
```

### Determine if logs are being sent to Logs Explorer

1. From the Google Console home page, open the hamburger menu in the top left.
2. In the menu that pops open, scroll down to Logs Explorer under Operations.
3. In the query box, paste the following and search

```
resource.type="cloudsql_database"
logName="projects//logs/cloudaudit.googleapis.com%2Fdata_access"
protoPayload.request.@type="type.googleapis.com/google.cloud.sql.audit.v1.PgAuditEntry"
```

If it returns any log sources, they are correctly setup.

### Default Value:

By default `cloudsql.enable_pgaudit` database flag is set to `off` and the extension is not enabled.

### References:

1. <https://cloud.google.com/sql/docs/postgres/flags#list-flags-postgres>
2. <https://cloud.google.com/sql/docs/postgres/pg-audit#enable-auditing-flag>
3. <https://cloud.google.com/sql/docs/postgres/pg-audit#customizing-database-audit-logging>
4. <https://cloud.google.com/logging/docs/audit/configure-data-access#config-console-enable>

### Additional Information:

WARNING: This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags -

<https://cloud.google.com/sql/docs/postgres/flags> - to see if your instance will be restarted when this patch is submitted.

Note: Configuring the 'cloudsql.enable\_pgaudit' database flag requires restarting the Cloud SQL PostgreSQL instance.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v8	<b>8.9 <u>Centralize Audit Logs</u></b> Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	<b>6.5 <u>Central Log Management</u></b> Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●



## 6.3 SQL Server

This section covers recommendations addressing Cloud SQL for SQL Server on Google Cloud Platform.

### 6.3.1 Ensure 'external scripts enabled' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated)

#### Profile Applicability:

- Level 1

#### Description:

It is recommended to set `external scripts enabled` database flag for Cloud SQL SQL Server instance to `off`

#### Rationale:

`external scripts enabled` enable the execution of scripts with certain remote language extensions. This property is OFF by default. When Advanced Analytics Services is installed, setup can optionally set this property to true. As the External Scripts Enabled feature allows scripts external to SQL such as files located in an R library to be executed, which could adversely affect the security of the system, hence this should be disabled. This recommendation is applicable to SQL Server database instances.

#### Impact:

Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

#### Audit:

##### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its `Instance Overview` page
3. Ensure the database flag `external scripts enabled` that has been set is listed under the `Database flags` section.

##### From Google Cloud CLI

1. Ensure the below command returns `off` for every Cloud SQL SQL Server database instance

```
gcloud sql instances describe <INSTANCE_NAME> --format=json | jq
'.settings.databaseFlags[] | select(.name=="external scripts
enabled")|.value'
```

In the output, database flags are listed under the `settings` as the collection `databaseFlags`.

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the SQL Server instance for which you want to enable the database flag.
3. Click `Edit`.
4. Scroll down to the `Flags` section.
5. To set a flag that has not been set on the instance before, click `Add item`, choose the flag `external scripts enabled` from the drop-down menu, and set its value to `off`.
6. Click `Save` to save your changes.
7. Confirm your changes under `Flags` on the Overview page.

### From Google Cloud CLI

1. Configure the `external scripts enabled` database flag for every Cloud SQL SQL Server database instance using the below command.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags "external scripts enabled"=off
```

#### Note:

This command will overwrite all database flags previously set. To keep those and add new ones, include the values for all flags you want set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

#### Default Value:

By default `external scripts enabled` is `off`

#### References:

1. <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/external-scripts-enabled-server-configuration-option?view=sql-server-ver15>
2. <https://cloud.google.com/sql/docs/sqlserver/flags>
3. <https://docs.microsoft.com/en-us/sql/advanced-analytics/concepts/security?view=sql-server-ver15>
4. [https://www.stigviewer.com/stig/ms\\_sql\\_server\\_2016\\_instance/2018-03-09/finding/V-79347](https://www.stigviewer.com/stig/ms_sql_server_2016_instance/2018-03-09/finding/V-79347)

### Additional Information:

**WARNING:** This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags -

<https://cloud.google.com/sql/docs/sqlserver/flags> - to see if your instance will be restarted when this patch is submitted.

**Note:** some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines."

**Note:** Configuring the above flag restarts the Cloud SQL instance.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>2.7 <u>Allowlist Authorized Scripts</u></b> Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●
v7	<b>2.9 <u>Implement Application Whitelisting of Scripts</u></b> The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.			●

### 6.3.2 Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated)

#### Profile Applicability:

- Level 1

#### Description:

It is recommended to set `cross db ownership chaining` database flag for Cloud SQL SQL Server instance to `off`.

This flag is deprecated for all SQL Server versions in CGP. Going forward, you can't set its value to on. However, if you have this flag enabled, we strongly recommend that you either remove the flag from your database or set it to off. For cross-database access, use the [Microsoft tutorial for signing stored procedures with a certificate](#).

#### Rationale:

Use the `cross db ownership` for chaining option to configure cross-database ownership chaining for an instance of Microsoft SQL Server. This server option allows you to control cross-database ownership chaining at the database level or to allow cross-database ownership chaining for all databases. Enabling `cross db ownership` is not recommended unless all of the databases hosted by the instance of SQL Server must participate in cross-database ownership chaining and you are aware of the security implications of this setting. This recommendation is applicable to SQL Server database instances.

#### Impact:

Updating flags may cause the database to restart. This may cause it to be unavailable for a short amount of time, so this is best done at a time of low usage. You should also determine if the tables in your databases reference another table without using credentials for that database, as turning off cross database ownership will break this relationship.

#### Audit:

**NOTE:** This flag is deprecated for all SQL Server versions. Going forward, you can't set its value to on. However, if you have this flag enabled it should be removed from your database or set to off.

#### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console.
2. Select the instance to open its `Instance Overview` page
3. Ensure the database flag `cross db ownership chaining` that has been set is listed under the `Database flags` section.

## From Google Cloud CLI

1. Ensure the below command returns `off` for every Cloud SQL SQL Server database instance:

```
gcloud sql instances describe <INSTANCE_NAME> --format=json | jq  
'settings.databaseFlags[] | select(.name=="cross db ownership  
chaining")|.value'
```

In the output, database flags are listed under the `settings` as the collection `databaseFlags`.

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the SQL Server instance for which you want to enable to database flag.
3. Click `Edit`.
4. Scroll down to the `Flags` section.
5. To set a flag that has not been set on the instance before, click `Add item`, choose the flag `cross db ownership chaining` from the drop-down menu, and set its value to `off`.
6. Click `Save`.
7. Confirm the changes under `Flags` on the Overview page.

## From Google Cloud CLI

1. Configure the `cross db ownership chaining` database flag for every Cloud SQL SQL Server database instance using the below command:

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags "cross db  
ownership chaining"=off
```

### Note:

This command will overwrite all database flags previously set. To keep those and add new ones, include the values for all flags to be set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("`=`").

### Default Value:

This flag is deprecated for all SQL Server versions. Going forward, you can't set its value to on.

### References:

1. <https://cloud.google.com/sql/docs/sqlserver/flags>

2. <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/cross-db-ownership-chaining-server-configuration-option?view=sql-server-ver15>

### Additional Information:







**WARNING:** This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags -

<https://cloud.google.com/sql/docs/sqlserver/flags> - to see if your instance will be restarted when this patch is submitted.

**Note:** Some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

**Note:** Configuring the above flag does not restart the Cloud SQL instance.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 Protect Information through Access Control Lists</b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

### 6.3.3 Ensure 'user Connections' Database Flag for Cloud Sql Sql Server Instance Is Set to a Non-limiting Value (Automated)

#### Profile Applicability:

- Level 1

#### Description:

It is recommended to check the `user connections` for a Cloud SQL SQL Server instance to ensure that it is not artificially limiting connections.

#### Rationale:

The `user connections` option specifies the maximum number of simultaneous user connections that are allowed on an instance of SQL Server. The actual number of user connections allowed also depends on the version of SQL Server that you are using, and also the limits of your application or applications and hardware. SQL Server allows a maximum of 32,767 user connections. Because `user connections` is by default a self-configuring value, with SQL Server adjusting the maximum number of user connections automatically as needed, up to the maximum value allowable. For example, if only 10 users are logged in, 10 user connection objects are allocated. In most cases, you do not have to change the value for this option. The default is 0, which means that the maximum (32,767) user connections are allowed. However if there is a number defined here that limits connections, SQL Server will not allow anymore above this limit. If the connections are at the limit, any new requests will be dropped, potentially causing lost data or outages for those using the database.

#### Impact:

Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

#### Audit:

#### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its `Instance Overview` page
3. Ensure the database flag `user connections` listed under the `Database flags` section is 0.



## From Google Cloud CLI

1. Ensure the below command returns a value of 0, for every Cloud SQL SQL Server database instance.

```
gcloud sql instances describe <INSTANCE_NAME> --format=json | jq  
'settings.databaseFlags[] | select(.name=="user connections")|.value'
```

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the SQL Server instance for which you want to enable to database flag.
3. Click **Edit**.
4. Scroll down to the **Flags** section.
5. To set a flag that has not been set on the instance before, click **Add item**, choose the flag `user connections` from the drop-down menu, and set its value to your organization recommended value.
6. Click **Save** to save your changes.
7. Confirm your changes under **Flags** on the Overview page.

## From Google Cloud CLI

1. Configure the `user connections` database flag for every Cloud SQL SQL Server database instance using the below command.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags "user  
connections=[0-32,767]"
```

### Note:

This command will overwrite all database flags previously set. To keep those and add new ones, include the values for all flags you want set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

### Default Value:

By default `user connections` is set to '0' which does not limit the number of connections, giving the server free reign to facilitate a max of 32,767 connections.

### References:

1. <https://cloud.google.com/sql/docs/sqlserver/flags>
2. <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-the-user-connections-server-configuration-option?view=sql-server-ver15>

3. [https://www.stigviewer.com/stig/ms\\_sql\\_server\\_2016\\_instance/2018-03-09/finding/V-79119](https://www.stigviewer.com/stig/ms_sql_server_2016_instance/2018-03-09/finding/V-79119)

#### Additional Information:







**WARNING:** This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags -

<https://cloud.google.com/sql/docs/sqlserver/flags> - to see if your instance will be restarted when this patch is submitted.

**Note:** some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

**Note:** Configuring the above flag does not restart the Cloud SQL instance.

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b>5.1 <u>Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

### 6.3.4 Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured (Automated)

#### Profile Applicability:

- Level 1

#### Description:

It is recommended that, `user options` database flag for Cloud SQL SQL Server instance should not be configured.

#### Rationale:

The `user options` option specifies global defaults for all users. A list of default query processing options is established for the duration of a user's work session. The `user options` option allows you to change the default values of the SET options (if the server's default settings are not appropriate).

A user can override these defaults by using the SET statement. You can configure user options dynamically for new logins. After you change the setting of user options, new login sessions use the new setting; current login sessions are not affected. This recommendation is applicable to SQL Server database instances.

#### Impact:

Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

#### Audit:

##### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its `Instance Overview` page
3. Ensure the database flag `user options` that has been set is not listed under the `Database flags` section.

##### From Google Cloud CLI

1. Ensure the below command returns empty result for every Cloud SQL SQL Server database instance

```
gcloud sql instances describe <INSTANCE_NAME> --format=json | jq  
' .settings.databaseFlags[] | select(.name=="user options")|.value '
```

In the output, database flags are listed under the `settings` as the collection `databaseFlags`.

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the SQL Server instance for which you want to enable to database flag.
3. Click `Edit`.
4. Scroll down to the `Flags` section.
5. Click the X next `user options` flag shown
6. Click `Save` to save your changes.
7. Confirm your changes under `Flags` on the Overview page.

### From Google Cloud CLI

1. List all Cloud SQL database Instances

```
gcloud sql instances list
```

2. Clear the `user options` database flag for every Cloud SQL SQL Server database instance using either of the below commands.

#### Clearing all flags to their default value

```
gcloud sql instances patch <INSTANCE_NAME> --clear-database-flags
```

OR

To clear only `user options` database flag, configure the database flag by overriding the `user options`. **Exclude** `user options` flag and its value, and keep all other flags you want to configure.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags  
[FLAG1=VALUE1,FLAG2=VALUE2]
```

#### Note:

This command will overwrite all database flags previously set. To keep those and add new ones, include the values for all flags you want set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

#### Default Value:

By default 'user options' is not configured.

## References:

1. <https://cloud.google.com/sql/docs/sqlserver/flags>
2. <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-the-user-options-server-configuration-option?view=sql-server-ver15>
3. [https://www.stigviewer.com/stig/ms\\_sql\\_server\\_2016\\_instance/2018-03-09/finding/V-79335](https://www.stigviewer.com/stig/ms_sql_server_2016_instance/2018-03-09/finding/V-79335)







## Additional Information:

**WARNING:** This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags - <https://cloud.google.com/sql/docs/sqlserver/flags> - to see if your instance will be restarted when this patch is submitted.

**Note:** some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

**Note:** Configuring the above flag does not restart the Cloud SQL instance.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

### 6.3.5 Ensure 'remote access' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated)

#### Profile Applicability:

- Level 1

#### Description:

It is recommended to set `remote access` database flag for Cloud SQL SQL Server instance to `off`.

#### Rationale:

The `remote access` option controls the execution of stored procedures from local or remote servers on which instances of SQL Server are running. This default value for this option is 1. This grants permission to run local stored procedures from remote servers or remote stored procedures from the local server. To prevent local stored procedures from being run from a remote server or remote stored procedures from being run on the local server, this must be disabled. The Remote Access option controls the execution of local stored procedures on remote servers or remote stored procedures on local server. 'Remote access' functionality can be abused to launch a Denial-of-Service (DoS) attack on remote servers by off-loading query processing to a target, hence this should be disabled. This recommendation is applicable to SQL Server database instances.

#### Impact:

Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

#### Audit:

##### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its `Instance Overview` page
3. Ensure the database flag `remote access` that has been set is listed under the `Database flags` section.

##### From Google Cloud CLI

1. Ensure the below command returns `off` for every Cloud SQL SQL Server database instance

```
gcloud sql instances describe <INSTANCE_NAME> --format=json | jq  
'settings.databaseFlags[] | select(.name=="remote access")|.value'
```

In the output, database flags are listed under the `settings` as the collection `databaseFlags`.

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the SQL Server instance for which you want to enable to database flag.
3. Click `Edit`.
4. Scroll down to the `Flags` section.
5. To set a flag that has not been set on the instance before, click `Add item`, choose the flag `remote access` from the drop-down menu, and set its value to `off`.
6. Click `Save` to save your changes.
7. Confirm your changes under `Flags` on the Overview page.

### From Google Cloud CLI

1. Configure the `remote access` database flag for every Cloud SQL SQL Server database instance using the below command

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags "remote  
access=off"
```

#### Note:

This command will overwrite all database flags previously set. To keep those and add new ones, include the values for all flags you want set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

#### Default Value:

By default 'remote access' is 'on'.

#### References:

1. <https://cloud.google.com/sql/docs/sqlserver/flags>
2. <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-the-remote-access-server-configuration-option?view=sql-server-ver15>
3. [https://www.stigviewer.com/stig/ms\\_sql\\_server\\_2016\\_instance/2018-03-09/finding/V-79337](https://www.stigviewer.com/stig/ms_sql_server_2016_instance/2018-03-09/finding/V-79337)

### Additional Information:





**WARNING:** This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags -

<https://cloud.google.com/sql/docs/sqlserver/flags> - to see if your instance will be restarted when this patch is submitted.

**Note:** some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

**Note:** Configuring the above flag does not restart the Cloud SQL instance.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			



### 6.3.6 Ensure '3625 (trace flag)' database flag for all Cloud SQL SQL Server instances is set to 'on' (Automated)

#### Profile Applicability:

- Level 1

#### Description:

It is recommended to set `3625 (trace flag)` database flag for Cloud SQL SQL Server instance to `on`.

#### Rationale:

Microsoft SQL Trace Flags are frequently used to diagnose performance issues or to debug stored procedures or complex computer systems, but they may also be recommended by Microsoft Support to address behavior that is negatively impacting a specific workload. All documented trace flags and those recommended by Microsoft Support are fully supported in a production environment when used as directed.

`3625 (trace log)` Limits the amount of information returned to users who are not members of the `sysadmin` fixed server role, by masking the parameters of some error messages using `'*****'`. Setting this in a Google Cloud flag for the instance allows for security through obscurity and prevents the disclosure of sensitive information, hence this is recommended to set this flag globally to `on` to prevent the flag having been left off, or changed by bad actors. This recommendation is applicable to SQL Server database instances.

#### Impact:

Changing flags on a database may cause it to be restarted. The best time to do this is at a time where there is low usage.

#### Audit:

##### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its `Instance Overview` page
3. Ensure the database flag `3625` that has been set is listed under the `Database flags` section.

##### From Google Cloud CLI

1. Ensure the below command returns `on` for every Cloud SQL SQL Server database instance

```
gcloud sql instances describe <INSTANCE_NAME> --format=json | jq
'.settings.databaseFlags[] | select(.name=="3625")|.value'
```

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the SQL Server instance for which you want to enable the database flag.
3. Click `Edit`.
4. Scroll down to the `Flags` section.
5. To set a flag that has not been set on the instance before, click `Add item`, choose the flag `3625` from the drop-down menu, and set its value to `on`.
6. Click `Save` to save your changes.
7. Confirm your changes under `Flags` on the Overview page.

### From Google Cloud CLI

1. Configure the `3625` database flag for every Cloud SQL SQL Server database instance using the below command.

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags "3625=on"
```

## Note:

This command will overwrite all database flags previously set. To keep those and add new ones, include the values for all flags you want set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

## Default Value:

MySQL implementations by default have trace flags turned off, as they are used for logging purposes.

## References:

1. <https://cloud.google.com/sql/docs/sqlserver/flags>
2. <https://docs.microsoft.com/en-us/sql/t-sql/database-console-commands/dbcc-traceon-trace-flags-transact-sql?view=sql-server-ver15#trace-flags>
3. <https://github.com/ktaranov/sqlserver-kit/blob/master/SQL%20Server%20Trace%20Flag.md>







## Additional Information:

WARNING: This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags - <https://cloud.google.com/sql/docs/sqlserver/flags> - to see if your instance will be restarted when this patch is submitted.

**Note:** some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

**Note:** Configuring the above flag restarts the Cloud SQL instance.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b>5.1 <u>Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

### *6.3.7 Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is not set to 'on' (Automated)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

It is recommended not to set `contained database authentication` database flag for Cloud SQL on the SQL Server instance to `on`.

#### **Rationale:**

A contained database includes all database settings and metadata required to define the database and has no configuration dependencies on the instance of the Database Engine where the database is installed. Users can connect to the database without authenticating a login at the Database Engine level. Isolating the database from the Database Engine makes it possible to easily move the database to another instance of SQL Server. Contained databases have some unique threats that should be understood and mitigated by SQL Server Database Engine administrators. Most of the threats are related to the USER WITH PASSWORD authentication process, which moves the authentication boundary from the Database Engine level to the database level, hence this is recommended not to enable this flag. This recommendation is applicable to SQL Server database instances.

#### **Impact:**

When `contained database authentication` is off (0) for the instance, contained databases cannot be created, or attached to the Database Engine. Turning on logging will increase the required storage over time. Mismanaged logs may cause your storage costs to increase. Setting custom flags via command line on certain instances will cause all omitted flags to be reset to defaults. This may cause you to lose custom flags and could result in unforeseen complications or instance restarts. Because of this, it is recommended you apply these flags changes during a period of low usage.

#### **Audit:**

##### **From Google Cloud Console**

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the instance to open its `Instance Overview` page
3. Under the 'Database flags' section, if the database flag `contained database authentication` is present, then ensure that it is not set to 'on'.

## From Google Cloud CLI

1. Ensure the below command doesn't return `on` for any Cloud SQL for SQL Server database instance.

```
gcloud sql instances describe <INSTANCE_NAME> --format=json | jq  
' .settings.databaseFlags[] | select(.name=="contained database  
authentication")|.value '
```

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the SQL Server instance for which you want to enable to database flag.
3. Click `Edit`.
4. Scroll down to the `Flags` section.
5. If the flag `contained database authentication` is present and its value is set to `'on'`, then change it to `'off'`.
5. Click `Save`.
6. Confirm the changes under `Flags` on the Overview page.

## From Google Cloud CLI

1. If any Cloud SQL for SQL Server instance has the database flag `contained database authentication` set to `'on'`, then change it to `'off'` using the below command:

```
gcloud sql instances patch <INSTANCE_NAME> --database-flags "contained  
database authentication=off"
```

## Note:

This command will overwrite all database flags previously set. To keep those and add new ones, include the values for all flags to be set on the instance; any flag not specifically included is set to its default value. For flags that do not take a value, specify the flag name followed by an equals sign ("=").

## References:

1. <https://cloud.google.com/sql/docs/sqlserver/flags>
2. <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/contained-database-authentication-server-configuration-option?view=sql-server-ver15>
3. <https://docs.microsoft.com/en-us/sql/relational-databases/databases/security-best-practices-with-contained-databases?view=sql-server-ver15>

### Additional Information:







**WARNING:** This patch modifies database flag values, which may require your instance to be restarted. Check the list of supported flags -

<https://cloud.google.com/sql/docs/sqlserver/flags> - to see if your instance will be restarted when this patch is submitted.

**Note:** Some database flag settings can affect instance availability or stability, and remove the instance from the Cloud SQL SLA. For information about these flags, see Operational Guidelines.

**Note:** Configuring the above flag does not restart the Cloud SQL instance.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

## 6.4 Ensure That the Cloud SQL Database Instance Requires All Incoming Connections To Use SSL (Automated)

### Profile Applicability:

- Level 1

### Description:

It is recommended to enforce all incoming connections to SQL database instance to use SSL.

### Rationale:

SQL database connections if successfully trapped (MITM); can reveal sensitive data like credentials, database queries, query outputs etc. For security, it is recommended to always use SSL encryption when connecting to your instance. This recommendation is applicable for Postgresql, MySQL generation 1, MySQL generation 2 and SQL Server 2017 instances.

### Impact:

After enforcing SSL requirement for connections, existing client will not be able to communicate with Cloud SQL database instance unless they use SSL encrypted connections to communicate to Cloud SQL database instance.

### Audit:

#### From Google Cloud Console

1. Go to <https://console.cloud.google.com/sql/instances>.
2. Click on an instance name to see its configuration overview.
3. In the left-side panel, select `Connections`.
4. In the `Security` section, ensure that `Allow only SSL connections` option is selected.

#### From Google Cloud CLI

1. Get the detailed configuration for every SQL database instance using the following command:

```
gcloud sql instances list --format=json
```

Ensure that section `settings: ipConfiguration` has the parameter `sslMode` set to `ENCRYPTED_ONLY` .

### Remediation:

#### From Google Cloud Console

1. Go to <https://console.cloud.google.com/sql/instances>.
2. Click on an instance name to see its configuration overview.
3. In the left-side panel, select `Connections`.
4. In the `security` section, select `SSL mode` as `Allow only SSL connections`.
5. Under `Configure SSL server certificates` click `Create new certificate` and save the setting

## From Google Cloud CLI

To enforce SSL encryption for an instance run the command:

```
gcloud sql instances patch INSTANCE_NAME --ssl-mode= ENCRYPTED_ONLY
```

Note:

`RESTART` is required for type MySQL Generation 1 Instances (`backendType: FIRST_GEN`) to get this configuration in effect.

## Default Value:

By default parameter `settings: ipConfiguration: sslMode` is not set which is equivalent to `sslMode:ALLOW_UNENCRYPTED_AND_ENCRYPTED`.







## References:

1. <https://cloud.google.com/sql/docs/postgres/configure-ssl-instance/>

## Additional Information:

By default `Settings: ipConfiguration` has no `authorizedNetworks` set/configured. In that case even if by default `sslMode` is not set, which is equivalent to `sslMode:ALLOW_UNENCRYPTED_AND_ENCRYPTED` there is no risk as instance cannot be accessed outside of the network unless `authorizedNetworks` are configured. However, If default for `sslMode` is not updated to `ENCRYPTED_ONLY` any `authorizedNetworks` created later on will not enforce SSL only connection.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.			
v7	<b>16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u></b> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			



## 6.5 Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses (Automated)

### Profile Applicability:

- Level 1

### Description:

Database Server should accept connections only from trusted Network(s)/IP(s) and restrict access from public IP addresses.

### Rationale:

To minimize attack surface on a Database server instance, only trusted/known and required IP(s) should be white-listed to connect to it.

An authorized network should not have IPs/networks configured to `0.0.0.0/0` which will allow access to the instance from anywhere in the world. Note that authorized networks apply only to instances with public IPs.

### Impact:

The Cloud SQL database instance would not be available to public IP addresses.

### Audit:

#### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Click the instance name to open its `Instance details` page.
3. Under the `Configuration` section click `Edit configurations`
4. Under `Configuration options` expand the `Connectivity` section.
5. Ensure that no authorized network is configured to allow `0.0.0.0/0`.

#### From Google Cloud CLI

1. Get detailed configuration for every Cloud SQL database instance.

```
gcloud sql instances list --format=json
```

Ensure that the section `settings: ipConfiguration : authorizedNetworks` does not have any parameter value containing `0.0.0.0/0`.

### Remediation:

#### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Click the instance name to open its Instance details page.
3. Under the Configuration section click Edit configurations
4. Under Configuration options expand the Connectivity section.
5. Click the delete icon for the authorized network 0.0.0.0/0.
6. Click Save to update the instance.

### From Google Cloud CLI

Update the authorized network list by dropping off any addresses.

```
gcloud sql instances patch <INSTANCE_NAME> --authorized-networks=IP_ADDR1,IP_ADDR2...
```

### Prevention:

To prevent new SQL instances from being configured to accept incoming connections from any IP addresses, set up a Restrict Authorized Networks on Cloud SQL instances Organization Policy at: <https://console.cloud.google.com/iam-admin/orgpolicies/sql-restrictAuthorizedNetworks>.

### Default Value:

By default, authorized networks are not configured. Remote connection to Cloud SQL database instance is not possible unless authorized networks are configured.




### References:




1. <https://cloud.google.com/sql/docs/mysql/configure-ip>
2. <https://console.cloud.google.com/iam-admin/orgpolicies/sql-restrictAuthorizedNetworks>
3. <https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints>
4. <https://cloud.google.com/sql/docs/mysql/connection-org-policy>

### Additional Information:

There is no IPv6 configuration found for Google cloud SQL server services.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><b>14.6 <u>Protect Information through Access Control Lists</u></b></p> <p>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.</p>			

## 6.6 Ensure That Cloud SQL Database Instances Do Not Have Public IPs (Automated)

### Profile Applicability:

- Level 2

### Description:

It is recommended to configure Second Generation Sql instance to use private IPs instead of public IPs.

### Rationale:

To lower the organization's attack surface, Cloud SQL databases should not have public IPs. Private IPs provide improved network security and lower latency for your application.

### Impact:

Removing the public IP address on SQL instances may break some applications that relied on it for database connectivity.

### Audit:

#### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console:  
<https://console.cloud.google.com/sql/instances>
2. Ensure that every instance has a private IP address and no public IP address configured.

#### From Google Cloud CLI

1. List all Cloud SQL database instances using the following command:

```
gcloud sql instances list
```

2. For every instance of type `instanceType: CLOUD_SQL_INSTANCE` with `backendType: SECOND_GEN`, get detailed configuration. Ignore instances of type `READ_REPLICA_INSTANCE` because these instances inherit their settings from the primary instance. Also, note that first generation instances cannot be configured to have a private IP address.

```
gcloud sql instances describe <INSTANCE_NAME>
```

3. Ensure that the setting `ipAddresses` has an IP address configured of `type: PRIVATE` and has no IP address of `type: PRIMARY`. PRIMARY IP addresses are public addresses. An instance can have both a private and public address at the same time. Note also that you cannot use private IP with First Generation instances.

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console:  
<https://console.cloud.google.com/sql/instances>
2. Click the instance name to open its Instance details page.
3. Select the `Connections` tab.
4. Deselect the `Public IP` checkbox.
5. Click `Save` to update the instance.

### From Google Cloud CLI

1. For every instance remove its public IP and assign a private IP instead:

```
gcloud sql instances patch <INSTANCE_NAME> --network=<VPC_NETWORK_NAME> --no-assign-ip
```

2. Confirm the changes using the following command::

```
gcloud sql instances describe <INSTANCE_NAME>
```

## Prevention:

To prevent new SQL instances from getting configured with public IP addresses, set up a `Restrict Public IP access on Cloud SQL instances` Organization policy at:  
<https://console.cloud.google.com/iam-admin/orgpolicies/sql-restrictPublicIp>.

## Default Value:

By default, Cloud SQL instances have a public IP.







## References:

1. <https://cloud.google.com/sql/docs/mysql/configure-private-ip>
2. <https://cloud.google.com/sql/docs/mysql/private-ip>
3. <https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints>
4. <https://console.cloud.google.com/iam-admin/orgpolicies/sql-restrictPublicIp>

### Additional Information:

Replicas inherit their private IP status from their primary instance. You cannot configure a private IP directly on a replica.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

## 6.7 Ensure That Cloud SQL Database Instances Are Configured With Automated Backups (Automated)

### Profile Applicability:

- Level 1

### Description:

It is recommended to have all SQL database instances set to enable automated backups.

### Rationale:

Backups provide a way to restore a Cloud SQL instance to recover lost data or recover from a problem with that instance. Automated backups need to be set for any instance that contains data that should be protected from loss or damage. This recommendation is applicable for SQL Server, PostgreSQL, MySQL generation 1 and MySQL generation 2 instances.

### Impact:

Automated Backups will increase required size of storage and costs associated with it.

### Audit:

#### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Click the instance name to open its instance details page.
3. Go to the `Backups` menu.
4. Ensure that `Automated backups` is set to `Enabled` and `Backup time` is mentioned.

#### From Google Cloud CLI

1. List all Cloud SQL database instances using the following command:

```
gcloud sql instances list --format=json | jq '. | map(select(.instanceType != "READ_REPLICA_INSTANCE")) | .[].name'
```

NOTE: `gcloud` command has been added with the filter to exclude read-replicas instances, as GCP do not provide Automated Backups for read-replica instances.

2. Ensure that the below command returns `True` for every Cloud SQL database instance.

```
gcloud sql instances describe <INSTANCE_NAME> --  
format="value('Enabled':settings.backupConfiguration.enabled) "
```

## Remediation:

### From Google Cloud Console

1. Go to the Cloud SQL Instances page in the Google Cloud Console by visiting <https://console.cloud.google.com/sql/instances>.
2. Select the instance where the backups need to be configured.
3. Click `Edit`.
4. In the `Backups` section, check 'Enable automated backups', and choose a backup window.
5. Click `Save`.

### From Google Cloud CLI

1. List all Cloud SQL database instances using the following command:

```
gcloud sql instances list --format=json | jq '. | map(select(.instanceType !=  
"READ_REPLICA_INSTANCE")) | .[].name'
```

NOTE: `gcloud` command has been added with the filter to exclude read-replicas instances, as GCP do not provide Automated Backups for read-replica instances.

2. Enable `Automated backups` for every Cloud SQL database instance using the below command:

```
gcloud sql instances patch <INSTANCE_NAME> --backup-start-time <[HH:MM]>
```

The `backup-start-time` parameter is specified in 24-hour time, in the UTC±00 time zone, and specifies the start of a 4-hour backup window. Backups can start any time during the backup window.

## Default Value:







By default, automated backups are not configured for Cloud SQL instances. Data backup is not possible on any Cloud SQL instance unless Automated Backup is configured.

## References:

1. <https://cloud.google.com/sql/docs/mysql/backup-recovery/backups>
2. <https://cloud.google.com/sql/docs/postgres/backup-recovery/backing-up>



**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>11.2 <u>Perform Automated Backups</u></b> Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.			
v7	<b>10.1 <u>Ensure Regular Automated Back Ups</u></b> Ensure that all system data is automatically backed up on regular basis.			

## 7 BigQuery

This section addresses Google CloudPlatform BigQuery. BigQuery is a serverless, highly-scalable, and cost-effective cloud data warehouse with an in-memory BI Engine and machine learning built in.

## 7.1 Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible (Automated)

### Profile Applicability:

- Level 1

### Description:

It is recommended that the IAM policy on BigQuery datasets does not allow anonymous and/or public access.

### Rationale:

Granting permissions to `allUsers` or `allAuthenticatedUsers` allows anyone to access the dataset. Such access might not be desirable if sensitive data is being stored in the dataset. Therefore, ensure that anonymous and/or public access to a dataset is not allowed.

### Impact:

The dataset is not publicly accessible. Explicit modification of IAM privileges would be necessary to make them publicly accessible.

### Audit:

#### From Google Cloud Console

1. Go to BigQuery by visiting: <https://console.cloud.google.com/bigquery>.
2. Select a dataset from `Resources`.
3. Click `SHARING` near the right side of the window and select `Permissions`.
4. Validate that none of the attached roles contain `allUsers` or `allAuthenticatedUsers`.

#### From Google Cloud CLI

List the name of all datasets.

```
bq ls
```

Retrieve each dataset details using the following command:

```
bq show PROJECT_ID:DATASET_NAME
```

Ensure that `allUsers` and `allAuthenticatedUsers` have not been granted access to the dataset.

### Remediation:

#### From Google Cloud Console

1. Go to BigQuery by visiting: <https://console.cloud.google.com/bigquery>.

2. Select the dataset from 'Resources'.
3. Click `SHARING` near the right side of the window and select `Permissions`.
4. Review each attached role.
5. Click the delete icon for each member `allUsers` or `allAuthenticatedUsers`. On the popup click `Remove`.

## From Google Cloud CLI

List the name of all datasets.

```
bq ls
```

Retrieve the data set details:

```
bq show --format=prettyjson PROJECT_ID:DATASET_NAME > PATH_TO_FILE
```

In the access section of the JSON file, update the dataset information to remove all roles containing `allUsers` or `allAuthenticatedUsers`.

Update the dataset:

```
bq update --source PATH_TO_FILE PROJECT_ID:DATASET_NAME
```

## Prevention:

You can prevent Bigquery dataset from becoming publicly accessible by setting up the Domain restricted sharing organization policy at:

<https://console.cloud.google.com/iam-admin/orgpolicies/iam-allowedPolicyMemberDomains> .







## Default Value:

By default, BigQuery datasets are not publicly accessible.

## References:

1. <https://cloud.google.com/bigquery/docs/dataset-access-controls>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

## 7.2 Ensure That All BigQuery Tables Are Encrypted With Customer-Managed Encryption Key (CMEK) (Automated)

### Profile Applicability:

- Level 2

### Description:

BigQuery by default encrypts the data at rest by employing Envelope Encryption using Google managed cryptographic keys. The data is encrypted using the data encryption keys and data encryption keys themselves are further encrypted using key encryption keys. This is seamless and does not require any additional input from the user. However, if you want to have greater control, Customer-managed encryption keys (CMEK) can be used as encryption key management solution for BigQuery Data Sets. If CMEK is used, the CMEK is used to encrypt the data encryption keys instead of using google-managed encryption keys.

### Rationale:

BigQuery by default encrypts the data at rest by employing Envelope Encryption using Google managed cryptographic keys. This is seamless and does not require any additional input from the user.

For greater control over the encryption, customer-managed encryption keys (CMEK) can be used as encryption key management solution for BigQuery tables. The CMEK is used to encrypt the data encryption keys instead of using google-managed encryption keys. BigQuery stores the table and CMEK association and the encryption/decryption is done automatically.

Applying the Default Customer-managed keys on BigQuery data sets ensures that all the new tables created in the future will be encrypted using CMEK but existing tables need to be updated to use CMEK individually.

Note: Google does not store your keys on its servers and cannot access your protected data unless you provide the key. This also means that if you forget or lose your key, there is no way for Google to recover the key or to recover any data encrypted with the lost key.

### Impact:

Using Customer-managed encryption keys (CMEK) will incur additional labor-hour investment to create, protect, and manage the keys.

### Audit:

#### From Google Cloud Console

1. Go to Analytics
2. Go to BigQuery

3. Under `SQL Workspace`, select the project
4. Select `Data Set`, select the table
5. Go to `Details` tab
6. Under `Table info`, verify `Customer-managed key` is present.
7. Repeat for each table in all data sets for all projects.

### From Google Cloud CLI

List all dataset names

```
bq ls
```

Use the following command to view the table details. Verify the `kmsKeyName` is present.

```
bq show <table_object>
```

### Remediation:

#### From Google Cloud CLI

Use the following command to copy the data. The source and the destination needs to be same in case copying to the original table.

```
bq cp --destination_kms_key <customer_managed_key>  
source_dataset.source_table destination_dataset.destination_table
```

### Default Value:

Google Managed keys are used as `key encryption keys`.

### References:

1. <https://cloud.google.com/bigquery/docs/customer-managed-encryption>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 Encrypt Sensitive Data at Rest</b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	<b>14.8 Encrypt Sensitive Information at Rest</b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

## 7.3 Ensure That a Default Customer-Managed Encryption Key (CMEK) Is Specified for All BigQuery Data Sets (Automated)

### Profile Applicability:

- Level 2

### Description:

BigQuery by default encrypts the data at rest by employing `Envelope Encryption` using Google managed cryptographic keys. The data is encrypted using the `data encryption keys` and data encryption keys themselves are further encrypted using `key encryption keys`. This is seamless and does not require any additional input from the user. However, if you want to have greater control, Customer-managed encryption keys (CMEK) can be used as encryption key management solution for BigQuery Data Sets.

### Rationale:

BigQuery by default encrypts the data at rest by employing `Envelope Encryption` using Google managed cryptographic keys. This is seamless and does not require any additional input from the user.

For greater control over the encryption, customer-managed encryption keys (CMEK) can be used as encryption key management solution for BigQuery Data Sets. Setting a Default Customer-managed encryption key (CMEK) for a data set ensure any tables created in future will use the specified CMEK if none other is provided.

Note: Google does not store your keys on its servers and cannot access your protected data unless you provide the key. This also means that if you forget or lose your key, there is no way for Google to recover the key or to recover any data encrypted with the lost key.

### Impact:

Using Customer-managed encryption keys (CMEK) will incur additional labor-hour investment to create, protect, and manage the keys.

### Audit:

#### From Google Cloud Console

1. Go to `Analytics`
2. Go to `BigQuery`
3. Under `Analysis` click on `SQL Workspaces`, select the project
4. Select `Data Set`
5. Ensure `Customer-managed key` is present under `Dataset info` section.
6. Repeat for each data set in all projects.

## From Google Cloud CLI

List all dataset names

```
bq ls
```

Use the following command to view each dataset details.

```
bq show <data_set_object>
```

Verify the `kmsKeyName` is present.

## Remediation:

## From Google Cloud CLI

The default CMEK for existing data sets can be updated by specifying the default key in the `EncryptionConfiguration.kmsKeyName` field when calling the `datasets.insert` or `datasets.patch` methods




## Default Value:

Google Managed keys are used as `key encryption keys`.

## References:

1. <https://cloud.google.com/bigquery/docs/customer-managed-encryption>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	<b>14.8 <u>Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			



## 7.4 Ensure all data in BigQuery has been classified (Manual)

### Profile Applicability:

- Level 2

### Description:

BigQuery tables can contain sensitive data that for security purposes should be discovered, monitored, classified, and protected. Google Cloud's Sensitive Data Protection tools can automatically provide data classification of all BigQuery data across an organization.

### Rationale:

Using a cloud service or 3rd party software to continuously monitor and automate the process of data discovery and classification for BigQuery tables is an important part of protecting the data.

Sensitive Data Protection is a fully managed data protection and data privacy platform that uses machine learning and pattern matching to discover and classify sensitive data in Google Cloud.

### Impact:

There is a cost associated with using Sensitive Data Protection. There is also typically a cost associated with 3rd party tools that perform similar processes and protection.

### Audit:

1. Go to Cloud DLP by visiting <https://console.cloud.google.com/dlp/landing/dataProfiles/configurations>.
2. Verify there is a discovery scan configuration either for the organization or project.

### Remediation:

#### Enable profiling:

1. Go to Cloud DLP by visiting <https://console.cloud.google.com/dlp/landing/dataProfiles/configurations>
2. Click "Create Configuration"
3. For projects follow <https://cloud.google.com/dlp/docs/profile-project>. For organizations or folders follow <https://cloud.google.com/dlp/docs/profile-org-folder>

## Review findings:

- Columns or tables with high data risk have evidence of sensitive information without additional protections. To lower the data risk score, consider doing the following:
- For columns containing sensitive data, apply a BigQuery policy tag to restrict access to accounts with specific access rights.
- De-identify the raw sensitive data using de-identification techniques like masking and tokenization.









## Incorporate findings into your security and governance operations:

- Enable sending findings into your security and posture services. You can publish data profiles to Security Command Center and Chronicle.
- Automate remediation or enable alerting of new or changed data risk with Pub/Sub.

## References:

1. <https://cloud.google.com/dlp/docs/data-profiles>
2. <https://cloud.google.com/dlp/docs/analyze-data-profiles>
3. <https://cloud.google.com/dlp/docs/data-profiles-remediation>
4. <https://cloud.google.com/dlp/docs/send-profiles-to-scc>
5. <https://cloud.google.com/dlp/docs/profile-org-folder#chronicle>
6. <https://cloud.google.com/dlp/docs/profile-org-folder#publish-pubsub>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.1 Establish and Maintain a Data Management Process</b> Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<b>3.7 Establish and Maintain a Data Classification Scheme</b> Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

## 8 Dataproc

Dataproc, a service within Google Cloud Platform (GCP), offers a fully managed and easy-to-use service for running Apache Spark and Apache Hadoop clusters. It simplifies the management of big data processing and analytics by handling the underlying infrastructure, allowing users to focus on data analysis rather than operational complexities. Dataproc is notable for its quick start-up and scaling capabilities, accommodating data loads from gigabytes to petabytes efficiently. It seamlessly integrates with other GCP services like BigQuery, Cloud Storage, and Cloud Bigtable, enhancing data processing and transfer capabilities. Additionally, its cost-effectiveness, with a pay-as-you-go model, makes it an attractive option for businesses seeking scalable and efficient big data solutions.

<https://cloud.google.com/dataproc>

## 8.1 Ensure that Dataproc Cluster is encrypted using Customer-Managed Encryption Key (Automated)

### Profile Applicability:

- Level 2

### Description:

When you use Dataproc, cluster and job data is stored on Persistent Disks (PDs) associated with the Compute Engine VMs in your cluster and in a Cloud Storage staging bucket. This PD and bucket data is encrypted using a Google-generated data encryption key (DEK) and key encryption key (KEK). The CMEK feature allows you to create, use, and revoke the key encryption key (KEK). Google still controls the data encryption key (DEK).

### Rationale:

"Cloud services offer the ability to protect data related to those services using encryption keys managed by the customer within Cloud KMS. These encryption keys are called customer-managed encryption keys (CMEK). When you protect data in Google Cloud services with CMEK, the CMEK key is within your control.

### Impact:

Using Customer Managed Keys involves additional overhead in maintenance by administrators.

### Audit:

#### From Google Cloud Console

1. Login to the GCP Console and navigate to the Dataproc Cluster page by visiting <https://console.cloud.google.com/dataproc/clusters>.
2. Select the project from the project dropdown list.
3. On the `Dataproc Clusters` page, select the cluster and click on the Name attribute value that you want to examine.
4. On the `details` page, select the `Configurations` tab.
5. On the `Configurations` tab, check the `Encryption type` configuration attribute value. If the value is set to `Google-managed key`, then Dataproc Cluster is not encrypted with Customer managed encryption keys.

Repeat step no. 3 - 5 for other Dataproc Clusters available in the selected project.

6. Change the project from the project dropdown list and repeat the audit procedure for other projects.

## From Google Cloud CLI

1. Run clusters list command to list all the Dataproc Clusters available in the region:

```
gcloud dataproc clusters list --region='us-central1'
```

2. Run clusters describe command to get the key details of the selected cluster:

```
gcloud dataproc clusters describe <cluster_name> --region=us-central1 --  
flatten=config.encryptionConfig.gcePdKmsKeyName
```

3. If the above command output return "null", then the selected cluster is not encrypted with Customer managed encryption keys.
4. Repeat step no. 2 and 3 for other Dataproc Clusters available in the selected region. Change the region by updating --region and repeat step no. 2 for other clusters available in the project. Change the project by running the below command and repeat the audit procedure for other Dataproc clusters available in other projects:

```
gcloud config set project <project_ID>
```

## Remediation:

### From Google Cloud Console

1. Login to the GCP Console and navigate to the Dataproc Cluster page by visiting <https://console.cloud.google.com/dataproc/clusters>.
2. Select the project from the projects dropdown list.
3. On the Dataproc Cluster page, click on the Create Cluster to create a new cluster with Customer managed encryption keys.
4. On Create a cluster page, perform below steps:
  - Inside Set up cluster section perform below steps:
    - In the Name textbox, provide a name for your cluster.
      - From Location select the location in which you want to deploy a cluster.
      - Configure other configurations as per your requirements.
  - Inside Configure Nodes and Customize cluster section configure the settings as per your requirements.
  - Inside Manage security section, perform below steps:
    - From Encryption, select Customer-managed key.
    - Select a customer-managed key from dropdown list.
    - Ensure that the selected KMS Key have Cloud KMS CryptoKey Encrypter/Decrypter role assign to Dataproc Cluster service account ("serviceAccount:service-<project\_number>@compute-system.iam.gserviceaccount.com").
    - Click on Create to create a cluster.

- Once the cluster is created migrate all your workloads from the older cluster to the new cluster and delete the old cluster by performing the below steps:
  - On the **Clusters** page, select the old cluster and click on **Delete cluster**.
  - On the **Confirm deletion** window, click on **Confirm** to delete the cluster.
  - Repeat step above for other Dataproc clusters available in the selected project.
- Change the project from the project dropdown list and repeat the remediation procedure for other Dataproc clusters available in other projects.

### From Google Cloud CLI

Before creating cluster ensure that the selected KMS Key have Cloud KMS CryptoKey Encrypter/Decrypter role assign to Dataproc Cluster service account ("serviceAccount:service-<project\_number>@compute-system.iam.gserviceaccount.com").

Run clusters create command to create new cluster with customer-managed key:

```
gcloud dataproc clusters create <cluster_name> --region=us-central1 --gce-pd-kms-key=<key_resource_name>
```

The above command will create a new cluster in the selected region.

Once the cluster is created migrate all your workloads from the older cluster to the new cluster and Run clusters delete command to delete cluster:

```
gcloud dataproc clusters delete <cluster_name> --region=us-central1
```

Repeat step no. 1 to create a new Dataproc cluster.




Change the project by running the below command and repeat the remediation procedure for other projects:

```
gcloud config set project <project_ID>
```

### References:

1. <https://cloud.google.com/docs/security/encryption/default-encryption>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	<b>14.8 <u>Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			



# Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
<b>1</b>	<b>Identity and Access Management</b>		
1.1	Ensure that Corporate Login Credentials are Used (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Ensure that Multi-Factor Authentication is 'Enabled' for All Non-Service Accounts (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Ensure that Security Key Enforcement is Enabled for All Admin Accounts (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.4	Ensure That There Are Only GCP-Managed Service Account Keys for Each Service Account (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5	Ensure That Service Account Has No Admin Privileges (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure That IAM Users Are Not Assigned the Service Account User or Service Account Token Creator Roles at Project Level (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.7	Ensure User-Managed/External Keys for Service Accounts Are Rotated Every 90 Days or Fewer (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.8	Ensure That Separation of Duties Is Enforced While Assigning Service Account Related Roles to Users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.9	Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.10	Ensure KMS Encryption Keys Are Rotated Within a Period of 90 Days (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.11	Ensure That Separation of Duties Is Enforced While Assigning KMS Related Roles to Users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>



CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.12	Ensure API Keys Only Exist for Active Services (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.13	Ensure API Keys Are Restricted To Use by Only Specified Hosts and Apps (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.14	Ensure API Keys Are Restricted to Only APIs That Application Needs Access (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.15	Ensure API Keys Are Rotated Every 90 Days (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.16	Ensure Essential Contacts is Configured for Organization (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.17	Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2</b>	<b>Logging and Monitoring</b>		
2.1	Ensure That Cloud Audit Logging Is Configured Properly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure That Sinks Are Configured for All Log Entries (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket Lock (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure Log Metric Filter and Alerts Exist for Project Ownership Assignments/Changes (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure That the Log Metric Filter and Alerts Exist for Audit Configuration Changes (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.8	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.9	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.10	Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.11	Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.12	Ensure That Cloud DNS Logging Is Enabled for All VPC Networks (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.13	Ensure Cloud Asset Inventory Is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.14	Ensure 'Access Transparency' is 'Enabled' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.15	Ensure 'Access Approval' is 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.16	Ensure Logging is enabled for HTTP(S) Load Balancer (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>3</b>	<b>Networking</b>		
3.1	Ensure That the Default Network Does Not Exist in a Project (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure Legacy Networks Do Not Exist for Older Projects (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure That DNSSEC Is Enabled for Cloud DNS (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Ensure That RSASHA1 Is Not Used for the Key-Signing Key in Cloud DNS DNSSEC (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Ensure That RSASHA1 Is Not Used for the Zone-Signing Key in Cloud DNS DNSSEC (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.6	Ensure That SSH Access Is Restricted From the Internet (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure That RDP Access Is Restricted From the Internet (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.9	Ensure No HTTPS or SSL Proxy Load Balancers Permit SSL Policies With Weak Cipher Suites (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.10	Use Identity Aware Proxy (IAP) to Ensure Only Traffic From Google IP Addresses are 'Allowed' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>4</b>	<b>Virtual Machines</b>		
4.1	Ensure That Instances Are Not Configured To Use the Default Service Account (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure “Block Project-Wide SSH Keys” Is Enabled for VM Instances (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure Oslogin Is Enabled for a Project (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5	Ensure ‘Enable Connecting to Serial Ports’ Is Not Enabled for VM Instance (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.6	Ensure That IP Forwarding Is Not Enabled on Instances (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7	Ensure VM Disks for Critical VMs Are Encrypted With Customer-Supplied Encryption Keys (CSEK) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.8	Ensure Compute Instances Are Launched With Shielded VM Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.9	Ensure That Compute Instances Do Not Have Public IP Addresses (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.10	Ensure That App Engine Applications Enforce HTTPS Connections (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.11	Ensure That Compute Instances Have Confidential Computing Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.12	Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5</b>	<b>Storage</b>		
5.1	Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Ensure That Cloud Storage Buckets Have Uniform Bucket-Level Access Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>6</b>	<b>Cloud SQL Database Services</b>		
<b>6.1</b>	<b>MySQL Database</b>		
6.1.1	Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure 'Skip_show_database' Database Flag for Cloud SQL MySQL Instance Is Set to 'On' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.3	Ensure That the 'Local_infile' Database Flag for a Cloud SQL MySQL Instance Is Set to 'Off' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>6.2</b>	<b>PostgreSQL Database</b>		
6.2.1	Ensure 'Log_error_verbosity' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'DEFAULT' or Stricter (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.2.2	Ensure That the 'Log_connections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.3	Ensure That the 'Log_disconnections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.4	Ensure 'Log_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set Appropriately (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.5	Ensure that the 'Log_min_messages' Flag for a Cloud SQL PostgreSQL Instance is set at minimum to 'Warning' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.6	Ensure 'Log_min_error_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Error' or Stricter (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.7	Ensure That the 'Log_min_duration_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to '-1' (Disabled) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.8	Ensure That 'cloudsql.enable_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>6.3</b>	<b>SQL Server</b>		
6.3.1	Ensure 'external scripts enabled' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.3.2	Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.3.3	Ensure 'user Connections' Database Flag for Cloud Sql Sql Server Instance Is Set to a Non-limiting Value (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.3.4	Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.3.5	Ensure 'remote access' database flag for Cloud SQL SQL Server instance is set to 'off' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.3.6	Ensure '3625 (trace flag)' database flag for all Cloud SQL Server instances is set to 'on' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.3.7	Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is not set to 'on' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure That the Cloud SQL Database Instance Requires All Incoming Connections To Use SSL (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.5	Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.6	Ensure That Cloud SQL Database Instances Do Not Have Public IPs (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.7	Ensure That Cloud SQL Database Instances Are Configured With Automated Backups (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>7</b>	<b>BigQuery</b>		
7.1	Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Ensure That All BigQuery Tables Are Encrypted With Customer-Managed Encryption Key (CMEK) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.3	Ensure That a Default Customer-Managed Encryption Key (CMEK) Is Specified for All BigQuery Data Sets (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.4	Ensure all data in BigQuery has been classified (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>8</b>	<b>Dataproc</b>		
8.1	Ensure that Dataproc Cluster is encrypted using Customer-Managed Encryption Key (Automated)	<input type="checkbox"/>	<input type="checkbox"/>



# Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.5	Ensure That Service Account Has No Admin Privileges	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure That IAM Users Are Not Assigned the Service Account User or Service Account Token Creator Roles at Project Level	<input type="checkbox"/>	<input type="checkbox"/>
1.8	Ensure That Separation of Duties Is Enforced While Assigning Service Account Related Roles to Users	<input type="checkbox"/>	<input type="checkbox"/>
1.9	Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
1.11	Ensure That Separation of Duties Is Enforced While Assigning KMS Related Roles to Users	<input type="checkbox"/>	<input type="checkbox"/>
1.12	Ensure API Keys Only Exist for Active Services	<input type="checkbox"/>	<input type="checkbox"/>
1.16	Ensure Essential Contacts is Configured for Organization	<input type="checkbox"/>	<input type="checkbox"/>
2.1	Ensure That Cloud Audit Logging Is Configured Properly	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure That Sinks Are Configured for All Log Entries	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket Lock	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure Log Metric Filter and Alerts Exist for Project Ownership Assignments/Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure That the Log Metric Filter and Alerts Exist for Audit Configuration Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.9	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.10	Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes	<input type="checkbox"/>	<input type="checkbox"/>



Recommendation		Set Correctly	
		Yes	No
2.11	Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.12	Ensure That Cloud DNS Logging Is Enabled for All VPC Networks	<input type="checkbox"/>	<input type="checkbox"/>
2.13	Ensure Cloud Asset Inventory Is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.14	Ensure 'Access Transparency' is 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.15	Ensure 'Access Approval' is 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.16	Ensure Logging is enabled for HTTP(S) Load Balancer	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Ensure That SSH Access Is Restricted From the Internet	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure That RDP Access Is Restricted From the Internet	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network	<input type="checkbox"/>	<input type="checkbox"/>
4.9	Ensure That Compute Instances Do Not Have Public IP Addresses	<input type="checkbox"/>	<input type="checkbox"/>
4.12	Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects	<input type="checkbox"/>	<input type="checkbox"/>
5.1	Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Ensure That Cloud Storage Buckets Have Uniform Bucket-Level Access Enabled	<input type="checkbox"/>	<input type="checkbox"/>
6.1.1	Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure 'Skip_show_database' Database Flag for Cloud SQL MySQL Instance Is Set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.2	Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.3	Ensure 'user Connections' Database Flag for Cloud Sql Sql Server Instance Is Set to a Non-limiting Value	<input type="checkbox"/>	<input type="checkbox"/>
6.3.4	Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured	<input type="checkbox"/>	<input type="checkbox"/>
6.3.6	Ensure '3625 (trace flag)' database flag for all Cloud SQL SQL Server instances is set to 'on'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.7	Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is not set to 'on'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
6.5	Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses	<input type="checkbox"/>	<input type="checkbox"/>
6.6	Ensure That Cloud SQL Database Instances Do Not Have Public IPs	<input type="checkbox"/>	<input type="checkbox"/>
6.7	Ensure That Cloud SQL Database Instances Are Configured With Automated Backups	<input type="checkbox"/>	<input type="checkbox"/>
7.1	Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
7.4	Ensure all data in BigQuery has been classified	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure that Corporate Login Credentials are Used	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Ensure that Multi-Factor Authentication is 'Enabled' for All Non-Service Accounts	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Ensure that Security Key Enforcement is Enabled for All Admin Accounts	<input type="checkbox"/>	<input type="checkbox"/>
1.5	Ensure That Service Account Has No Admin Privileges	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure That IAM Users Are Not Assigned the Service Account User or Service Account Token Creator Roles at Project Level	<input type="checkbox"/>	<input type="checkbox"/>
1.8	Ensure That Separation of Duties Is Enforced While Assigning Service Account Related Roles to Users	<input type="checkbox"/>	<input type="checkbox"/>
1.9	Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
1.11	Ensure That Separation of Duties Is Enforced While Assigning KMS Related Roles to Users	<input type="checkbox"/>	<input type="checkbox"/>
1.12	Ensure API Keys Only Exist for Active Services	<input type="checkbox"/>	<input type="checkbox"/>
1.16	Ensure Essential Contacts is Configured for Organization	<input type="checkbox"/>	<input type="checkbox"/>
1.17	Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager	<input type="checkbox"/>	<input type="checkbox"/>
2.1	Ensure That Cloud Audit Logging Is Configured Properly	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure That Sinks Are Configured for All Log Entries	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket Lock	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure Log Metric Filter and Alerts Exist for Project Ownership Assignments/Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure That the Log Metric Filter and Alerts Exist for Audit Configuration Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.7	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.9	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.10	Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.11	Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.12	Ensure That Cloud DNS Logging Is Enabled for All VPC Networks	<input type="checkbox"/>	<input type="checkbox"/>
2.13	Ensure Cloud Asset Inventory Is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.14	Ensure 'Access Transparency' is 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.15	Ensure 'Access Approval' is 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.16	Ensure Logging is enabled for HTTP(S) Load Balancer	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure That the Default Network Does Not Exist in a Project	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure Legacy Networks Do Not Exist for Older Projects	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure That DNSSEC Is Enabled for Cloud DNS	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Ensure That RSASHA1 Is Not Used for the Key-Signing Key in Cloud DNS DNSSEC	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Ensure That RSASHA1 Is Not Used for the Zone-Signing Key in Cloud DNS DNSSEC	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Ensure That SSH Access Is Restricted From the Internet	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure That RDP Access Is Restricted From the Internet	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network	<input type="checkbox"/>	<input type="checkbox"/>
3.9	Ensure No HTTPS or SSL Proxy Load Balancers Permit SSL Policies With Weak Cipher Suites	<input type="checkbox"/>	<input type="checkbox"/>
3.10	Use Identity Aware Proxy (IAP) to Ensure Only Traffic From Google IP Addresses are 'Allowed'	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure That Instances Are Not Configured To Use the Default Service Account	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.2	Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure “Block Project-Wide SSH Keys” Is Enabled for VM Instances	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure Oslogin Is Enabled for a Project	<input type="checkbox"/>	<input type="checkbox"/>
4.5	Ensure ‘Enable Connecting to Serial Ports’ Is Not Enabled for VM Instance	<input type="checkbox"/>	<input type="checkbox"/>
4.6	Ensure That IP Forwarding Is Not Enabled on Instances	<input type="checkbox"/>	<input type="checkbox"/>
4.8	Ensure Compute Instances Are Launched With Shielded VM Enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.9	Ensure That Compute Instances Do Not Have Public IP Addresses	<input type="checkbox"/>	<input type="checkbox"/>
4.10	Ensure That App Engine Applications Enforce HTTPS Connections	<input type="checkbox"/>	<input type="checkbox"/>
4.12	Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects	<input type="checkbox"/>	<input type="checkbox"/>
5.1	Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Ensure That Cloud Storage Buckets Have Uniform Bucket-Level Access Enabled	<input type="checkbox"/>	<input type="checkbox"/>
6.1.1	Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure ‘Skip_show_database’ Database Flag for Cloud SQL MySQL Instance Is Set to ‘On’	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1	Ensure ‘Log_error_verbosity’ Database Flag for Cloud SQL PostgreSQL Instance Is Set to ‘DEFAULT’ or Stricter	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2	Ensure That the ‘Log_connections’ Database Flag for Cloud SQL PostgreSQL Instance Is Set to ‘On’	<input type="checkbox"/>	<input type="checkbox"/>
6.2.3	Ensure That the ‘Log_disconnections’ Database Flag for Cloud SQL PostgreSQL Instance Is Set to ‘On’	<input type="checkbox"/>	<input type="checkbox"/>
6.2.4	Ensure ‘Log_statement’ Database Flag for Cloud SQL PostgreSQL Instance Is Set Appropriately	<input type="checkbox"/>	<input type="checkbox"/>
6.2.5	Ensure that the ‘Log_min_messages’ Flag for a Cloud SQL PostgreSQL Instance is set at minimum to 'Warning'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
6.2.6	Ensure 'Log_min_error_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Error' or Stricter	<input type="checkbox"/>	<input type="checkbox"/>
6.2.7	Ensure That the 'Log_min_duration_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to '-1' (Disabled)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.8	Ensure That 'cloudsql.enable_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging	<input type="checkbox"/>	<input type="checkbox"/>
6.3.2	Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.3	Ensure 'user Connections' Database Flag for Cloud Sql Sql Server Instance Is Set to a Non-limiting Value	<input type="checkbox"/>	<input type="checkbox"/>
6.3.4	Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured	<input type="checkbox"/>	<input type="checkbox"/>
6.3.5	Ensure 'remote access' database flag for Cloud SQL SQL Server instance is set to 'off'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.6	Ensure '3625 (trace flag)' database flag for all Cloud SQL Server instances is set to 'on'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.7	Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is not set to 'on'	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure That the Cloud SQL Database Instance Requires All Incoming Connections To Use SSL	<input type="checkbox"/>	<input type="checkbox"/>
6.5	Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses	<input type="checkbox"/>	<input type="checkbox"/>
6.6	Ensure That Cloud SQL Database Instances Do Not Have Public IPs	<input type="checkbox"/>	<input type="checkbox"/>
6.7	Ensure That Cloud SQL Database Instances Are Configured With Automated Backups	<input type="checkbox"/>	<input type="checkbox"/>
7.1	Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
7.4	Ensure all data in BigQuery has been classified	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure that Corporate Login Credentials are Used	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Ensure that Multi-Factor Authentication is 'Enabled' for All Non-Service Accounts	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Ensure that Security Key Enforcement is Enabled for All Admin Accounts	<input type="checkbox"/>	<input type="checkbox"/>
1.5	Ensure That Service Account Has No Admin Privileges	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure That IAM Users Are Not Assigned the Service Account User or Service Account Token Creator Roles at Project Level	<input type="checkbox"/>	<input type="checkbox"/>
1.8	Ensure That Separation of Duties Is Enforced While Assigning Service Account Related Roles to Users	<input type="checkbox"/>	<input type="checkbox"/>
1.9	Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
1.10	Ensure KMS Encryption Keys Are Rotated Within a Period of 90 Days	<input type="checkbox"/>	<input type="checkbox"/>
1.11	Ensure That Separation of Duties Is Enforced While Assigning KMS Related Roles to Users	<input type="checkbox"/>	<input type="checkbox"/>
1.12	Ensure API Keys Only Exist for Active Services	<input type="checkbox"/>	<input type="checkbox"/>
1.16	Ensure Essential Contacts is Configured for Organization	<input type="checkbox"/>	<input type="checkbox"/>
1.17	Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager	<input type="checkbox"/>	<input type="checkbox"/>
2.1	Ensure That Cloud Audit Logging Is Configured Properly	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure That Sinks Are Configured for All Log Entries	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket Lock	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure Log Metric Filter and Alerts Exist for Project Ownership Assignments/Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure That the Log Metric Filter and Alerts Exist for Audit Configuration Changes	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.6	Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.9	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.10	Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.11	Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.12	Ensure That Cloud DNS Logging Is Enabled for All VPC Networks	<input type="checkbox"/>	<input type="checkbox"/>
2.13	Ensure Cloud Asset Inventory Is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.14	Ensure 'Access Transparency' is 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.15	Ensure 'Access Approval' is 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.16	Ensure Logging is enabled for HTTP(S) Load Balancer	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure That the Default Network Does Not Exist in a Project	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure Legacy Networks Do Not Exist for Older Projects	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure That DNSSEC Is Enabled for Cloud DNS	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Ensure That RSASHA1 Is Not Used for the Key-Signing Key in Cloud DNS DNSSEC	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Ensure That RSASHA1 Is Not Used for the Zone-Signing Key in Cloud DNS DNSSEC	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Ensure That SSH Access Is Restricted From the Internet	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure That RDP Access Is Restricted From the Internet	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network	<input type="checkbox"/>	<input type="checkbox"/>
3.9	Ensure No HTTPS or SSL Proxy Load Balancers Permit SSL Policies With Weak Cipher Suites	<input type="checkbox"/>	<input type="checkbox"/>
3.10	Use Identity Aware Proxy (IAP) to Ensure Only Traffic From Google IP Addresses are 'Allowed'	<input type="checkbox"/>	<input type="checkbox"/>



Recommendation		Set Correctly	
		Yes	No
4.1	Ensure That Instances Are Not Configured To Use the Default Service Account	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure “Block Project-Wide SSH Keys” Is Enabled for VM Instances	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure Oslogin Is Enabled for a Project	<input type="checkbox"/>	<input type="checkbox"/>
4.5	Ensure ‘Enable Connecting to Serial Ports’ Is Not Enabled for VM Instance	<input type="checkbox"/>	<input type="checkbox"/>
4.6	Ensure That IP Forwarding Is Not Enabled on Instances	<input type="checkbox"/>	<input type="checkbox"/>
4.7	Ensure VM Disks for Critical VMs Are Encrypted With Customer-Supplied Encryption Keys (CSEK)	<input type="checkbox"/>	<input type="checkbox"/>
4.8	Ensure Compute Instances Are Launched With Shielded VM Enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.9	Ensure That Compute Instances Do Not Have Public IP Addresses	<input type="checkbox"/>	<input type="checkbox"/>
4.10	Ensure That App Engine Applications Enforce HTTPS Connections	<input type="checkbox"/>	<input type="checkbox"/>
4.11	Ensure That Compute Instances Have Confidential Computing Enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.12	Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects	<input type="checkbox"/>	<input type="checkbox"/>
5.1	Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Ensure That Cloud Storage Buckets Have Uniform Bucket-Level Access Enabled	<input type="checkbox"/>	<input type="checkbox"/>
6.1.1	Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure ‘Skip_show_database’ Database Flag for Cloud SQL MySQL Instance Is Set to ‘On’	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1	Ensure ‘Log_error_verbosity’ Database Flag for Cloud SQL PostgreSQL Instance Is Set to ‘DEFAULT’ or Stricter	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2	Ensure That the ‘Log_connections’ Database Flag for Cloud SQL PostgreSQL Instance Is Set to ‘On’	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
6.2.3	Ensure That the 'Log_disconnections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
6.2.4	Ensure 'Log_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set Appropriately	<input type="checkbox"/>	<input type="checkbox"/>
6.2.5	Ensure that the 'Log_min_messages' Flag for a Cloud SQL PostgreSQL Instance is set at minimum to 'Warning'	<input type="checkbox"/>	<input type="checkbox"/>
6.2.6	Ensure 'Log_min_error_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Error' or Stricter	<input type="checkbox"/>	<input type="checkbox"/>
6.2.7	Ensure That the 'Log_min_duration_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to '-1' (Disabled)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.8	Ensure That 'cloudsql.enable_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging	<input type="checkbox"/>	<input type="checkbox"/>
6.3.1	Ensure 'external scripts enabled' database flag for Cloud SQL SQL Server instance is set to 'off'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.2	Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.3	Ensure 'user Connections' Database Flag for Cloud Sql Sql Server Instance Is Set to a Non-limiting Value	<input type="checkbox"/>	<input type="checkbox"/>
6.3.4	Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured	<input type="checkbox"/>	<input type="checkbox"/>
6.3.5	Ensure 'remote access' database flag for Cloud SQL SQL Server instance is set to 'off'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.6	Ensure '3625 (trace flag)' database flag for all Cloud SQL Server instances is set to 'on'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.7	Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is not set to 'on'	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure That the Cloud SQL Database Instance Requires All Incoming Connections To Use SSL	<input type="checkbox"/>	<input type="checkbox"/>
6.5	Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses	<input type="checkbox"/>	<input type="checkbox"/>
6.6	Ensure That Cloud SQL Database Instances Do Not Have Public IPs	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
6.7	Ensure That Cloud SQL Database Instances Are Configured With Automated Backups	<input type="checkbox"/>	<input type="checkbox"/>
7.1	Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Ensure That All BigQuery Tables Are Encrypted With Customer-Managed Encryption Key (CMEK)	<input type="checkbox"/>	<input type="checkbox"/>
7.3	Ensure That a Default Customer-Managed Encryption Key (CMEK) Is Specified for All BigQuery Data Sets	<input type="checkbox"/>	<input type="checkbox"/>
7.4	Ensure all data in BigQuery has been classified	<input type="checkbox"/>	<input type="checkbox"/>
8.1	Ensure that Dataproc Cluster is encrypted using Customer-Managed Encryption Key	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v7.0	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.5	Ensure That Service Account Has No Admin Privileges	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure That IAM Users Are Not Assigned the Service Account User or Service Account Token Creator Roles at Project Level	<input type="checkbox"/>	<input type="checkbox"/>
1.8	Ensure That Separation of Duties Is Enforced While Assigning Service Account Related Roles to Users	<input type="checkbox"/>	<input type="checkbox"/>
1.9	Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
1.11	Ensure That Separation of Duties Is Enforced While Assigning KMS Related Roles to Users	<input type="checkbox"/>	<input type="checkbox"/>
1.16	Ensure Essential Contacts is Configured for Organization	<input type="checkbox"/>	<input type="checkbox"/>
2.1	Ensure That Cloud Audit Logging Is Configured Properly	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure That Sinks Are Configured for All Log Entries	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket Lock	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure Log Metric Filter and Alerts Exist for Project Ownership Assignments/Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure That the Log Metric Filter and Alerts Exist for Audit Configuration Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.9	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.10	Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.11	Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.12	Ensure That Cloud DNS Logging Is Enabled for All VPC Networks	<input type="checkbox"/>	<input type="checkbox"/>
2.13	Ensure Cloud Asset Inventory Is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.14	Ensure 'Access Transparency' is 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.15	Ensure 'Access Approval' is 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.16	Ensure Logging is enabled for HTTP(S) Load Balancer	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure That the Default Network Does Not Exist in a Project	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure Legacy Networks Do Not Exist for Older Projects	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure That DNSSEC Is Enabled for Cloud DNS	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Ensure That RSASHA1 Is Not Used for the Key-Signing Key in Cloud DNS DNSSEC	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Ensure That RSASHA1 Is Not Used for the Zone-Signing Key in Cloud DNS DNSSEC	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Ensure That SSH Access Is Restricted From the Internet	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure That RDP Access Is Restricted From the Internet	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure That Instances Are Not Configured To Use the Default Service Account	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure “Block Project-Wide SSH Keys” Is Enabled for VM Instances	<input type="checkbox"/>	<input type="checkbox"/>
4.6	Ensure That IP Forwarding Is Not Enabled on Instances	<input type="checkbox"/>	<input type="checkbox"/>
4.9	Ensure That Compute Instances Do Not Have Public IP Addresses	<input type="checkbox"/>	<input type="checkbox"/>
4.12	Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects	<input type="checkbox"/>	<input type="checkbox"/>
5.1	Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.2	Ensure That Cloud Storage Buckets Have Uniform Bucket-Level Access Enabled	<input type="checkbox"/>	<input type="checkbox"/>
6.1.1	Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure 'Skip_show_database' Database Flag for Cloud SQL MySQL Instance Is Set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.2	Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.3	Ensure 'user Connections' Database Flag for Cloud Sql Sql Server Instance Is Set to a Non-limiting Value	<input type="checkbox"/>	<input type="checkbox"/>
6.3.4	Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured	<input type="checkbox"/>	<input type="checkbox"/>
6.3.6	Ensure '3625 (trace flag)' database flag for all Cloud SQL Server instances is set to 'on'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.7	Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is not set to 'on'	<input type="checkbox"/>	<input type="checkbox"/>
6.5	Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses	<input type="checkbox"/>	<input type="checkbox"/>
6.6	Ensure That Cloud SQL Database Instances Do Not Have Public IPs	<input type="checkbox"/>	<input type="checkbox"/>
6.7	Ensure That Cloud SQL Database Instances Are Configured With Automated Backups	<input type="checkbox"/>	<input type="checkbox"/>
7.1	Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
7.4	Ensure all data in BigQuery has been classified	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure that Corporate Login Credentials are Used	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Ensure that Multi-Factor Authentication is 'Enabled' for All Non-Service Accounts	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Ensure that Security Key Enforcement is Enabled for All Admin Accounts	<input type="checkbox"/>	<input type="checkbox"/>
1.5	Ensure That Service Account Has No Admin Privileges	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure That IAM Users Are Not Assigned the Service Account User or Service Account Token Creator Roles at Project Level	<input type="checkbox"/>	<input type="checkbox"/>
1.8	Ensure That Separation of Duties Is Enforced While Assigning Service Account Related Roles to Users	<input type="checkbox"/>	<input type="checkbox"/>
1.9	Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
1.10	Ensure KMS Encryption Keys Are Rotated Within a Period of 90 Days	<input type="checkbox"/>	<input type="checkbox"/>
1.11	Ensure That Separation of Duties Is Enforced While Assigning KMS Related Roles to Users	<input type="checkbox"/>	<input type="checkbox"/>
1.12	Ensure API Keys Only Exist for Active Services	<input type="checkbox"/>	<input type="checkbox"/>
1.13	Ensure API Keys Are Restricted To Use by Only Specified Hosts and Apps	<input type="checkbox"/>	<input type="checkbox"/>
1.14	Ensure API Keys Are Restricted to Only APIs That Application Needs Access	<input type="checkbox"/>	<input type="checkbox"/>
1.15	Ensure API Keys Are Rotated Every 90 Days	<input type="checkbox"/>	<input type="checkbox"/>
1.16	Ensure Essential Contacts is Configured for Organization	<input type="checkbox"/>	<input type="checkbox"/>
1.17	Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager	<input type="checkbox"/>	<input type="checkbox"/>
2.1	Ensure That Cloud Audit Logging Is Configured Properly	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure That Sinks Are Configured for All Log Entries	<input type="checkbox"/>	<input type="checkbox"/>



Recommendation		Set Correctly	
		Yes	No
2.3	Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket Lock	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure Log Metric Filter and Alerts Exist for Project Ownership Assignments/Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure That the Log Metric Filter and Alerts Exist for Audit Configuration Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.9	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.10	Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.11	Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.12	Ensure That Cloud DNS Logging Is Enabled for All VPC Networks	<input type="checkbox"/>	<input type="checkbox"/>
2.13	Ensure Cloud Asset Inventory Is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.14	Ensure 'Access Transparency' is 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.15	Ensure 'Access Approval' is 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.16	Ensure Logging is enabled for HTTP(S) Load Balancer	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure That the Default Network Does Not Exist in a Project	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure Legacy Networks Do Not Exist for Older Projects	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure That DNSSEC Is Enabled for Cloud DNS	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Ensure That RSASHA1 Is Not Used for the Key-Signing Key in Cloud DNS DNSSEC	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Ensure That RSASHA1 Is Not Used for the Zone-Signing Key in Cloud DNS DNSSEC	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Ensure That SSH Access Is Restricted From the Internet	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure That RDP Access Is Restricted From the Internet	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.8	Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network	<input type="checkbox"/>	<input type="checkbox"/>
3.9	Ensure No HTTPS or SSL Proxy Load Balancers Permit SSL Policies With Weak Cipher Suites	<input type="checkbox"/>	<input type="checkbox"/>
3.10	Use Identity Aware Proxy (IAP) to Ensure Only Traffic From Google IP Addresses are 'Allowed'	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure That Instances Are Not Configured To Use the Default Service Account	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure “Block Project-Wide SSH Keys” Is Enabled for VM Instances	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure Oslogin Is Enabled for a Project	<input type="checkbox"/>	<input type="checkbox"/>
4.5	Ensure ‘Enable Connecting to Serial Ports’ Is Not Enabled for VM Instance	<input type="checkbox"/>	<input type="checkbox"/>
4.6	Ensure That IP Forwarding Is Not Enabled on Instances	<input type="checkbox"/>	<input type="checkbox"/>
4.7	Ensure VM Disks for Critical VMs Are Encrypted With Customer-Supplied Encryption Keys (CSEK)	<input type="checkbox"/>	<input type="checkbox"/>
4.9	Ensure That Compute Instances Do Not Have Public IP Addresses	<input type="checkbox"/>	<input type="checkbox"/>
4.10	Ensure That App Engine Applications Enforce HTTPS Connections	<input type="checkbox"/>	<input type="checkbox"/>
4.11	Ensure That Compute Instances Have Confidential Computing Enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.12	Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects	<input type="checkbox"/>	<input type="checkbox"/>
5.1	Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Ensure That Cloud Storage Buckets Have Uniform Bucket-Level Access Enabled	<input type="checkbox"/>	<input type="checkbox"/>
6.1.1	Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure ‘Skip_show_database’ Database Flag for Cloud SQL MySQL Instance Is Set to ‘On’	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
6.1.3	Ensure That the 'Local_infile' Database Flag for a Cloud SQL MySQL Instance Is Set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1	Ensure 'Log_error_verbosity' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'DEFAULT' or Stricter	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2	Ensure That the 'Log_connections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
6.2.3	Ensure That the 'Log_disconnections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
6.2.4	Ensure 'Log_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set Appropriately	<input type="checkbox"/>	<input type="checkbox"/>
6.2.5	Ensure that the 'Log_min_messages' Flag for a Cloud SQL PostgreSQL Instance is set at minimum to 'Warning'	<input type="checkbox"/>	<input type="checkbox"/>
6.2.6	Ensure 'Log_min_error_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Error' or Stricter	<input type="checkbox"/>	<input type="checkbox"/>
6.2.7	Ensure That the 'Log_min_duration_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to '-1' (Disabled)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.8	Ensure That 'cloudsql.enable_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging	<input type="checkbox"/>	<input type="checkbox"/>
6.3.2	Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.3	Ensure 'user Connections' Database Flag for Cloud Sql Sql Server Instance Is Set to a Non-limiting Value	<input type="checkbox"/>	<input type="checkbox"/>
6.3.4	Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured	<input type="checkbox"/>	<input type="checkbox"/>
6.3.5	Ensure 'remote access' database flag for Cloud SQL SQL Server instance is set to 'off'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.6	Ensure '3625 (trace flag)' database flag for all Cloud SQL Server instances is set to 'on'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.7	Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is not set to 'on'	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure That the Cloud SQL Database Instance Requires All Incoming Connections To Use SSL	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
6.5	Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses	<input type="checkbox"/>	<input type="checkbox"/>
6.6	Ensure That Cloud SQL Database Instances Do Not Have Public IPs	<input type="checkbox"/>	<input type="checkbox"/>
6.7	Ensure That Cloud SQL Database Instances Are Configured With Automated Backups	<input type="checkbox"/>	<input type="checkbox"/>
7.1	Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Ensure That All BigQuery Tables Are Encrypted With Customer-Managed Encryption Key (CMEK)	<input type="checkbox"/>	<input type="checkbox"/>
7.3	Ensure That a Default Customer-Managed Encryption Key (CMEK) Is Specified for All BigQuery Data Sets	<input type="checkbox"/>	<input type="checkbox"/>
7.4	Ensure all data in BigQuery has been classified	<input type="checkbox"/>	<input type="checkbox"/>
8.1	Ensure that Dataproc Cluster is encrypted using Customer-Managed Encryption Key	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure that Corporate Login Credentials are Used	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Ensure that Multi-Factor Authentication is 'Enabled' for All Non-Service Accounts	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Ensure that Security Key Enforcement is Enabled for All Admin Accounts	<input type="checkbox"/>	<input type="checkbox"/>
1.5	Ensure That Service Account Has No Admin Privileges	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure That IAM Users Are Not Assigned the Service Account User or Service Account Token Creator Roles at Project Level	<input type="checkbox"/>	<input type="checkbox"/>
1.8	Ensure That Separation of Duties Is Enforced While Assigning Service Account Related Roles to Users	<input type="checkbox"/>	<input type="checkbox"/>
1.9	Ensure That Cloud KMS Cryptokeys Are Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
1.10	Ensure KMS Encryption Keys Are Rotated Within a Period of 90 Days	<input type="checkbox"/>	<input type="checkbox"/>
1.11	Ensure That Separation of Duties Is Enforced While Assigning KMS Related Roles to Users	<input type="checkbox"/>	<input type="checkbox"/>
1.12	Ensure API Keys Only Exist for Active Services	<input type="checkbox"/>	<input type="checkbox"/>
1.13	Ensure API Keys Are Restricted To Use by Only Specified Hosts and Apps	<input type="checkbox"/>	<input type="checkbox"/>
1.14	Ensure API Keys Are Restricted to Only APIs That Application Needs Access	<input type="checkbox"/>	<input type="checkbox"/>
1.15	Ensure API Keys Are Rotated Every 90 Days	<input type="checkbox"/>	<input type="checkbox"/>
1.16	Ensure Essential Contacts is Configured for Organization	<input type="checkbox"/>	<input type="checkbox"/>
1.17	Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager	<input type="checkbox"/>	<input type="checkbox"/>
2.1	Ensure That Cloud Audit Logging Is Configured Properly	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure That Sinks Are Configured for All Log Entries	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3	Ensure That Retention Policies on Cloud Storage Buckets Used for Exporting Logs Are Configured Using Bucket Lock	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure Log Metric Filter and Alerts Exist for Project Ownership Assignments/Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure That the Log Metric Filter and Alerts Exist for Audit Configuration Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.9	Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.10	Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.11	Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes	<input type="checkbox"/>	<input type="checkbox"/>
2.12	Ensure That Cloud DNS Logging Is Enabled for All VPC Networks	<input type="checkbox"/>	<input type="checkbox"/>
2.13	Ensure Cloud Asset Inventory Is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.14	Ensure 'Access Transparency' is 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.15	Ensure 'Access Approval' is 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.16	Ensure Logging is enabled for HTTP(S) Load Balancer	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure That the Default Network Does Not Exist in a Project	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure Legacy Networks Do Not Exist for Older Projects	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure That DNSSEC Is Enabled for Cloud DNS	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Ensure That RSASHA1 Is Not Used for the Key-Signing Key in Cloud DNS DNSSEC	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Ensure That RSASHA1 Is Not Used for the Zone-Signing Key in Cloud DNS DNSSEC	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Ensure That SSH Access Is Restricted From the Internet	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure That RDP Access Is Restricted From the Internet	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.8	Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network	<input type="checkbox"/>	<input type="checkbox"/>
3.9	Ensure No HTTPS or SSL Proxy Load Balancers Permit SSL Policies With Weak Cipher Suites	<input type="checkbox"/>	<input type="checkbox"/>
3.10	Use Identity Aware Proxy (IAP) to Ensure Only Traffic From Google IP Addresses are 'Allowed'	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure That Instances Are Not Configured To Use the Default Service Account	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Ensure “Block Project-Wide SSH Keys” Is Enabled for VM Instances	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Ensure Oslogin Is Enabled for a Project	<input type="checkbox"/>	<input type="checkbox"/>
4.5	Ensure ‘Enable Connecting to Serial Ports’ Is Not Enabled for VM Instance	<input type="checkbox"/>	<input type="checkbox"/>
4.6	Ensure That IP Forwarding Is Not Enabled on Instances	<input type="checkbox"/>	<input type="checkbox"/>
4.7	Ensure VM Disks for Critical VMs Are Encrypted With Customer-Supplied Encryption Keys (CSEK)	<input type="checkbox"/>	<input type="checkbox"/>
4.9	Ensure That Compute Instances Do Not Have Public IP Addresses	<input type="checkbox"/>	<input type="checkbox"/>
4.10	Ensure That App Engine Applications Enforce HTTPS Connections	<input type="checkbox"/>	<input type="checkbox"/>
4.11	Ensure That Compute Instances Have Confidential Computing Enabled	<input type="checkbox"/>	<input type="checkbox"/>
4.12	Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects	<input type="checkbox"/>	<input type="checkbox"/>
5.1	Ensure That Cloud Storage Bucket Is Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Ensure That Cloud Storage Buckets Have Uniform Bucket-Level Access Enabled	<input type="checkbox"/>	<input type="checkbox"/>
6.1.1	Ensure That a MySQL Database Instance Does Not Allow Anyone To Connect With Administrative Privileges	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Ensure ‘Skip_show_database’ Database Flag for Cloud SQL MySQL Instance Is Set to ‘On’	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
6.1.3	Ensure That the 'Local_infile' Database Flag for a Cloud SQL MySQL Instance Is Set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1	Ensure 'Log_error_verbosity' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'DEFAULT' or Stricter	<input type="checkbox"/>	<input type="checkbox"/>
6.2.2	Ensure That the 'Log_connections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
6.2.3	Ensure That the 'Log_disconnections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
6.2.4	Ensure 'Log_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set Appropriately	<input type="checkbox"/>	<input type="checkbox"/>
6.2.5	Ensure that the 'Log_min_messages' Flag for a Cloud SQL PostgreSQL Instance is set at minimum to 'Warning'	<input type="checkbox"/>	<input type="checkbox"/>
6.2.6	Ensure 'Log_min_error_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Error' or Stricter	<input type="checkbox"/>	<input type="checkbox"/>
6.2.7	Ensure That the 'Log_min_duration_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to '-1' (Disabled)	<input type="checkbox"/>	<input type="checkbox"/>
6.2.8	Ensure That 'cloudsql.enable_pgaudit' Database Flag for each Cloud Sql Postgresql Instance Is Set to 'on' For Centralized Logging	<input type="checkbox"/>	<input type="checkbox"/>
6.3.1	Ensure 'external scripts enabled' database flag for Cloud SQL SQL Server instance is set to 'off'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.2	Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.3	Ensure 'user Connections' Database Flag for Cloud Sql Sql Server Instance Is Set to a Non-limiting Value	<input type="checkbox"/>	<input type="checkbox"/>
6.3.4	Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured	<input type="checkbox"/>	<input type="checkbox"/>
6.3.5	Ensure 'remote access' database flag for Cloud SQL SQL Server instance is set to 'off'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.6	Ensure '3625 (trace flag)' database flag for all Cloud SQL Server instances is set to 'on'	<input type="checkbox"/>	<input type="checkbox"/>
6.3.7	Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is not set to 'on'	<input type="checkbox"/>	<input type="checkbox"/>



Recommendation		Set Correctly	
		Yes	No
6.4	Ensure That the Cloud SQL Database Instance Requires All Incoming Connections To Use SSL	<input type="checkbox"/>	<input type="checkbox"/>
6.5	Ensure That Cloud SQL Database Instances Do Not Implicitly Whitelist All Public IP Addresses	<input type="checkbox"/>	<input type="checkbox"/>
6.6	Ensure That Cloud SQL Database Instances Do Not Have Public IPs	<input type="checkbox"/>	<input type="checkbox"/>
6.7	Ensure That Cloud SQL Database Instances Are Configured With Automated Backups	<input type="checkbox"/>	<input type="checkbox"/>
7.1	Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Ensure That All BigQuery Tables Are Encrypted With Customer-Managed Encryption Key (CMEK)	<input type="checkbox"/>	<input type="checkbox"/>
7.3	Ensure That a Default Customer-Managed Encryption Key (CMEK) Is Specified for All BigQuery Data Sets	<input type="checkbox"/>	<input type="checkbox"/>
7.4	Ensure all data in BigQuery has been classified	<input type="checkbox"/>	<input type="checkbox"/>
8.1	Ensure that Dataproc Cluster is encrypted using Customer-Managed Encryption Key	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8.0	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: Change History

Date	Version	Changes for this version
Jan 25, 2024	3.0.0	ADD - Ensure Secrets are Not Stored in Cloud Run Environment Variables by Using Secret Manager (Ticket 16955)
Feb 6, 2024	3.0.0	UPDATE - Ensure That Service Account Has No Admin Privileges - Audit steps have changed (Ticket 18735)
Feb 6, 2024	3.0.0	ADD - Dataproc Section (Ticket 20897)
Feb 8, 2024	3.0.0	Update made to Additional Information (Ticket 18629)
Feb 8, 2024	3.0.0	Update to Additional Information (Ticket 18630)
Feb 12, 2024	3.0.0	UPDATE - Ensure 'Log_error_verbosity' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'DEFAULT' or Stricter (Automated) (Ticket 17914)
Feb 12, 2024	3.0.0	UPDATE - 6.2.2 Ensure That the 'Log_connections' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'On' (Ticket 18220)
Feb 15, 2024	3.0.0	UPDATE - Ensure Essential Contacts is Configured for Organization - additional cost for technical incidents (Ticket 17456)
Feb 28, 2024	3.0.0	UPDATE - 6.3.4 Ensure 'user options' database flag for Cloud SQL SQL Server instance is not configured (Ticket 18222)
Feb 29, 2024	3.0.0	UPDATE - 6.3.1 Ensure 'external scripts enabled' database flag for Cloud SQL SQL Server instance is set to 'off' (Ticket 18219)
Feb 29, 2024	3.0.0	UPDATE - 6.3.2 Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off' (Ticket 21062)
Feb 29, 2024	3.0.0	UPDATE - 6.3.3 Ensure 'user Connections' Database Flag for Cloud Sql Sql Server Instance Is Set to a Non-limiting Value (Ticket 21075)

Date	Version	Changes for this version
Feb 29, 2024	3.0.0	UPDATE - Ensure that Corporate Login Credentials are Used - add to remediation and fix references (Ticket 20958)
Feb 29, 2024	3.0.0	UPDATE - Ensure Cloud Asset Inventory Is Enabled - Clarification of wording (Ticket 19133)
Feb 29, 2024	3.0.0	UPDATE - 6.3.5 Ensure 'remote access' database flag for Cloud SQL SQL Server instance is set to 'off' (Ticket 18221)
Feb 29, 2024	3.0.0	UPDATE - 6.2.6 Ensure 'Log_min_error_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Error' or Stricter (Ticket 18237)
Feb 29, 2024	3.0.0	UPDATE - 6.2.7 Ensure That the 'Log_min_duration_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to '-1' (Disabled) (Ticket 18239)
Mar 6, 2024	3.0.0	UPDATE - Ensure That the Default Network Does Not Exist in a Project - update rationale and impact wording (Ticket 20656)
Mar 8, 2024	3.0.0	DELETE - Ensure Instance IP assignment is set to private (Automated) (Ticket 17794)
Mar 8, 2024	3.0.0	UPDATE - Ensure That Cloud SQL Database Instances Are Configured With Automated Backups - note exceptions for read-replica instances (Ticket 20340)
Mar 11, 2024	3.0.0	UPDATE - Ensure 'Log_min_error_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'Error' or Stricter - Explain the most and least strict values for clarity (Ticket 21032)
Mar 14, 2024	3.0.0	UPDATE - Cloud SQL Database Services Section - inline code, code blocks and Console steps (Ticket 21077)
Mar 14, 2024	3.0.0	UPDATE - Ensure that the 'Log_min_messages' Flag for a Cloud SQL PostgreSQL Instance is set at minimum to 'Warning' - Improvement in the description (Ticket 17472)

Date	Version	Changes for this version
Mar 14, 2024	3.0.0	UPDATE - Ensure that the 'cross db ownership chaining' database flag for Cloud SQL SQL Server instance is set to 'off' - flag is deprecated for all Cloud SQL instances (Ticket 21143)
Mar 15, 2024	3.0.0	Change the wording of the recommendation for "contained database authentication" flag (Ticket 21187)
Mar 15, 2024	3.0.0	Change the guidance to use the new 'SSL mode' setting instead of old 'require ssl' setting (Ticket 21144)
Mar 15, 2024	3.0.0	UPDATE - Ensure That Instances Are Not Configured To Use the Default Service Account - Clarification regarding valid remediation (Ticket 19590)
Mar 15, 2024	3.0.0	UPDATE - Ensure 'Enable Connecting to Serial Ports' Is Not Enabled for VM Instance - change audit console steps (Ticket 18938)
Mar 15, 2024	3.0.0	ADD - Ensure all data in BigQuery has been classified (Ticket 21115)
Mar 22, 2024	3.0.0	MOVE - Ensure that Dataproc Cluster is encrypted using Customer-Managed Encryption Key - to Dataproc section (Ticket 21194)
Mar 27, 2024	3.0.0	UPDATE - Ensure That Compute Instances Have Confidential Computing Enabled - Confidential Computing available for N2D,C2D machine type (Ticket 18717)
May 19, 2022	2.0.0	UPDATE - Ensure Cloud Asset Inventory Is Enabled - fix profile listing (Ticket 15304)
May 19, 2022	2.0.0	UPDATE - Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes - Missing double quotes (Ticket 15470)
May 19, 2022	2.0.0	UPDATE - Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes - missing double quotes (Ticket 15472)
Jul 14, 2022	2.0.0	UPDATE - Ensure That the Log Metric Filter and Alerts Exist for VPC Network Route Changes - Add a missing closing parenthesis at the end of the log metric filter. (Ticket 15827)

Date	Version	Changes for this version
Jul 14, 2022	2.0.0	UPDATE - Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes -The suggested log metric filter is missing parentheses to group rules (Ticket 15825)
Jul 14, 2022	2.0.0	UPDATE - Ensure That the Log Metric Filter and Alerts Exist for VPC Network Firewall Rule Changes -The suggested log metric filter is missing parentheses to group rules (Ticket 15826)
Oct 13, 2022	2.0.0	UPDATE - Ensure That IP Forwarding Is Not Enabled on Instances - Pantheon VM Instances link in remediation steps to Google Console VM Instances link (Ticket 15339)
Oct 18, 2022	2.0.0	UPDATE - Ensure That RSASHA1 Is Not Used for the Zone-Signing Key in Cloud DNS DNSSEC - Change assessment status to be automated (Ticket 15399)
Oct 18, 2022	2.0.0	UPDATE - Ensure That RSASHA1 Is Not Used for the Key-Signing Key in Cloud DNS DNSSEC - Change assessment status to be automated (Ticket 15398)
Oct 27, 2022	2.0.0	UPDATE - Ensure that the 'Log_min_messages' Flag for a Cloud SQL PostgreSQL Instance is set to at minimum to 'Warning' - Remove reference to log_min_error_statement in the Rationale section (Ticket 15908)
Oct 27, 2022	2.0.0	UPDATE - Ensure that the 'Log_min_messages' Flag for a Cloud SQL PostgreSQL Instance is set to at minimum to 'Warning' - Update title removing the 'at least' term (Ticket 16226)
Nov 3, 2022	2.0.0	UPDATE - Ensure That Instances Are Not Configured To Use the Default Service Account With Full Access to All Cloud APIs - Update to audit CLI to include email address (Ticket 16329)
Nov 4, 2022	2.0.0	UPDATE - Ensure That Cloud Audit Logging Is Configured Properly Across all Services and all Users from a Project - Change title for clarity (Ticket 15545)
Nov 4, 2022	2.0.0	UPDATE - Ensure 'Access Transparency' is 'Enabled' - change to L2 (Ticket 16900)
Nov 10, 2022	2.0.0	UPDATE - Ensure Cloud Asset Inventory Is Enabled - Profile Level Correction (Ticket 16622)

Date	Version	Changes for this version
Nov 29, 2022	2.0.0	UPDATE - Ensure That the Log Metric Filter and Alerts Exist for VPC Network Changes - Update Gcloud CLI command to latest release (Ticket 17099)
Nov 29, 2022	2.0.0	UPDATE - Ensure That the Log Metric Filter and Alerts Exist for Cloud Storage IAM Permission Changes - Update Gcloud CLI command to latest release (Ticket 17100)
Nov 29, 2022	2.0.0	UPDATE - Ensure That the Log Metric Filter and Alerts Exist for SQL Instance Configuration Changes - Update Gcloud CLI command to latest release (Ticket 17101)
Nov 29, 2022	2.0.0	UPDATE - Ensure Log Metric Filter and Alerts Exist for Project Ownership Assignments/Changes - Change Recommendation GCloud CLI commands to reference production versions (Ticket 17080)
Dec 9, 2022	2.0.0	UPDATE - Ensure that VPC Flow Logs is Enabled for Every Subnet in a VPC Network - Change to L2 (Ticket 16864)
Dec 15, 2022	2.0.0	UPDATE - Multiple recommendations - Standardize Verbiage in headings (Ticket 17079)
Dec 15, 2022	2.0.0	UPDATE - Ensure that Dataproc Cluster is encrypted using Customer-Managed Encryption Key - needs an impact statement (Ticket 17156)
Dec 15, 2022	2.0.0	UPDATE - Multiple Recommendations - Google Cloud Commands release status should be checked before publishing (Ticket 16959)
Dec 15, 2022	2.0.0	UPDATE - Ensure That Compute Instances Have Confidential Computing Enabled - Update Gcloud CLI command to latest release (Ticket 17116)
Dec 15, 2022	2.0.0	UPDATE - Ensure 'Log_statement' Database Flag for Cloud SQL PostgreSQL Instance Is Set Appropriately - Assessment status changed to automated and level changed to L2 (Ticket 15480)
Dec 15, 2022	2.0.0	UPDATE - Ensure 'Log_error_verbosity' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'DEFAULT' or Stricter - Assessment status changed to automated (Ticket 15479)

Date	Version	Changes for this version
Dec 15, 2022	2.0.0	UPDATE - Ensure 'Access Approval' is 'Enabled' - Suggest to update '+add' to '+ ADD' in Remediation Procedure (Ticket 15696)
Dec 15, 2022	2.0.0	UPDATE - Ensure That Compute Instances Do Not Have Public IP Addresses - Typo in Audit Procedure in control 4.9 (Ticket 15343)
Dec 15, 2022	2.0.0	UPDATE - Ensure That a Default Customer-Managed Encryption Key (CMEK) Is Specified for All BigQuery Data Sets - Assessment status should be reverted back to automated (Ticket 15328)
Dec 15, 2022	2.0.0	UPDATE - Ensure That BigQuery Datasets Are Not Anonymously or Publicly Accessible - Assessment status should be reverted back to automated (Ticket 15327)
Dec 15, 2022	2.0.0	UPDATE - Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Server instance is set to 'off' - Update wording in description for recommendation (Ticket 15342)
Dec 15, 2022	2.0.0	UPDATE - Ensure Oslogin Is Enabled for a Project - Propose update 'instances' to 'instance' in remediation step 5 (Ticket 15338)
Dec 15, 2022	2.0.0	UPDATE - Ensure That the Log Metric Filter and Alerts Exist for Custom Role Changes - Update GCloud CLI command to latest release (Ticket 17097)
Dec 15, 2022	2.0.0	UPDATE - Ensure that the 'Log_min_messages' Flag for a Cloud SQL PostgreSQL Instance is set at minimum to 'Warning'- Assessment status should be changed to automated (Ticket 15481)
Dec 16, 2022	2.0.0	UPDATE - Ensure 'Access Approval' is 'Enabled' - add output examples for CLI audit (Ticket 16338)
Dec 16, 2022	2.0.0	UPDATE - Ensure API Keys Are Rotated Every 90 Days - Add CLI steps and change to Automated (Ticket 16548)
Dec 16, 2022	2.0.0	UPDATE - Ensure API Keys Are Restricted to Only APIs That Application Needs Access - Add CLI steps and change to Automated (Ticket 16547)



Date	Version	Changes for this version
Dec 22, 2022	2.0.0	ADD : Ensure Logging is enabled for HTTP(S) Load Balancer (Ticket 12876)
Dec 23, 2022	2.0.0	UPDATE - Multiple in Logging and Monitoring section - Change some monitoring recommendations to Level 2 (Ticket 16270)
Dec 29, 2022	2.0.0	UPDATE - Ensure API Keys Are Restricted To Use by Only Specified Hosts and Apps - Should API Keys Assessment Status be changed to Automated? (Ticket 16546)
Dec 29, 2022	2.0.0	UPDATE - Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects - adjust wording to give more clarity to intent (Ticket 16865)
Dec 30, 2022	2.0.0	ADD - Ensure Instance IP assignment is set to private (Ticket 17011)
Dec 30, 2022	2.0.0	UPDATE - Ensure API Keys Only Exist for Active Services - Updated recommendation to account for Google's recommended standard authentication flow (Ticket 16545)
Dec 30, 2022	2.0.0	UPDATE - Ensure Secrets are Not Stored in Cloud Functions Environment Variables by Using Secret Manager - Correction in prose (Ticket 16577)
Dec 30, 2022	2.0.0	DELETE - Ensure 'Log_hostname' Database Flag for Cloud SQL PostgreSQL Instance Is Set to 'on' (Ticket 15876)