February 2025
Google Workspace
CMMC Level 2 Implementation Guide
FINAL

Google Workspace

CMMC Level 2 Implementation Guide

Google Workspace

Table of Contents

Overview of the CMMC Implementation Guide

Purpose

The purpose of this Cybersecurity Maturity Model Certification (CMMC) Implementation Guide is to provide detailed guidance on the use of Google Workspace to support customers' **CMMC Version 2.0 Level 2 ("CMMC")** compliance needs.

This implementation guide will also demonstrate how Google Workspace can enable customers to meet their cybersecurity and compliance goals.

Important: This document provides guidance on Google Workspace capabilities to support customer compliance with the CMMC Organizations should seek independent legal advice relating to their responsibilities under CMMC . Nothing in this document is intended to provide or be used as a substitute for legal advice.

Audience

The audience of this CMMC Implementation Guide may include any organization seeking compliance with the Defense Federal Acquisition Regulation Supplement (**DFARS**) (48 CFR § 252.204-7012), National Institute of Standards and Technology (**NIST**) Special Publication (SP) 800-171, and/or CMMC Level 2, including but not limited to: the Defense Contract Management Agency (**DCMA**), members of the Defense Industrial Base (**DIB**), federal contractors and subcontractors, organizations seeking assessment (OSAs), or other Google Workspace customers, hereto referred to as a **Customer.** Specifically, this should be used by individuals or teams responsible for implementing and managing their Google Workspace account.

Scope

The scope of the CMMC Implementation Guide is limited to the controls found in NIST SP 800-171 Revision 2 for a CMMC Level 2 implementation.

In addition, the guide is limited to the Customer's Google Workspace **Enterprise Plus Edition** and **Assured Controls Plus** environment and excludes additional services, systems, applications, tools, endpoints, or other processes that may be included within the Customer's **CUI boundary**. While this guide can be used by Customers accessing Google Workspace by any endpoints (e.g., PC, Macbook), Customers using Chromebooks should see Appendix A for additional compliance considerations.

Overview of CMMC

CMMC Program

The CMMC Program was established by the Department of Defense (DoD) to formally verify that DoD contractors and subcontractors within the DIB implement appropriate cyber security measures necessary to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). To achieve this, the CMMC program leverages the security controls outlined in NIST SP 800-171 Rev 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

After several years of deliberation, the CMMC Rule (32 CFR Part 170) formally went into effect on December 16, 2024. The table below defines the requirements for each CMMC Level and assessment type:

CMMC Level	Security Requirements	Assessment Requirement	Assessment Frequency
Level 1 (Self)	15 requirements from FAR clause 52.204-21	Self assessment	Annual
Level 2 (Self)	110 requirements from NIST 800-171 Rev 2	Self assessment	Every 3 years
Level 2 (Certification)	110 requirements from NIST SP 800-171 Rev 2	C3PAO assessment	Every 3 years
Level 3 (Certification)	110 requirements from NIST SP 800-171 Rev 2 24 requirements from NIST SP 800-172	DCMA assessment	Every 3 years

Cloud Service Provider (CSP) Requirements

In addition to the security requirements listed above, the DFARS 252.204-7012 clause ("**DFARS**") also dictates that any contractor intending to leverage an external Cloud Service Provider (**CSP**) to store, process, or transmit CUI must ensure that the CSP meet a FedRAMP Moderate Equivalency and complies with the additional requirements in the clause.

Google Workspace Enterprise obtained a FedRAMP High Authority to Operate (ATO) in 2021, therefore, it supports Customers seeking compliance with DFARS and CMMC.

Key CMMC Requirements

Customers can consider the following during the CMMC journey:

1. **Understand requirements**: Know the CMMC levels, required levels within contracts, and respective control requirements. Understand the individual objectives of each requirement which must be satisfied to meet the control.
2. **Define scope and boundary:** Identify CUI and how CUI is received, handled, stored and managed within Google Workspace, as well as other systems, applications, etc. CMMC has provided an official CMMC Level 2 Scoping Guide to better identify CUI assets and define a boundary.
3. **Conduct a gap analysis:** Conduct a gap analysis against your defined boundary to identify and address security gaps in the technical controls. Consider using the official CMMC Level 2 Assessment Guide to mimic how an assessor would approach testing the controls.
4. **Leverage technologies:** Configuring key security features in Google Workspace to enhance security and implement controls.

Overview of Google Workspace

Purpose

Google Workspace is a comprehensive suite of secure, cloud-based collaboration tools. It is designed to help teams work more efficiently and effectively, offering seamless integration and real-time collaboration features. This guide aims to help Customers enable services and features within their Google Workspace Enterprise Edition to support CMMC requirements.

Overview of Google Workspace Services

Google Workspace includes a suite of administration and collaboration capabilities, including:

- **Communication:** Gmail, Meet, Contacts, Groups for Business
- **Collaboration:** Drive, Docs, Sheets, Slides, Sites, Forms
- **Organization:** Calendar, Keep, Cloud Search
- **Identity and Administration:** Admin Console, Identity-as-a-Service, Vault, Chrome Sync, Chrome Device Management (CDM)

Furthermore, these services include Enabling Features (e.g., Admin Role Director, SSO Profiles) which can be leveraged to utilize Google Workspace Services effectively, securely, and in alignment with CMMC controls.

Customer Responsibility Matrix (CRM)

Google maintains a Google Workspace CMMC Customer Responsibility Matrix (CRM) in order to define which controls, as it relates to the Google Workspace environment, can be inherited or partially inherited from Google and which are a customer's responsibility.

Google is responsible for the design, development, release and maintenance of the software it provides as a service and the performance and availability of the related common infrastructure on which the core service is provided. Service management relies on the underlying infrastructure and related data security mechanisms designed to provide reliable and secure services to customers. Therefore, several Physical Protection, Media Protection, and Systems & Communication Protection controls can be inherited from Google.

Once a Google Workspace domain has been established and validated, a Customer can use the Enabling Features in the Admin Console to configure and customize services and meet control within domains such as Access Control, Audit & Accountability, etc. APIs are also available to integrate Google Workspace services with existing client infrastructure or third-party service providers.

For specifics on Google implementation on inherited/partially inherited controls and customer responsibility, please reach out to your Google Workspace customer representative and request the CRM.

How to Use this Guide

Control Implementation Tables

This section provides an overview of how to interpret the control implementation tables below in order to implement and manage security controls in their Google Workspace domain.

For each control, a table will include the following content:

- **Control Domain:** The CMMC control domain, based on NIST SP 800-171
- **Control #:** The CMMC control identifier, composed of three distinct elements, the domain, the CMMC Level, and security requirement number
- **Control Description:** The CMMC control language descriptor
- **Google Workspace Enabling Features:** Recommended tools and features within the Google Workspace Services that can be utilized by the Customer as part of the control implementation. Additional or alternative tools and features may also be utilized and are up to the Customer to determine the best approach for their CUI Boundary
- **Control Responsibility:** Control responsibility as defined in the Google Workspace CMMC CRM. Control identified as "Shared" and "Customer" are controls that require specific implementation by the Customer
- **Customer Implementation Description:** A step-by-step description for the Customer to follow to utilize the Enabling Features to support their CMMC control. The guidance takes into consideration the NIST SP 800-171A control objectives

- **Supplemental Guidance:** Where additional, more detailed, implementation guidance exists, a reference will be provided for the Customer for further exploration and reading

An example control implementation table is depicted below:

Control Domain	**Access Control**		
Control #	**AC.L1-3.1.1**		
Control Description	Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems)		
Google Workspace Enabling Features	User Directory	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
As a Customer of a Google Workspace account, you should consider: 1. Step 1 2. Step 2 3. Step 3			
Supplemental Guidance			
Additional documentation			

Control Categories

This guide has categorized the CMMC controls into three (3) distinct categories:

1. **Controls Requiring Customer Implementation in Google Workspace**

   Specific to the Customer's Google Workspace domain, the Customer is responsible for leveraging underlying services and utilizing Enabling Features (e.g., Admin Console) to enable compliance with the control. While the Customer Implementation Description provides technical implementation, there may be additional administrative requirements that exist outside of the scope of Google Workspace (e.g., policies and procedures) the Customer may need to deploy to meet the control.

   The controls in this category include:

AC.L1-3.1.1	AC.L2-3.1.15	AU.L2-3.3.9	IA.L1-3.5.2	SC.L2-3.13.8
AC.L1-3.1.2	AC.L2-3.1.18	CM.L2-3.4.1	IA.L2-3.5.3	SC.L2-3.13.9

AC.L2-3.1.3	AC.L2-3.1.19	CM.L2-3.4.2	IA.L2-3.5.6	SC.L2-3.13.12
AC.L2-3.1.4	AC.L1-3.1.20	CM.L2-3.4.3	IA.L2-3.5.7	SC.L2-3.13.15
AC.L2-3.1.5	AC.L1-3.1.22	CM.L2-3.4.5	IA.L2-3.5.8	SI.L2-3.14.3
AC.L2-3.1.6	AU.L2-3.3.1	CM.L2-3.4.6	IA.L2-3.5.9	SI.L2-3.14.6
AC.L2-3.1.7	AU.L2-3.3.3	CM.L2-3.4.7	IR.L2-3.6.1	SI.L2-3.14.7
AC.L2-3.1.8	AU.L2-3.3.5	CM.L2-3.4.8	PS.L2-3.9.2	
AC.L2-3.1.11	AU.L2-3.3.6	CM.L2-3.4.9	SC.L1-3.13.1	
AC.L2-3.1.12	AU.L2-3.3.8	IA.L1-3.5.1	SC.L2-3.13.3	

2. Controls Natively Implemented by Google Workspace

Natively implemented controls are those the Customer inherits directly from Google Workspace. While Google has implemented the control, there may be opportunities for Customers to deploy security enhancements via Enabling Features.

The Customer's CUI boundary may contain systems, applications, facilities, or tools outside of Google Workspace; it is the sole responsibility of the Customer to decide how to address controls for the organizational systems that fall outside the Google Workspace environment.

The controls in this category include:

AC.L2-3.1.13	IA.L2-3.5.11	MP.L2-3.8.6	RA.L2-3.11.2	SC.L2-3.13.14
AC.L2-3.1.14	MA.L2-3.7.1	MP.L2-3.8.7	RA.L2-3.11.3	SC.L2-3.13.16
AC.L2-3.1.16	MA.L2-3.7.2	MP.L2-3.8.8	SC.L2-3.13.4	SI.L1-3.14.1
AC.L2-3.1.17	MA.L2-3.7.3	MP.L2-3.8.9	SC.L1-3.13.5	SI.L1-3.14.2
AU.L2-3.3.2	MA.L2-3.7.4	PE.L1-3.10.1	SC.L2-3.13.6	SI.L1-3.14.4
AU.L2-3.3.4	MA.L2-3.7.5	PE.L2-3.10.2	SC.L2-3.13.7	SI.L1-3.14.5
AU.L2-3.3.7	MA.L2-3.7.6	PE.L1-3.10.3	SC.L2-3.13.10	

IA.L2-3.5.4	MP.L1-3.8.3	PE.L1-3.10.4	SC.L2-3.13.11	
IA.L2-3.5.10	MP.L2-3.8.5	PE.L1-3.10.5	SC.L2-3.13.13	

3. Controls Requiring Implementation Outside of Google Workspace

These controls do not apply to a Google Workspace implementation. The Customer's CUI boundary may contain systems, applications, facilities, or tools outside of Google Workspace; it is the sole responsibility of the Customer to decide how to address controls for the organizational systems that fall outside the Google Workspace environment.

The controls in this category include:

AC.L2-3.1.9	AT.L2-3.2.3	MP.L2-3.8.1	RA.L2-3.11.1	SC.L2-3.13.2
AC.L2-3.1.10	CM.L2-3.4.4	MP.L2-3.8.2	CA.L2-3.12.1	
AC.L2-3.1.21	IA.L2-3.5.5	MP.L2-3.8.4	CA.L2-3.12.2	
AT.L2-3.2.1	IR.L2-3.6.2	PS.L2-3.9.1	CA.L2-3.12.3	
AT.L2-3.2.2	IR.L2-3.6.3	PE.L2-3.10.6	CA.L2-3.12.4	

Controls Requiring Implementation in Google Workspace

Control Domain	Access Control		
Control #	**AC.L1-3.1.1**		
Control Description	Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems)		
Google Workspace Enabling Features	User Directory Google Cloud Directory Sync Directory Sync SSO Profiles API Controls Basic & Advanced Mobile Security Endpoint Management Company-owned device management	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			

Google Workspace Customers are responsible for:

a. Identifying authorized users of their Google Workspace account
b. Identifying processes acting on behalf of authorized users which may access their Google Workspace account
c. Identifying devices (and other systems) authorized to connect to their Google Workspace account
d. Limiting Google Workspace access to authorized users;
e. Limiting Google Workspace access to processes acting on behalf of authorized users
f. Limiting Google Workspace access to authorized devices (including other systems)

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **User Directory**
- **Google Cloud Directory Sync**
- **Directory Sync**
- **SSO Profiles**
- **API Controls**
- **Basic mobile security**
- **Advanced mobile security and app management**
- **Endpoint management**
- **Company-owned device management**

A description of each feature and implementation guidance is included below.

User Directory
You must create user accounts in Google Workspace to grant access to the Google Workspace services and CUI data. This can be done one at a time using the following steps:

1. Sign in with an administrator account to the Google Admin console
2. In the Admin console, go to **Menu**, select **Directory**, select **Users**.
3. At the top of the user list, click Add New User
4. Add the user's account information
5. (Optional) Click Manage user's password, organizational unit, and profile photo
6. Click Add New User.
7. Choose an option to send account information to the new user
8. Click Done

Google Cloud Directory Sync
Google Cloud Directory Sync (GCDS) runs on premises, in your server environment. You can use GCDS to synchronize your Google users, groups, and shared contacts to match the information in your LDAP server.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Directory Sync
Directory Sync synchronizes your LDAP user and group data with your Google cloud directory. The sync process takes place in the cloud, so there's no need to install a client or application. Using Directory Sync requires a connection between Google Cloud and your LDAP server, usually Cloud VPN or Cloud Interconnect.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

SSO Profiles
Single sign-on (SSO) allows users to sign in to many enterprise cloud applications using a single set of credentials. Google Workspace supports SSO from third-party identity providers (IdPs). Instead of manually creating and maintaining user accounts in Google Workspace, you can automate the process by combining SAML-based single sign-on with automatic user provisioning, if offered by your choice of IdP.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

API Controls

API Controls can be used to manage the API access that both internal apps and third-party apps have to users' data in Google Workspace. When users sign in to third-party apps using the "Sign in with Google" option (single sign-on), you can control how those apps access your organization's Google data using this service. This service also allows you to customize the message that users see when they try to install an unauthorized app.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Basic mobile security
Basic mobile management is on by default and provides core security like hijacking protection. You can see a list of mobile devices that users have used to sign in to your managed accounts. Google Workspace Admins can also see details including the device type and model, the last time it synchronized work data, and the name of the user who accessed data on it. From the list, Google Workspace Admins can also block a device from syncing work data, wipe data from a lost device, and more.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Advanced mobile security and app management
Advanced management offers additional features for controlling devices that access your Google Workspace account. You can use advanced management for more control over device policies and passwords, to manage apps on Android and Apple iOS devices, and to wipe all data from devices. You can individually review user-owned devices that request access to a work or school account. When a user adds a work or school account to their device, they see a message that an admin needs to review and approve the device. Once the Google Workspace Admin approves a device, the user can access their work account data on the device.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Endpoint Management
Google Workspace Admins can control which laptops, desktops, and other endpoints can access your organization's data and get details about those devices. You can also see when a user signs in to your managed account and some details about the device.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Company-owned device management

You can also manage all of your company-owned devices—mobile devices, laptops, desktops—in one place in your Google Workspace Admin console. Company-owned devices are devices that your organization purchased through a reseller or device vendor, and which they secure and manage for your employees.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. Third party IDP and SSO Profiles may also be considered if they support CMMC controls.
2. Consider granting system access to Google Workspace services based on valid access authorization, intended system usage (including need for access to CUI), and any other requirements defined by your company policies.
3. Management of a paid Google Workspace, Cloud Identity, or add-on subscription can be transferred from Google to a reseller, a reseller to Google, or between resellers. Resold customers should remember to remove reseller access once it's no longer needed. Please refer to supplemental guidance for more details.

Supplemental Guidance

- Google Workspace Directory
- Google Cloud Directory Sync
- Directory Sync (beta)
- SSO Profiles
- API Controls
- Basic & Advanced Mobile Management
- Endpoint Management
- Company-owned device management
- Manage reseller access

Control Domain	Access Control		
Control #	**AC.L1-3.1.2**		
Control Description	Limit system access to the types of transactions and functions that authorized users are permitted to execute.		
Google Workspace Enabling Features	Prebuilt Admin Roles Custom Roles	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Defining the types of transactions and functions that authorized users are permitted to execute in Google Workspace
b. Limiting access to the defined types of transactions and functions using roles

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Prebuilt Admin Roles**
- **Custom Roles**

A description of each feature and implementation guidance is included below.

Prebuilt Admin Roles
An easy way to grant administrator privileges to another user is to assign prebuilt administrator roles. Each role grants one or more privileges that together allow you to perform a common business function. For example, one role manages user accounts, another role manages groups, another role manages calendars and resources, and so on. Assign multiple roles to grant all privileges in those roles.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Custom Roles
If the pre-built administrator roles do not grant the privileges that you want to assign to a user, create a custom role that does. Each custom role can include one or more administrator privileges for specific management tasks in your Google Admin console. The privileges you select determine which Home page controls are in the user's Admin console and what settings the user can manage. Regardless of the privileges you select, a user with a Custom Role can never make changes to your or any other administrator account.

You can create up to 750 custom roles for your entire organization.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Once you have decided on the type of roles that you will use, you can use Google Workspace to either:

1. Assign roles to one user
2. Assign roles to several users at once
3. Assign a role to a group
4. Assign a role to a service account

For more information, please refer to the supplemental guidance.

Additional Considerations

1. If using Directory Sync or Google Cloud Directory Sync, then consider assigning admin roles that limit user functionality to Google Groups which are automatically generated from your LDAP.

Supplemental Guidance

- Prebuilt Admin Roles
- Custom Roles
- Instructions for assigning roles

Control Domain	**Access Control**		
Control #	**AC.L2-3.1.3**		
Control Description	Control the flow of CUI in accordance with approved authorizations.		
Google Workspace Enabling Features	Third-party connections DLP for Drive DLP for Chat DLP for Gmail (beta) Chrome DLP	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Information flow control regulates where information can travel within a system and between systems (versus who can access the information). Google Workspace Customers are responsible for:			

a. Managing and limiting connections between your Google Account and third-parties
b. Configuring Data Loss Prevention (DLP) to detect and prevent the loss, leakage, or misuse of CUI in your Google Workspace Account

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Third-party connections**
- **DLP for Drive**
- **DLP for Gmail (beta)**
- **DLP for Chat**
- **Chrome DLP**

A description of each feature and implementation guidance is included below.

Third-party Connections
To unlock helpful features, you may choose to share data between your Google Account and third-party apps and services. Third parties are companies or developers that are not Google. Only share your data with third parties that you trust. Google does not set up connections without your permission. Google does not share your Google Account password with any third-party app or service. You can review the type of data that you consented to share from your Google Account to the third-party. You can remove the access a third-party has to your Google Account at any time

To review all your current third-party connections:

1. Visit your Google Account's third-party connections page.
2. Find the app or service in the list.
3. Select the app or service whose connections you want to review.

To review or remove what a third-party app or service can access:

1. Go to your Google Account's third-party connections page.
2. Select **Have access to your Google Account.**
3. Select the third-party app or service you want to review.
4. To filter for third-party apps and services with specific access to your Google Account, select Access to and choose a Google product or select **Other access**.
5. Select **See details**.
6. Review the access that the third-party app or service has to your Google Account.
7. If you want to remove the app or service's access, select **Remove access** and then **Confirm**.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

DLP for Drive

You can use DLP policies in Google Workspace to detect sensitive information, such as credit card numbers, in email and Google Drive files. You can set up policy-based actions and block users from sharing email and Drive files when sensitive content is detected. Content detectors, used with DLP, specify sensitive content types to scan and report. Some rule templates use predefined content detectors that automatically scan and report sensitive data. How the content is scanned and reported depends on the type of content.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

DLP for Gmail (beta)
You can create DLP rules in your Google Admin console to manage sensitive content that your users share in email messages. With DLP for Gmail, rules apply to messages sent to users inside and outside of your organization. Use rules to identify sensitive information and help prevent it from being shared inside and outside your organization.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

DLP for Chat
Using DLP for Chat, you can create data protection rules to prevent data leaks from Chat messages and attachments (uploaded files and images).

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. As an admin, you can use DLP rules to automatically apply labels to Drive files based on detection of sensitive content. For more information, please refer to the supplemental guidance.
2. You can also use DLP rules to automatically apply classification labels to Gmail messages. For more information, please refer to the supplemental guidance.
3. To have greater control over which users and devices can transfer sensitive content, you can combine DLP rules with Context-Aware Access conditions, such as user location, device security status (managed, encrypted) and IP address. When you add a Context-Aware Access policy to a DLP rule, the rule is enforced only if the context conditions are met. For more information, please refer to the supplemental guidance.

Supplemental Guidance

- Third Party Connections
- DLP for Drive
- DLP for Gmail

- DLP for Chat
- DLP with Chrome
- Apply classification labels to Drive files automatically with DLP rules
- Gmail DLP & automatic classification labels (beta)
- Combine DLP rules with Context-Aware Access conditions

Control Domain	Access Control		
Control #	**AC.L2-3.1.4**		
Control Description	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.		
Google Workspace Enabling Features	Prebuilt Admin Roles Custom Roles	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			

Google Workspace Customers are responsible for:

a. Defining the duties of individuals that require separation
b. Assigning responsibilities to separate individuals
c. Implementing separation of duties through assigned group and role authorizations

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Prebuilt Admin Roles**
- **Custom Roles**

A description of each feature and implementation guidance is included below.

Prebuilt Admin Roles
The easiest way to grant administrator privileges to another user is to assign prebuilt administrator roles. Each role grants one or more privileges that together allow you to perform a common business function. For example, one role manages user accounts, another role manages groups, another role manages calendars and resources, and so on. Assign multiple roles to grant all privileges in those roles.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Custom Roles
If the pre-built administrator roles do not grant the privileges that you want to assign to a user, create a custom role that does. Each custom role can include one or more administrator privileges for specific management tasks in your Google Admin console. The privileges you select determine which Home page controls are in the user's Admin console and what settings the user can manage. Regardless of the privileges you select, a user with a Custom Role can never make changes to your or any other administrator account.

You can create up to 750 custom roles for your entire organization. If your organization had more than 750 custom roles before the limit went into effect, we recommend adjusting your roles to bring them under the limit.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Once you have decided on the roles that you will use, you can use Google Workspace to either:

1. Assign roles to one user
2. Assign roles to several users at once
3. Assign a role to a group
4. Assign a role to a service account

For more information, please refer to the supplemental guidance.

Additional Considerations

1. If using Directory Sync or Google Cloud Directory Sync, then consider assigning admin roles that limit user functionality to Google Groups which are automatically generated from your LDAP.

Supplemental Guidance

- Prebuilt Admin Roles
- Custom Roles
- Instructions for assigning roles

Control Domain	Access Control		
Control #	**AC.L2-3.1.5**		
Control Description	Employ the principle of least privilege, including for specific security functions and privileged accounts.		
Google Workspace Enabling Features	Prebuilt Admin Roles Custom Roles	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			

Google Workspace Customers are responsible for:

a. Defining privileged functions
b. Identifying non-privileged users/roles
c. Preventing non-privileged users from executing privileged functions using Google Workspace pre-built roles, custom roles or a combination of Google Workspace pre-built roles and custom roles.

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Prebuilt Admin Roles**
- **Custom Roles**

A description of each feature and implementation guidance is included below.

Prebuilt Admin Roles
The easiest way to grant administrator privileges to another user is to assign prebuilt administrator roles. Each role grants one or more privileges that together allow you to perform a common business function. For example, one role manages user accounts, another role manages groups, another role manages calendars and resources, and so on. Assign multiple roles to grant all privileges in those roles.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Custom Roles
If the pre-built administrator roles do not grant the privileges that you want to assign to a user, create a custom role that does. Each custom role can include one or more administrator privileges for specific management tasks in your Google Admin console. The privileges you select determine which Home page controls are in the user's Admin console and what

settings the user can manage. Regardless of the privileges you select, a user with a Custom Role can never make changes to your or any other administrator account.

You can create up to 750 custom roles for your entire organization.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Assign Roles
Once you have decided on the roles that you will use, you can use Google Workspace to either:

1. Assign roles to one user
2. Assign roles to several users at once
3. Assign a role to a group
4. Assign a role to a service account

For more information, please refer to the supplemental guidance.

Additional Considerations

1. If using Directory Sync or Google Cloud Directory Sync, then consider assigning admin roles that limit user functionality to Google Groups which are automatically generated from your LDAP.

Supplemental Guidance

- Prebuilt Admin Roles
- Custom Roles
- Instructions for assigning roles

Control Domain	Access Control		
Control #	**AC.L2-3.1.6**		
Control Description	Use non-privileged accounts or roles when accessing nonsecurity functions.		
Google Workspace Enabling Features	User Directory Google Cloud Directory Sync Directory Sync SSO Profiles	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description
Google Workspace Customers are responsible for: a. Defining nonsecurity functions b. Requiring users to use non-privileged accounts or roles when accessing nonsecurity functions To address this requirement, you should create secondary, non-privileged accounts, for each user with privileged roles configured in AC.L2-3.1.4 by using one of the Google Workspace user account management features described in AC.L1-3.1.1. **Additional Considerations** 1. As an administrator for your organization's Google Workspace, you can see a list of all the admin roles and privileges assigned to a user or group. You can also see a list of all the direct assignments for a given role. This information can help you to quickly determine a user's or group's level of administrative access to your organization's Google Workspace account and services. For more information, please refer to the supplemental guidance.
Supplemental Guidance
• View role assignments & privileges

Control Domain	Access Control		
Control #	**AC.L2-3.1.7**		
Control Description	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.		
Google Workspace Enabling Features	Prebuilt Admin Roles Custom Roles	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Defining privileged functions b. Identifying non-privileged users c. Preventing non-privileged users from executing privileged functions by assigning them to the correct role			

You can prevent non-privileged users from executing privileged functions by assigning users to the appropriate roles in Google Workspace. Please refer to AC.L2-3.1.4 for information on the prebuilt admin roles and custom roles and how to assign roles.

Additional Considerations

1. As an administrator for your organization's Google Workspace, you can see a list of all the admin roles and privileges assigned to a user or group. You can also see a list of all the direct assignments for a given role. This information can help you to quickly determine a user's or group's level of administrative access to your organization's Google Workspace account and services. For more information, please refer to the supplemental guidance.

Supplemental Guidance

- Prebuilt Admin Roles
- Custom Roles
- View role assignments & privileges

Control Domain	Access Control		
Control #	**AC.L2-3.1.8**		
Control Description	Limit unsuccessful logon attempts.		
Google Workspace Enabling Features	Security Investigation Tool	**Control Responsibility**	[ ] Google [ ] Shared [X] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Defining the means of limiting unsuccessful logon attempts
b. Implementing the means of limiting unsuccessful logon attempts

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Security Investigation Tool**

A description of each feature and implementation guidance is included below.

Security Investigation Tool
As an administrator, you can set up rules in the Google Admin console. To configure a rule, you set up conditions for the rule, and specify what actions to perform when the conditions are met. A rule is simply a way of saying, if x happens, automatically do y. For example, you can set up rules to be notified of specific activity within your domain—such as a suspicious sign-in attempt, a compromised mobile device, or when another administrator changes settings. Set up rules using the security investigation tool to automate actions that happen in response to activity within your domain.

To create a rule to limit unsuccessful logon attempts:

1. Sign in with an administrator account to the **Google Admin** console
2. From the **Google Admin** console Home page, click **Rules** and then **Create rule** and then **Activity**.
3. Enter a Rule name (for example, External data sharing).
4. Enter a Description (for example, Notify if documents are shared outside the company).
5. Click Next: View conditions.
6. Under conditions, select **User log events** as the Data Source
7. Build the condition to match: "**Event"** -> "**Is**" -> "**Failed login**"
8. Click **Next: add Actions**
9. Set **Failed login Threshold** (e.g. "Every 24 hours" -> when count ">" -> "5"
10. Click **Next: add Actions**
11. Select **Suspend users**
12. Click **Next: add Actions**
13. Choose whether you want this rule to trigger an alert in the alert center. You can choose a severity of High, Medium, or Low. You can also choose to send email notifications by checking the All super administrators box, or by clicking Add email recipients to send emails to select administrators when the rule is triggered.
14. To review or edit the rule details, click **Next: Review**.
15. Click **Create rule**.

Additional Considerations

1. Customers using SSO profiles should configure failed login attempts using their authentication service provider.

Supplemental Guidance

- Security Investigation Tool

Control Domain	Access Control		
Control #	**AC.L2-3.1.11**		
Control Description	Terminate (automatically) a user session after a defined condition.		
Google Workspace Enabling Features	Google Session Terminate	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			

Google Workspace Customers are responsible for:

a. Defining the conditions requiring a user session to terminate
b. Terminating a user session after any of the defined conditions occur

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Google Session Terminate**

A description of each feature and implementation guidance is included below.

Google Session Terminate

As an administrator, you can control how long users can access Google services, such as Gmail on the web, without having to sign in again. For example, for users that work remotely or from untrusted locations, you might want to limit the time that they can access sensitive resources by applying a shorter web session length. If users want to continue accessing a resource when a session ends, they're prompted to sign in again and start a new session.

Steps to Configure:

1. Sign in with an administrator account to the **Google Admin** console.
    a. If you are not using an administrator account, you cannot access the Admin console.
2. In the Admin console, go to **Menu** and then **Security** and then **Access and Data Control** and then **Google Session** control.
3. On the left, select the organizational unit where you want to set session length.
4. For all users, select the top-level organizational unit. Otherwise, select another organization to make settings for its users. Initially, an organization inherits the settings of its parent organization.
5. For **Session control**, under **Web session duration**, choose the length of time after which the user has to sign in again.

6. Click **Override** to keep the setting the same, even if the parent setting changes.
7. If the organizational unit's status is already Overridden, choose one of the following options:
    a. **Inherit**—Reverts to the same setting as its parent
    b. **Save**—Saves your new setting (even if the parent setting changes)

Additional Considerations

1. The session length for admins using the Google Admin console is set to one hour and cannot be modified. After an hour, admins need to sign in again. This length applies only to the Admin console. Other Google services have the session lengths they are respectively set to.
2. You cannot configure session lengths for native mobile apps, such as Gmail or Google Calendar, on Android or Apple iOS devices. Session lengths are not enforced on OAuth-authenticated apps or ChromeOS.
3. Login sessions for native mobile apps do not expire unless there's an event that causes a need for reauthentication, such as when a user's password is reset.
4. You can apply session-length settings only to Chrome Browser on Android or iOS devices when the user is not signed in. If the user is signed in, settings won't apply. However, you can apply session-length settings as normal on other mobile browsers, such as Apple Safari and Mozilla Firefox.

Supplemental Guidance

- Google Session Terminate

Control Domain	**Access Control**		
Control #	**AC.L2-3.1.12**		
Control Description	Monitor and control remote access sessions.		
Google Workspace Enabling Features	Admin SDK (GCP) Security Investigation Tool	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Permitting remote access sessions b. Identifying the types of permitted remote access			

c. Controlling remote access sessions; and
d. Monitoring remote access sessions.

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Admin SDK (GCP)**
- **Security Investigation Tool**

A description of each feature and implementation guidance is included below.

Admin SDK (GCP)
The Admin SDK API is a collection of RESTful interfaces that empower administrators to manage Google Workspace organizations at scale. You can programmatically integrate with IT infrastructure, create users, update settings, audit activity, and more. The Admn SDK is part of Google Cloud Platform. Admin APIs are disabled by default. In order to use the Google Workspace APIs, you must log into the GCP console and enable the APIs. There is no charge to use the GCP console.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Security Investigation Tool
As your organization's administrator, you can run searches and take action on security issues related to Admin data action log events. You can view a record of actions performed in the Google Admin console or the Google Workspace Admin SDK Reports API, such as when an administrator accessed, removed, and restored sensitive data from any events.

To search and investigate user log events:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the **Admin console**, go to **Menu** and then **Security** and then **Security center** and then **Investigation tool**.
3. Choose **Admin data action log events** as the data source for your search.
4. Click Add Condition.

You can include one or more conditions in your search. For details about which conditions are available for User log events, see Customize searches within the investigation tool > Conditions for user log events. For example, you can narrow your search based on the Date of the event, the name of the user, or an Event type such as a password change, 2SV enrollment, or a failed login.

5. Click **Search**.
6. The search results are displayed at the bottom of the page.

Supplemental Guidance
• Admin SDK • Admin SDK APIs • Security investigation tool

Control Domain	Access Control		
Control #	**AC.L2-3.1.15**		
Control Description	Authorize remote execution of privileged commands and remote access to security-relevant information.		
Google Workspace Enabling Features	Admin SDK (GCP) Admin Roles	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			

Google Workspace Customers are responsible for:

a. Identifying privileged commands authorized for remote execution via Admin SDK
b. Identifying security-relevant information authorized to be accessed remotely via Admin SDK
c. Authorizing the execution of the identified privileged commands via remote access
d. Authorizing access to the identified security-relevant information via remote access

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Admin SDK (GCP)**
- **Admin Roles**

A description of each feature and implementation guidance is included below.

Admin SDK (GCP)
The Admin SDK API is a collection of RESTful interfaces that empower administrators to manage Google Workspace organizations at scale. You can programmatically integrate with IT infrastructure, create users, update settings, audit activity, and more.

Customers interested in using this feature can use the link in the supplemental guidance for more information. **Admin Roles** When you specify privileges in the Admin Console, you also grant corresponding Admin API resource privileges. For example, if a role is assigned the Groups privilege, then they can create, manage, and delete groups in the Admin Console and perform the same actions using the Admin API. *Customers interested in using this feature can use the link in the supplemental guidance for more information.* **Additional Considerations** 1. The Admn SDK is part of Google Cloud Platform. In order to use the Google Workspace APIs, you must log into the GCP console and enable the APIs. There is no charge to use the GCP console.
Supplemental Guidance
• Admin SDK • Admin SDK APIs • Admin Roles

Control Domain	**Access Control**		
Control #	**AC.L2-3.1.18**		
Control Description	Control connection of mobile devices		
Google Workspace Enabling Features	Advanced Mobile Security	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Identifying mobile devices that process, store, or transmit CUI; b. Authorizing mobile device connections; and c. Logging and monitoring mobile device connections			

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Advanced Mobile Security**

A description of each feature and implementation guidance is included below.

Advanced Mobile Security
As an administrator, you can see a list of mobile devices that users have used to sign in to their managed accounts. You can see details including the device type and model, the last time it synchronized work data, and the name of the user who accesses data on it. From the list, you can block a device from syncing work data, wipe data from a lost device, and more.

Steps to view the mobile devices list:

1. Sign in with an administrator account to the **Google Admin** console.
2. Go to **Menu** and then **Devices** and then **Overview**.
3. Click **Mobile devices** to get a list of your organization's managed devices.

As an administrator, you can also individually review user-owned devices that request access to Google Workspace. When a user adds a work or school account to their device, they see a message that an admin needs to review and approve the device. Once you approve a device, the user can access their work account data on the device.

Steps to turn on admin approval for device access:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the Admin console, go to **Menu**, then select **Devices,** then select **Mobile & endpoints**, then select Settings, and then select **Universal**.
3. Click **Security** and then Device approvals.
4. Check the **Require admin approval** box.
5. Enter an email address to get notifications when users enroll their devices and require approval before they can access their work data.
6. Click **Save**

Finally, as your organization's administrator, you can run searches and take action on security issues related to Device log events. You can view a record of actions on computers, mobile devices, and smart home devices that are used to access your organization's data. For example, you can see when a user added their account to a device or if a device's password doesn't follow your password policy. You can also set an alert to be notified when an activity occurs.

There is nothing that needs to be configured to use this feature. Please refer to supplemental guidance below for additional details about this feature.

Additional Considerations

1. Company owned devices that are registered by serial number are automatically approved, except Android devices with a work profile.
2. To see all audit events for mobile devices, the devices need to be managed using advanced device management.
3. To see changes to applications on Android devices, you must turn on application auditing.
4. You can't see activities for devices that sync corporate data using Google Sync.
5. If you downgrade to an edition that doesn't support the audit log, the audit log stops collecting data for new events. However, old data is still available to admins.

Supplemental Guidance

- View mobile devices that access your workspace account
- Turn on admin approval for device access
- Device log events

Control Domain	**Access Control**		
Control #	**AC.L2-3.1.19**		
Control Description	Encrypt CUI on mobile devices and mobile computing platforms.		
Google Workspace Enabling Features	Advanced Mobile Security		

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Identifying mobile devices and mobile computing platforms that process, store, or transmit CUI; and
b. Employing encryption to protect CUI on identified mobile devices and mobile computing platforms.

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Advanced mobile security and app management**

A description of each feature and implementation guidance is included below.

Advanced mobile security and app management

As an administrator, you can require data encryption on devices so that the data can only be read when a device is unlocked. Encryption adds protection if a device is lost or stolen. Unlocking the device decrypts the data.

Steps to Configure

1. Sign in with an administrator account to the Google Admin console.
2. In the Admin console, go to **Menu**, then select **Devices**, then select **Mobile & endpoints**, then select **Settings**, and then select **Universal**.
3. Click **Security**.
4. Turn on **Require Device Encryption**.
5. Click **Save**.

Additional Considerations

1. This feature is supported for Android 3.0 Honeycomb and later devices using Android Sync, and iOS devices using iOS Sync or Google Sync. For other devices and third-party apps, contact the device manufacturer or app developer.
2. You should ensure that any mobile devices which process, store, or transmit CUI use FIPS-validated cryptographic modules to comply with SC.L2-3.13.11.

Supplemental Guidance

- Advanced Mobile Management

Control Domain	**Access Control**		
Control #	**AC.L1-3.1.20**		
Control Description	Verify and control/limit connections to and use of external systems.		
Google Workspace Enabling Features	API Controls End User Access	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Identifying connections permitted to external systems from your Google Workspace account; b. Identifying the use of external systems; c. Verifying connections to external systems from your Google Workspace account;			

d. Verifying the use of external systems;
e. Controlling and limiting connections to external systems; and
f. Limiting and controlling the use of external systems.

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **API Controls**
- **End User Access**

A description of each feature and implementation guidance is included below.

API Controls
When users sign in to third-party apps using the "Sign in with Google" option (single sign-on), you can control how those apps access your organization's Google data. Use settings in the Google Admin console to govern access to Google Workspace services through OAuth 2.0. Some apps use OAuth 2.0 scopes—a mechanism to limit access to a user's account.

By default, users are permitted to access any third-party apps. To change this setting, follow the steps below:

1. Sign in with an administrator account to the Google Admin console.
2. In the Admin console, go to **Menu** and then **Security** and then **Access and data control** and then **API controls**.
3. Click **Settings** to expand the settings group.
4. Select either
    a. Allow users to access third-party apps that only request basic info need for Sign in with Google, or
    b. Don't allow users to access any third-party apps
5. Click **Save**.

End User Access
For users in your organization to synchronize their Google Workspace account email with other email clients, such as Microsoft Outlook or Apple Mail, you need to turn on POP or IMAP in the Google Admin console. You can turn them on for everyone or only for people in certain groups or departments.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. You are responsible for establishing terms and conditions with the services connected to your Google Workspace account.

Supplemental Guidance
• API Controls • End User Access

Control #	AC.L1-3.1.22		
Control Description	Control information posted or processed on publicly accessible information systems.		
Google Workspace Enabling Features	Admin Roles Google Sites	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			

Google Workspace Customers are responsible for:

a. Identifying individuals authorized to post or process information on publicly accessible systems;
b. Identifying procedures to ensure CUI is not posted or processed on publicly accessible systems;
c. Establishing a review process prior to posting of any content to publicly accessible systems;
d. Ensuring content on publicly accessible systems is reviewed to ensure that it does not include CUI;
e. Implementing mechanisms to remove and address improper posting of CUI.

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Admin Roles**
- **Google Sites**

A description of each feature and implementation guidance is included below.

Admin Roles
You can manage who is authorized to access and edit content in Google sites using Admin Roles.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Google Sites
By default, Google Sites is not public. If you decide to make your Google sites public, then you can review the changes made to your draft site since the last time it was published in a side-by-side comparison.

1. On your computer, open a site in new Google Sites.
2. At the top, click Publish.

The screen will split into a side-by-side display, with the draft on the left and the current published version on the right. Annotations on the left show unpublished changes to your site.

3. To show a different page, on the left, click a **page**.
4. To return to the draft site to make changes, in the top left, click **Back**.
5. When you're ready to publish the draft, in the top right, click **Publish**.

Additional Considerations

1. You should create procedures to ensure that publicly-accessible information does not contain CUI.
2. You should create a review process for the proposed content prior to posting to any publicly accessible Google Workspace site.
3. You should train authorized individuals to help ensure that publicly-accessible information does not contain non-public organizational information.
4. You should review the proposed content of publicly accessible information for CUI prior to posting onto Google Workspace.
5. You should review the content on the publicly accessible information system for CUI at a defined timeline and remove CUI from the publicly accessible Google Site, if discovered.

Supplemental Guidance

- Admin Roles
- Google Sites

Control Domain	Audit & Accountability		
Control #	**AU.L2-3.3.1**		
Control Description	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.		
Google Workspace Enabling Features	Reports API (GCP)	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			

Google Workspace Customers are responsible for:

a. Specifying audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
b. Defining retention requirements for audit records; and
c. Retaining audit records, as defined.

Google is responsible for:

d. Defining the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
e. Generating audit records;
f. Ensuring audit records, once created, contain the defined content;

When configured correctly, the following feature(s) may be used to support this control:

- **Reports API (GCP)**

A description of each feature and implementation guidance is included below.

Reports API (GCP)
The Reports API is a RESTful API you can use to access information about the Google Workspace activities of your users. The Reports API is part of the Admin SDK API. The Reports API provides both Activity reports, which report events for a specific application or service, such as Google Drive or the Admin console, and Usage reports, which list Google Workspace events caused by users. Customer usage reports list events for all users in your domain.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. You should carefully review the log event data captured by Google Workspace and the retention period for each event.
2. If your data retention needs are greater than the defined retention periods, then you should consider using the Reports API to export data to your central audit log repository.
3. You can also opt to share log data with Google Cloud. If you turn on sharing, data is forwarded to Cloud Logging, where you can query and view your logs, and control how you route and store your logs (Requires a GCP subscription).

Supplemental Guidance

- Reports API
- Event retention periods

Control Domain	**Audit & Accountability**		
Control #	**AU.L2-3.3.3**		
Control Description	Review and update logged events.		
Google Workspace Enabling Features	Security Investigation Tool	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Defining a process for determining when to review logged events;
b. Review event types being logged in accordance with the defined review process;
c. Updating event types being logged based on the review.

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Security Investigation Tool**

A description of each feature and implementation guidance is included below.

Security Investigation Tool

In the Google Admin console, you can use the security investigation tool to review user and administrator activity in your organization, and to take action based on search results. You can use the information to track users and admins, and for security purposes.

To access data in the investigation tool, from the Google Admin console Home page:

1. Click **Security** and then **Security center** and then **Investigation tool**.

Google Workspace collects multiple data sources and event logs. You should become familiar with the data sources and the attributes available. Please see the link in the supplemental guidance for additional information.

Additional Considerations

1. You cannot change which data sources are collected or which attributes are collected for each event log.
2. Access to specific data sources in the security investigation tool depends on your Google Workspace edition and your administrative privileges for specific features in the Google Admin console.

Supplemental Guidance

- Security Investigation Tool

Control Domain	Audit & Accountability		
Control #	**AU.L2-3.3.5**		
Control Description	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.		
Google Workspace Enabling Features	Security Investigation Tool	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Defining audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity; and
b. Correlating the defined audit record review, analysis, and reporting processes.

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Security Investigation Tool**

A description of each feature and implementation guidance is included below.

Security Investigation Tool
As an administrator, you can set up rules in the Google Admin console to support your incident response and investigation policies. To configure a rule, you set up conditions for the rule, and specify what actions to perform when the conditions are met. A rule is simply a way of saying, if x happens, automatically do y. For example, you can set up rules to be notified of specific activity within your domain—such as a suspicious sign-in attempt, a compromised mobile device, or when another administrator changes settings. Set up rules using the security investigation tool to automate actions that happen in response to activity within your domain.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. You can opt to share log data with Google Cloud. If you turn on sharing, data is forwarded to Cloud Logging, where you can query and view your logs, and control how you route and store your logs. (Requires a GCP subscription)

Supplemental Guidance

- Security Investigation Tool

Control Domain	Audit & Accountability		
Control #	**AU.L2-3.3.6**		
Control Description	Provide audit record reduction and report generation to support on-demand analysis and reporting.		
Google Workspace Enabling Features	Security Investigation Tool	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			

Google Workspace Customers are responsible for:

a. Providing an audit record reduction capability that supports on-demand analysis; and
b. Providing a report generation capability that supports on-demand reporting.

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Security Investigation Tool**

A description of each feature and implementation guidance is included below.

Security Investigation Tool
As an administrator, you can set up rules in the Google Admin console. To configure a rule, you set up conditions for the rule, and specify what actions to perform when the conditions are met. There are several types of rules on the Rules page, including reporting rules, activity rules, data protection rules, and system defined rules. Reporting rules are custom rules created by administrators from the audit and investigation page or from the Rules page. You can use these rules to create and manage custom alerts based on your organization's log event data (previously called audit logs).

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. You can opt to share log data with Google Cloud. If you turn on sharing, data is forwarded to Cloud Logging, where you can query and view your logs, and control how you route and store your logs. (Requires a GCP subscription)

Supplemental Guidance

- Security Investigation Tool

Control Domain	**Audit & Accountability**		
Control #	**AU.L2-3.3.8**		
Control Description	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.		
Google Workspace Enabling Features	Admin Roles	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description			
Google Workspace Customers are responsible for: a. Protecting audit information from unauthorized access; b. Protecting audit logging tools from unauthorized access; The following objectives can be inherited from Google: c. Protecting audit information from unauthorized modification; d. Protecting audit information from unauthorized deletion; e. Protecting audit logging tools from unauthorized modification; and f. Protecting audit logging tools from unauthorized deletion. When configured correctly, the following feature(s) in Google Workspace may be used to support this control: • **Admin Roles** A description of each feature and implementation guidance is included below. **Admin Roles** To use the security investigation tool, you need to be an administrator with security investigation tool privileges. Super administrators have these privileges by default, or you can add them to a custom administrator role. Soon, administrators will need the Audit and Investigation View privilege instead of the Reports privilege to access log events. To create an admin role for the security investigation tool: 1. Sign in with an administrator account to the Google Admin console. 2. In the Admin console, go to **Menu** and then **Account**, and then **Admin roles**. 3. Choose an option: a. To add the privileges to an existing role, point to the custom administrator role and click View privileges and then Open privileges. b. To create a new admin role, click Create new role, add a name and description, and click Continue. 4. In the Services section, next to Security Center, click the Right arrow to expand the privileges. 5. Next to **This user has full administrative rights for Security Center**, click the Right arrow to expand the privileges. 6. (Optional) To give the admin access to all Security Center features, including the security investigation tool, check the box for “This user has full administrative rights for Security Center” and go to Step 11. 7. Next to Audit and investigation, click the Right arrow to expand the privileges. 8. Choose an option:			

a. To allow the admin to run searches and see returned results, which could contain sensitive content, check the View box.
b. To allow the admin to update content, for example, change the access control list of a document or delete an email, check the Manage box.
c. To allow admins to view complete messages and attachments, including those that violate DLP rules (if the View sensitive content setting is ON) or are reported as inappropriate, check the View sensitive content box.

9. Click Save or Continue.
10. If prompted, review the privileges and click Create Role.
11. Assign the role to a subset of privileged users.

Supplemental Guidance

- Admin Roles

Control Domain	Audit & Accountability		
Control #	**AU.L2-3.3.9**		
Control Description	Limit management of audit logging functionality to a subset of privileged users.		
Google Workspace Enabling Features	Admin Roles	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Defining a subset of privileged users granted access to manage audit logging functionality;
b. Limiting management of audit logging functionality to the defined subset of privileged users.

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Admin Roles**

A description of each feature and implementation guidance is included below.

Admin Roles

To use the security investigation tool, you need to be an administrator with security investigation tool privileges. Super administrators have these privileges by default, or you can add them to a custom administrator role. Soon, administrators will need the Audit and Investigation View privilege instead of the Reports privilege to access log events.

To create an admin role for the security investigation tool:

1. Sign in with an administrator account to the Google Admin console.
2. In the Admin console, go to **Menu** and then **Account**, and then **Admin roles**.
3. Choose an option:
    a. To add the privileges to an existing role, point to the custom administrator role and click View privileges and then Open privileges.
    b. To create a new admin role, click Create new role, add a name and description, and click Continue.
4. In the Services section, next to Security Center, click the Right arrow to expand the privileges.
5. Next to **This user has full administrative rights for Security Center**, click the Right arrow to expand the privileges.
6. (Optional) To give the admin access to all Security Center features, including the security investigation tool, check the box for “This user has full administrative rights for Security Center” and go to Step 11.
7. Next to Audit and investigation, click the Right arrow to expand the privileges.
8. Choose an option:
    a. To allow the admin to run searches and see returned results, which could contain sensitive content, check the View box.
    b. To allow the admin to update content, for example, change the access control list of a document or delete an email, check the Manage box.
    c. To allow admins to view complete messages and attachments, including those that violate DLP rules (if the View sensitive content setting is ON) or are reported as inappropriate, check the View sensitive content box.
9. Click Save or Continue.
10. If prompted, review the privileges and click Create Role.
11. Assign the role to a subset of privileged users.

Supplemental Guidance

- Admin Roles

Control Domain	Configuration Management		
Control #	**CM.L2-3.4.1**		
Control Description	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.		
Google Workspace Enabling Features	Company-owned device management	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Establishing a system inventory
b. Ensuring the system inventory includes hardware, software, firmware, and documentation; and
c. Maintaining, reviewing, and updating the inventory throughout the system development life cycle.

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Company-owned device management**

A description of each feature and implementation guidance is included below.

Company-owned device management
You can manage all of your company-owned devices—mobile devices, laptops, desktops—in one place in your Google Workspace Admin console. Company-owned devices are devices that your organization purchased through a reseller or device vendor, and which they secure and manage for your employees. You can use this feature to populate a system inventory of company-owned devices.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. You should also consider establishing a baseline configuration for your Google Workspace account and maintaining, reviewing, and updating the baseline configuration to address this control.

2. The Center for Internet Security (CIS) is a nonprofit that promotes best practices for securing IT systems and data. They publish a variety of materials including CIS Benchmarks. The CIS Benchmarks are security guidelines that institutions across industries can use to assist in the configuration of their environments. You can access the CIS Benchmarks for configuration of Google Workspace on the CIS website. Please refer to the supplemental guidance for more information.
Supplemental Guidance
• Company-owned device management • CIS Benchmarks

Control Domain	**Configuration Management**		
Control #	**CM.L2-3.4.2**		
Control Description	Establish and enforce security configuration settings for information technology products employed in organizational systems.		
Google Workspace Enabling Features	Security Checklists Security Health	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			

Google Workspace Customers are responsible for:

a. Establishing security configuration settings for Google Workspace and including them in the baseline configuration; and
b. Enforcing security configuration settings for Google Workspace

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Security checklists**

A description of each feature and implementation guidance is included below.

Security checklists
Whether you're a small business owner or IT admin for a large enterprise, Google Workspace offers a range of best practices for protecting your security and privacy. For small businesses, Google Workspace offers a checklist of 14 settings that should be reviewed and configured. For large businesses, Google Workspace offers a checklist with more robust settings.

Customers interested in using this feature can use the links in the supplemental guidance for more information.

Security Health
The security health page allows you to monitor the configuration of your security-related Admin console settings—all from one location in the Google Admin console—and to make changes to those settings.

To view the security health page:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the **Admin console**, go to **Menu** and then **Security** and then **Security center** and then **Security health**.

Depending on the setting status, the far-right column displays a gray icon that you can click for a list of security recommendations, or it displays a green checkbox to indicate a secure configuration. Click the gray icons for more details and instructions.

Supplemental Guidance

- Security checklist for medium and large businesses (100+ users)
- Security checklist for small businesses (1-100 users)
- Security Health

Control Domain	**Configuration Management**		
Control #	**CM.L2-3.4.3**		
Control Description	Track, review, approve or disapprove, and log changes to organizational systems.		
Google Workspace Enabling Features	Multi-party Approval	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Defining logical access restrictions associated with changes to the system;			

b. Documenting logical access restrictions associated with changes to the system;
c. Approving logical access restrictions associated with changes to the system; and
d. Enforcing logical access restrictions associated with changes to the system.

Google is responsible for:

e. Defining physical access restrictions associated with changes to the system;
f. Documenting physical access restrictions associated with changes to the system;
g. Approving physical access restrictions associated with changes to the system;
h. Enforcing physical access restrictions associated with changes to the system;

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Multi-party Approval**

A description of each feature and implementation guidance is included below.

Multi-party Approval

Multi-party approval protects against malicious actions in the Admin console by requiring that any sensitive settings changes—such as turning 2-Step Verification enforcement on or off—must be approved by another super admin. Once a super admin receives and approves the settings change request, the change is carried out automatically, without any further action needed from the requesting admin. Multi-party approval is turned on by default for domains with 2 or more super admins.

Once on, Multi-party approval applies to the following settings:

- 2-Step Verification
- Account recovery
- Advanced Protection
- Google session control
- Login challenges
- Passwordless (beta)
- SSO with third-party IdP
- Domain-wide delegation

To turn on multi-party approval:

1. Sign in with an administrator account to the **Google Admin** console.
2. Go to **Security** and then **Authentication** and then **Multi-party approval** settings.
3. To turn multi-party approval on, check the **Require multi-party approval for sensitive admin actions** box. To turn off, uncheck the box.
4. Click **Save**.

Once enabled, either the requester or the approver can view pending or past requests on the Multi-party approval list page. Clicking a request in the list displays a details page for that

request. On the request details page, requesters can cancel a request, and approvers can approve or reject the request.

Additional Considerations

1. You should consider establishing a tool or process for tracking Google Workspace changes that are not managed by multi-party approval for settings that are important to your organization
2. Consider running searches and taking action on security issues related to Admin log events. For example, you can view a record of actions performed in your Google Admin console, such as when an administrator added a user or turned on a Google Workspace service. Please refer to the supplemental guidance for more information.

Supplemental Guidance

- Multi-party Approval
- View admin log events and create alerts

Control Domain	Configuration Management		
Control #	**CM.L2-3.4.5**		
Control Description	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.		
Google Workspace Enabling Features	Admin Roles	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Enforcing logical access restrictions associated with changes to Google Workspace.

Google is responsible for:

b. Defining physical access restrictions associated with changes to Google Workspace;
c. Documenting physical access restrictions associated with changes to Google Workspace;
d. Approving physical access restrictions associated with changes to Google Workspace;

e. Enforcing physical access restrictions associated with changes to Google Workspace;

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Admin Roles**

A description of each feature and implementation guidance is included below.

Admin Roles
You can enforce logical access restrictions associated with changes to Google Workspace by assigning users to the appropriate roles in Google Workspace. Please refer to AC.L2-3.1.4 for information on the prebuilt admin roles and Custom Roles and how to assign roles.

Additional Considerations

1. Google Workspace does not natively support all objectives for this control. You should consider documenting and approving logical access restrictions associated with changes to Google Workspace.

Supplemental Guidance

- N/A

Control Domain	Configuration Management		
Control #	**CM.L2-3.4.6**		
Control Description	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.		
Google Workspace Enabling Features	Apps	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Defining essential Google Workspace capabilities based on the principle of least functionality; and
b. Configuring Google Workspace to provide only the defined essential capabilities

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Apps**

A description of each feature and implementation guidance is included below.

Apps
As an administrator, you can control who can use which Google services. Just turn the service on or off for those users in your Google Admin console. When users sign in to their account, they have only the services that are turned on for them.

Turn a service on or off for **all** users in your organization:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the **Admin** console, go to **Menu** and then **Apps** and then **Google Workspace** and then **Service status**.
3. Click the service that you want to turn on or off.
4. Click **Service status**.
5. Click **On for everyone** or **Off for everyone.**
6. Click **Save**.

You can also turn a Google Workspace service on or off by department or across departments. Please use the links in the supplemental guidance for more information about and steps to configure or utilize this feature.

When you sign up for Google Workspace, you get core services, such as Gmail, Calendar, and Drive. You can also optionally turn on additional Google services, such as YouTube, Blogger, Google Analytics, and more. As an administrator, you can control access to these additional services. Some services have an individual On or Off control in the Admin console and others don't. For services that do not have this control, you must turn them on or off all at once.

1. Sign in with an administrator account to the **Google Admin** console.
2. In the **Admin** console, go to **Menu** and then **Apps** and then **Additional Google Services.**
3. Click the name of the service you want to turn on or off to open its settings page.
4. Click **Service status**.
5. To turn a service on or off for everyone in your organization, click **On for everyone** or **Off for everyone**
6. Click **Save**.

You can also turn an additional service on or off by department or across departments. Please use the links in the supplemental guidance for more information about and steps to configure or utilize this feature.

As an administrator, you can block user access to some system apps on managed mobile devices. System apps are preinstalled apps such as Clock and Calculator for Android, or FaceTime and iTunes Store for iOS. Many of these apps cannot be uninstalled, but you can allow or block access to them.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Finally, as an administrator, you can allow users in your organization to install and run any Google Workspace Marketplace app, only allowlisted apps, or no apps. If you do not allow users to install apps themselves or only allowlisted apps, you can still install any apps for them.

To add an app to the allowlist or excludelist:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the **Admin** console, go to **Menu** and then **Apps** and then **Google Workspace Marketplace apps** and then **Apps List.**
3. Click **Allowlist app**.
4. Search for the app. To review an app and ensure it's the one you want to allow or exclude, click its name to open the app listing. If you can't find the app, it may be available only for administrators to install and can’t be allowlisted.
5. Next to the app, click **Select**.
6. Select whether to allow or exclude the app and click **Continue**.
7. Select who this setting applies to. For the excludelist, you can only select organizational units. Note:
    a. If you allow the app for a child organizational unit or group, the app is excluded for all other users.
    b. If you add an app to the excludelist, users can still access it if they're allowed to install all apps or if you don't add it to an allowlist, too.
8. Allowlisted apps can still be excluded by API controls.
9. Click **Finish**.

Supplemental Guidance

- Turn a service on or off for Google Workspace users
- Turn on or off additional Google services
- Manage mobile apps for your organization
- Manage system apps on company-owned mobile devices
- Set whether users can install Marketplace apps
- Manage the Marketplace app allowlist for your organization

Control Domain	Configuration Management		
Control #	**CM.L2-3.4.7**		
Control Description	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.		
Google Workspace Enabling Features	Apps	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Defining essential programs; b. Defining the use of nonessential programs; c. Restricting, disabling, or preventing the use of nonessential programs as defined; d. Defining essential services; e. Defining the use of nonessential services; and f. Restricting, disabling, or preventing the use of nonessential services as defined. Google is responsible for: g. Defining essential functions; h. Defining the use of nonessential functions; i. Restricting, disabling, or preventing the use of nonessential functions as defined; j. Defining essential ports; k. Defining the use of nonessential ports; l. Restricting, disabling, or preventing the use of nonessential ports as defined; m. Defining essential protocols; n. Defining the use of nonessential protocols; o. Restricting, disabling, or preventing the use of nonessential protocols as defined; When configured correctly, the following feature(s) in Google Workspace may be used to support this control: • **Apps** Please refer to CM.L2-3.4.6 for a description of each feature and implementation guidance.			
Supplemental Guidance			
• Turn a service on or off for Google Workspace users			

- Turn on or off additional Google services
- Manage mobile apps for your organization
- Manage system apps on company-owned mobile devices
- Set whether users can install Marketplace apps
- Manage the Marketplace app allowlist for your organization

Control Domain	Configuration Management		
Control #	**CM.L2-3.4.8**		
Control Description	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.		
Google Workspace Enabling Features	Apps	**Control Responsibility**	[ ] Google [ ] Shared [X] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Identifying a policy specifying whether whitelisting or blacklisting is to be implemented; b. Specifying the software allowed to execute under whitelisting or denied use under blacklisting; and c. Implementing either whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software as specified. When configured correctly, the following feature(s) in Google Workspace may be used to support this control: • **Apps** Please refer to CM.L2-3.4.6 for a description of each feature and implementation guidance.			
Supplemental Guidance			
• Turn a service on or off for Google Workspace users • Turn on or off additional Google services • Manage mobile apps for your organization			

- Manage system apps on company-owned mobile devices
- Set whether users can install Marketplace apps
- Manage the Marketplace app allowlist for your organization

Control Domain	Configuration Management		
Control #	**CM.L2-3.4.9**		
Control Description	Control and monitor user-installed software.		
Google Workspace Enabling Features	Apps	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Establishing a policy for controlling the installation of software by users;
b. Controlling installation of software by users based on the established policy; and
c. Monitoring installation of software by users.

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Apps**

A description of each feature and implementation guidance is included below.

Apps

As an administrator, you can allow users in your organization to install and run any Google Workspace Marketplace app, only allowlisted apps, or no apps. If you don't allow users to install apps themselves or only allowlisted apps, you can still install any apps for them.

1. Sign in with an administrator account to the Google Admin console.
2. Sign in with an administrator account to the **Google Admin** console.
3. In the **Admin** console, go to **Menu** and then **Apps** and then **Google Workspace Marketplace apps** and then **Apps list**.
4. Click **User Install Settings**.
5. (Optional) To apply the setting only to some users, at the side, select an organizational unit (often used for departments) or configuration group (advanced).
6. In the **Manage access to apps** section, select whether users can install any apps, only allowlisted apps, or no apps.

7. (Optional) If you choose to allow only allowlisted apps, you can also choose if users can install all internal apps, even if they're not on your allowlist.
8. Click **Save**.

As an admin, you can control which apps Android and iOS device users can find and install for work or school by adding them to the Web and mobile app list in the Google Admin console. You can add public apps—such as third-party apps for security, business, and document management—and private apps. Though you can add a paid public app to the list, you can't bulk purchase the app for your users through Google endpoint management.

You can review all the apps available to an organizational unit or group, or which organizational units and groups have access to a specific mobile app:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the **Admin** console, go to **Menu** and then **Apps** and then **Web and mobile apps.**
3. To review the apps that a specific organizational unit or group can access:
    a. Click **Add a filter**.
    b. Click **Organizational unit** or **Group**.
    c. Select the organizational unit or group.
4. To review the distribution of a specific app, point to the row of the app you want to review and click **Access details**. A panel opens that lists the groups and organizational units and their app access status.

You can also add or remove private or internal apps for users to install. Please use the link in the supplemental guidance for more information about and steps to configure or utilize this service.

Supplemental Guidance

- Manage system apps on company-owned mobile devices
- Set whether users can install Marketplace apps

Control Domain	Identification & Authentication
Control #	**IA.L1-3.5.1**
Control Description	Identify system users, processes acting on behalf of users, and devices.

Google Workspace Enabling Features	User Directory Google Cloud Directory Sync Directory Sync (beta) SSO Profiles API Controls Basic & Advanced Mobile Security Endpoint Management Company-owned device management	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Identifying system users;
b. Identifying processes acting on behalf of users; and
c. Identifying devices accessing the system

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- Refer to AC.L1-3.1.1

Additional Considerations

1. Customers should consider establishing unique usernames that identify each user.

Supplemental Guidance

- Google Workspace Directory
- Google Cloud Directory Sync
- Directory Sync (beta)
- SSO Profiles
- API Controls
- Basic & Advanced Mobile Management
- Endpoint Management
- Company-owned device management

Control Domain	Identification & Authentication		
Control #	**IA.L1-3.5.2**		
Control Description	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.		
Google Workspace Enabling Features	Google Sign In SSO Profiles API Controls Context Aware Access	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Authenticating or verifying the identity of each user as a prerequisite to system access;
b. Authenticating or verifying the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access; and
c. Authenticating the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Google Sign In**
- **SSO Profiles**
- **API Controls**
- **Context Aware Access**

A description of each feature and implementation guidance is included below.

Google Sign In
All Google services, including Google Workspace, rely on Google Sign-In to authenticate users.

Google is responsible for authenticating users through Google Sign-in. You do not need to configure anything to use this service to authenticate users.

SSO Profiles
Single sign-on (SSO) allows users to sign in to many enterprise cloud applications using a single set of credentials. Google Workspace supports SSO from third-party identity providers (IdPs). Google Workspace supports both SAML and OIDC SSO protocols. SAML SSO supports any IdP. You can create up to 1000 profiles in your organization.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

API Controls
You can use API Controls to manage access by Third-Party Apps. Google Workspace utilizes OAuth 2.0 to issue tokens for third-party applications that require access to user data.

Google is responsible for authenticating processes acting on behalf of users in applications that you have permitted in API controls. You do not need to configure anything to use this feature.

Context Aware Access
Context-Aware Access gives you control over which apps a user can access based on their context, such as whether their device complies with your IT policy. Using Context-Aware Access, you can create granular access control policies to authenticate devices. For example, you can create a policy that only if a device has a serial number that matches one that's in the company's asset management system, or if a device has a valid enterprise certificate that's issued by the company, then the device may access Google Workspace data.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Supplemental Guidance
• Context Aware Access

Control Domain	**Identification & Authentication**		
Control #	**IA.L2-3.5.3**		
Control Description	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.		
Google Workspace Enabling Features	2-Step Verification	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for:			

a. Identifying privileged accounts;
b. Implementing multifactor authentication for network access to privileged accounts;
c. Implementing multifactor authentication for network access to non-privileged accounts.

Google is responsible for:

d. Implementing multifactor authentication for local access to privileged accounts;

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **2-Step Verification**

A description of each feature and implementation guidance is included below.

2-Step Verification

As an administrator, you can enable 2-Step Verification (2SV) for your users who access Google Workspace to put an extra barrier between your business and cybercriminals who try to steal usernames and passwords to access business data. When you set up 2SV, you choose the second verification step for your users. 2SV methods include:

- Security Keys
- Google Prompt
- Google Authenticator
- Backup Codes
- Text messages
- Passkeys

Steps to configure 2-Step Verification:

1. Sign in with a super administrator account to the Google Admin console.
2. In the Admin console, go to **Menu** and then **Security** and then **Authentication** and then **2-step verification**.
3. (Optional) To apply the setting only to some users, at the side, select an organizational unit (often used for departments) or configuration group (advanced)
4. Click **Allow users to turn on 2-Step Verification**.
5. For Enforcement, choose an option:
    - On—Starts immediately.
    - Turn on enforcement from date—Select the start date. Users see reminders to enroll in 2SV when they sign in.
6. For Methods, select the enforcement method
7. Click **Save**.

If using SSO, steps to set up 2-Step Verification with SSO:

1. Sign in with an administrator account to the Google Admin console.

2. In the Admin console, go to **Menu** and then **Security** and then **Authentication** and then **Login challenges**.
3. On the left, select the organizational unit where you want to set the policy.
4. For all users, select the top-level organizational unit. Initially, organizational units inherit the settings of its parent.
5. Click **Post-SSO verification**.
6. Choose settings according to how you use SSO profiles in your organization. You can apply a setting for users who use the legacy SSO profile and for users who sign in using other SSO profiles.
7. On the bottom right, click **Save**

Supplemental Guidance

- 2-Step Verification

Control Domain	Identification & Authentication		
Control #	**IA.L2-3.5.6**		
Control Description	Disable identifiers after a defined period of inactivity.		
Google Workspace Enabling Features	User Directory	**Control Responsibility**	[ ] Google [ ] Shared [X] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Defining a period of inactivity after which an identifier is disabled; and
b. Disabling identifiers after the defined period of inactivity

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **User Directory**

A description of each feature and implementation guidance is included below.

User Directory

As an administrator, you can view your users' last sign-in and manually suspend accounts that have been inactive for the defined period of inactivity. From the Google Admin console Home page, click Users. Under Last sign in, you will see the approximate time of the user's last

sign in (e.g., 2 minutes ago, 1 day ago, or 2 months ago). If a new user has not signed in to their account for the first time, the column shows “Hasn't signed in.”

You can temporarily block a user's access to your organization's Google services by suspending their account. When you suspend an account, the user's:

- Email, documents, calendars, and other data are not deleted.
- Shared documents are still accessible to collaborators.
- New email and calendar invitations are blocked.

After suspending a user, you can restore the account at any time.

To suspend an individual user:

1. Sign in with an administrator account to the **Google Admin** console
2. In the Admin console, go to **Menu** and then **Directory** and then **Users**.
3. In the **Users** list, find the user.
4. Hover over the user you want to suspend and click **More options** and then **Suspend** user.
5. To confirm, click **Suspend**.

Additional Considerations

1. If using Directory Sync or Google Cloud Directory Sync, then users can be suspended in your LDAP server and their status will be synced to their Google Workspace account.

Supplemental Guidance

- Suspend a user temporarily

Control Domain	Identification and Authentication (IA)		
Control #	**IA.L2-3.5.7**		
Control Description	Enforce a minimum password complexity and change of characters when new passwords are created.		
Google Workspace Enabling Features	Password Management Password Sync	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Defining password complexity requirements;
b. Defining password change of character requirements;
c. Enforcing minimum password complexity requirements when new passwords are created; and
d. Enforcing minimum password change of character requirements as defined when new passwords are created.

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Password Management**
- **Password Sync**

A description of each feature and implementation guidance is included below.

Password Management

Google Workspace provides built-in password management options within the Admin console. Follow the steps below to enforce a minimum password complexity and change of characters when new passwords are created.

1. Sign in with an administrator account to the Google Admin console.
2. In the Admin console, go to **Menu**, select **Security**, select **Authentication,** select **Password Management**.
3. On the left, select the organizational unit where you want to set the password policies. For all users, select the top-level organizational unit. Otherwise, select another organization to make settings for its users. Initially, an organization inherits the settings of its parent organization.
4. In the Strength section, check the “Enforce strong password” box

When checked, Google uses a password strength-rating algorithm to ensure that a password has a high level of randomness, called password entropy, which is achieved when users create passwords with a long string of characters of different types, such as uppercase letters, lowercase letters, numeral, and special characters. Note: a strong password doesn’t need to have a specific number of characters of a specific type.

5. In the Reuse section, ensure the “Allow password reuse” box is UNCHECKED (default)

When left unchecked, this will ensure that users must change at least one character when creating new passwords.

Depending on your organization’s security policies, you may also use the following Google Workspace features to meet this control:

6. In the Length section, enter a minimum and maximum length for your users' passwords. It can be between 8 and 100 characters.
7. In the Expiration section, select the period of time after which passwords expire.
8. Give your users tips for creating a strong password.

Password Sync

Password Sync can be used to update your users' Google Workspace and Cloud Identity passwords directly from Microsoft Active Directory (if used). After Password Sync is installed and configured, it sends updated passwords to your Google Account each time an Active Directory user changes your password. Please follow Google Support pages to enable Password Sync.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. Due to Google Workspace's use of entropy to determine password strength, you should ensure your company's policies do not require a specific number of uppercase, lowercase, numbers, or special characters in your passwords.
2. If Password Sync is enabled, then you should consider enforcing a minimum password complexity and change of characters requirement for new passwords within your Active Directory service.

Supplemental Guidance

- Password Management
- Password Sync

Control #	IA.L2-3.5.8		
Control Description	Prohibit password reuse for a specified number of generations		
Google Workspace Enabling Features	Password Management Password Sync	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for:			

a. Specifying the number of generations during which a password cannot be reused is specified and
b. Prohibiting reuse of passwords during the specified number of generations**.**

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Password Management**
- **Password Sync**

A description of each feature and implementation guidance is included below.

Password Management

Google Workspace provides built-in password management options within the Admin console.

1. Sign in with an administrator account to the Google Admin console.
   If you aren't using an administrator account, you can't access the Admin console.
2. In the Admin console, go to **Menu**, select **Security**, select **Authentication,** select **Password Management**.
3. In the Reuse section, ensure the "Allow password reuse" box is unchecked (default)

By default, Google Workspace is configured to prohibit the reuse of passwords.

Password Sync

Password Sync can be used to update your users' Google Workspace and Cloud Identity passwords directly from Microsoft Active Directory. After Password Sync is installed and configured, it sends updated passwords to Google Workspace each time an Active Directory user changes their password.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. If Password Sync is enabled, then you should consider enforcing a minimum password complexity and change of characters requirement for new passwords within your Active Directory service.
2. You cannot set the password history that Google reviews to prevent reuse.

Supplemental Guidance

- Password Management
- Password Sync

Control Domain	Identification & Authentication		
Control #	**IA.L2-3.5.9**		
Control Description	Allow temporary password use for system logons with an immediate change to a permanent password.		
Google Workspace Enabling Features	User Directory	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Requiring an immediate change to a permanent password when a temporary password is used for system logon

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **User Directory**

A description of each feature and implementation guidance is included below.

User Directory

If a user forgets the password for their managed Google account (for example, their Google Workspace or Cloud Identity account) or if you think their account has been compromised, you can reset their password from the Google Admin console. Resetting a password changes it for the user's online accounts. If the user has Google Drive for desktop, the password doesn't change there. After resetting a user's password, you must reset the user's sign-in cookies.

Steps to reset a user's password:

1. Sign in with an administrator account to the **Google Admin console**.
2. In the **Admin console**, go to **Menu** and then **Directory** and then **Users**.
3. In the **Users** list, find the user whose password needs reset.
4. Point to the user and then click **Reset password** at the right.
5. In the Reset password box, select an option:
    a. **Automatically generate** a password or
    b. **Create password**.
6. To have the user change the password the next time they sign in, select **Create Password** and check the **Ask for a password change at the next sign-in** box.

7. Click **Reset**
8. Choose one:
    a. To finish, click **Done**. Note: You need to send the user their new password.
    b. To email the password to the user, click **Email Password** and then **Send**.
9. Reset the users sign-in cookies

Supplemental Guidance

- Reset a user's password

Control Domain	Incident Response		
Control #	**IA.L2-3.6.1**		
Control Description	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.		
Google Workspace Enabling Features	Alert Center Security Investigation Tool	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description:

Google Workspace Customers are responsible for:

a. Establishing an operational incident-handling capability;
b. Including detection in the operational incident-handling capability;
c. Including analysis in the operational incident-handling capability;

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Alert Center**
- **Security Investigation Tool**

A description of each feature and implementation guidance is included below.

Alert Center

The alert center includes two types of pages:

- A list of alerts affecting your domain—This page is displayed after you sign in to the Google Admin console and navigate to the alert center. This list can span several pages, depending on the number of alerts that are active.

- A details page that provides more information about each alert—You can access the details by clicking any item on the list of alerts.

To access the alert center:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the **Admin** console, go to **Menu** and then **Security** and then **Alert center.**

Security Investigation Tool

As an administrator, you can use the security investigation tool to identify, triage, and take action on security and privacy issues in your domain.

For example, you can use the investigation tool to:

- Access data about devices.
- Access device log data to get a clear view of the devices and applications being used to access your data.
- Access data about Gmail messages, including email content.
- Access Gmail log data to find and erase malicious emails, mark emails as spam or phishing, or send emails to users' inboxes.
- View search results that list suspended users.
- Access Drive log data to investigate file sharing in your organization, investigate the creation and deletion of documents, investigate who accessed documents, and more.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. Depending on the nature of the incident, other features in Google Workspace may support your incident handling capability. You can use Google Workspace to recover deleted files and folders for Drive users, wipe corporate data from a device, block a managed device, and more.
2. You should consider creating Incident Response plans and procedures that include incident preparation, detection, analysis, containment, recovery, and user response activities for your Google Workspace data.

Supplemental Guidance

- Alert Center
- Security Investigation Tool

Control Domain	Personnel Security		
Control #	**PS.L2-3.9.2**		
Control Description	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.		
Google Workspace Enabling Features	User Directory	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			

Google Workspace Customers are responsible for:

a. Terminating system access and credentials consistent with personnel actions such as termination or transfer; and

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **User Directory**

A description of each feature and implementation guidance is included below.

User Directory

As a Google Workspace administrator, you can delete a user's Google Workspace account when they leave your organization and no longer need access to your Google Workspace services, or you can temporarily suspend a user's access to their account.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. You should consider establishing a policy and/or process for terminating system access and any credentials coincident with personnel actions;
2. You should also consider protecting the system during and after personnel transfer actions by requiring transferred or terminated personnel to return system-related property and by conducting exit interviews.
3. If you are using Directory Sync or Google Cloud Directory Sync, then you should terminate or suspend the user in your organization's LDAP solution and their status will be synced to Google Workspace.

Supplemental Guidance
• Delete or remove a user from your organization

Control Domain	System & Communications Protection		
Control #	**SC.L1-3.13.1**		
Control Description	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.		
Google Workspace Enabling Features	MTA-STS and TLS Secure transport (TLS) compliance S/MIME for message encryption	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			

Google Workspace Customers are responsible for:

a. Defining the external system boundary;
b. Defining key internal system boundaries;
c. Monitoring communications at the external system boundary;
d. Monitoring communications at key internal boundaries;
e. Controlling communications at the external system boundary;
f. Controlling communications at key internal boundaries;
g. Protecting communications at the external system boundary; and
h. Protecting communications at key internal boundaries

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **MTA-STS and TLS**
- **Secure transport (TLS) compliance**
- **S/MIME for message encryption**

A description of each feature and implementation guidance is included below.

MTA-STS and TLS

Like all mail providers, Gmail uses Simple Mail Transfer Protocol (SMTP) to send and receive messages. SMTP alone does not provide security, and many SMTP servers don't have added security to prevent malicious attacks. You can increase Gmail security by turning on MTA Strict Transport Security (MTA-STS) for your domain. MTA-STS improves Gmail security by requiring

authentication checks and encryption for email sent to your domain. Use Transport Layer Security (TLS) reporting to get information about external server connections to your domain.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Secure transport (TLS) compliance
Transport Layer Security (TLS) is a protocol that encrypts email messages for security and privacy. TLS prevents unauthorized access of messages when they're sent over internet connections. By default, Gmail always tries to send messages over a secure TLS connection. A secure, end-to-end TLS connection requires that both the sending and receiving server use TLS. If the receiving server doesn't use TLS, Gmail still sends messages but the connection is not secure. You can use Google Workspace to require TLS when communicating with specified domains OR you can require that email always be sent over a secure TLS connection, even when you're not sure receiving servers use TLS, by adding an alternate secure route setting. When you add an alternate secure route with this setting, outgoing email from your domain is sent through a host or third-party service that encrypts messages before they are delivered to receiving servers. To use TLS for messages sent to and from domains and addresses that you specify, use the Secure transport (TLS) compliance setting. This setting includes options to require a CA-signed certificate, verify the hostname associated with the certificate, and test the TLS connection.

Customers interested in using this feature can use the links in the supplemental guidance for more information.

S/MIME for message encryption
You can set up hosted Secure/Multipurpose Internet Mail Extensions (S/MIME) in your Google Admin console to help protect your people in your organization from phishing, harmful attachments, and other email threats. S/MIME improves email security by encrypting and adding a digital signature to messages. Messages are decrypted using the combination of a public key and a private key

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. Customers can choose to enable MTA-STS to disable weak ciphers (SSL, 3DES, and RC4) on mail servers. When configuring MTA-STS, it is important for customers to take a responsible approach to minimize loss of email. It is recommended that the feature is enabled in testing mode and customers investigate MTA-STS reports prior to enabling enforcement mode.

2. If needed, you can customize how email is routed and stored to suit your business or IT needs. You can configure inbound, outbound, and internal delivery options, such as for using Gmail with legacy email systems. Some of the options include:
    a. Add mail servers for Gmail email routing
    b. Set up Default routing for your organization
    c. Add Gmail Routing settings
    d. Deliver email to multiple inboxes with dual delivery
    e. Send email to two email systems with split delivery
    f. Get misaddressed email in a catch-all mailbox
    g. Redirect or forward Gmail messages to another user
    h. Forward email to a third-party CRM
    i. Add an outbound gateway for outgoing email
    j. Set up an inbound mail gateway
    k. Allow per-user outbound gateways
    l. Route journal messages to Google Vault
3. If the above features are not configured, then Google Workspace is responsible for the routing and delivery of email communications. Please refer to the supplemental guidance for additional information about these features.
4. With Google Workspace Client-side encryption (CSE), you can add another layer of encryption to your organization's data—like files and emails—in addition to the default encryption that Google Workspace provides. CSE helps to keep your organization's data private with end-to-end encryption that Google servers and third parties can't decrypt, giving your organization greater control over access to its data. CSE is especially beneficial for organizations that store sensitive or regulated data, like intellectual property, healthcare records, or financial data. Please refer to the supplemental guidance for additional information about these features.
5. Additionally, with Meet Client-side Encryption (CSE), all media is encrypted by each participant's browser using keys only made available to the participants. Only the meeting participants can decrypt the call media while it remains unreadable to Google's servers or any other service provider. Please refer to the supplemental guidance for additional information about these features.

Supplemental Guidance

- MTA-STS and TLS reporting
- Send email over an alternate secure route (TLS)
- Send email over a secure TLS connection
- S/MIME Encryption
- Advanced Email routing
- Client Side Encryption (CSE)
- Meet Client Side Encryption (CSE)

Control Domain	System & Communications Protection		
Control #	**SC.L2-3.13.3**		
Control Description	Separate user functionality from system management functionality.		
Google Workspace Enabling Features	Admin Roles	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Identifying user functionality; b. Identifying system management functionality; and c. Separating user functionality from system management functionality. When configured correctly, the following feature(s) in Google Workspace may be used to support this control: • **Admin Roles** You can prevent non-privileged users from executing privileged functions by assigning users to the appropriate roles in Google Workspace. Please refer to AC.L2-3.1.4 for information on the Prebuilt Admin Roles and Custom Roles and how to assign roles.			
Supplemental Guidance			
• Prebuilt Admin Roles • Custom Roles			

Control Domain	System & Communications Protection
Control #	**SC.L2-3.13.8**
Control Description	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

Google Workspace Enabling Features	MTA-STS and TLS Secure transport (TLS) compliance S/MIME for message encryption	Control Responsibility	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Identifying cryptographic mechanisms intended to prevent unauthorized disclosure of CUI;
b. Implementing either cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission.

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **MTA-STS and TLS**
- **Secure transport (TLS) compliance**
- **S/MIME for message encryption**

A description of each feature and implementation guidance is included in SC.L1-3.13.1.

Additional Considerations

1. Customers can choose to enable MTA-STS to disable weak ciphers (SSL, 3DES, and RC4) on mail servers. When configuring MTA-STS, it is important for customers to take a responsible approach to minimize loss of email. It is recommended that the feature is enabled in testing mode and customers investigate MTA-STS reports prior to enabling enforcement mode.

Supplemental Guidance

- MTA-STS and TLS reporting
- Send email over an alternate secure route (TLS)
- Send email over a secure TLS connection
- S/MIME Encryption
- Advanced Email routing
- Client Side Encryption (CSE)
- Meet Client Side Encryption (CSE)

Control Domain	System & Communications Protection		
Control #	**SC.L2-3.13.9**		
Control Description	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.		
Google Workspace Enabling Features	Google Session Control	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			

Google Workspace Customers are responsible for:

a. Protecting the authenticity of communications sessions

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Google Session Control**

A description of each feature and implementation guidance is included below.

Google Session Control

As an administrator, you can control how long users can access Google services, such as Gmail on the web, without having to sign in again. For example, for users that work remotely or from untrusted locations, you might want to limit the time that they can access sensitive resources by applying a shorter web session length. If users want to continue accessing a resource when a session ends, they are prompted to sign in again and start a new session.

To set session durations:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the **Admin** console, go to **Menu** and then **Security** and then **Access and data control** and then **Google Session control**.
3. On the left, select the organizational unit where you want to set session length.
4. For all users, select the top-level organizational unit. Otherwise, select another organization to make settings for its users. Initially, an organization inherits the settings of its parent organization.
5. For **Session control**, under **Web session duration**, choose the length of time after which the user has to sign in again.
6. Click **Override** to keep the setting the same, even if the parent setting changes.
7. If the organizational unit's status is already **Overridden**, choose an option:
   Inherit—Reverts to the same setting as its parent

Save—Saves your new setting (even if the parent setting changes)

Additional Considerations

1. How the settings work on mobile devices varies by device and app. By default, the web session length for Google services is 14 days.
2. The session length for admins using the Google Admin console is set to one hour and cannot be modified. After an hour, admins need to sign in again. This length applies only to the Admin console. Other Google services have the session lengths they are respectively set to.

Supplemental Guidance

- Google Session Control

Control Domain	System & Communications Protection		
Control #	**SC.L2-3.13.12**		
Control Description	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.		
Google Workspace Enabling Features	Google Meet hardware (optional)	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Identifying collaborative computing devices;
b. Ensuring collaborative computing devices provide indication to users of devices in use; and
c. Prohibiting remote activation of collaborative computing devices.

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Google Meet hardware (optional)**

A description of each feature and implementation guidance is included below.

Google Meet hardware (optional)

If used, Google Meet hardware displays video meetings on large displays in standard-size or large rooms so groups of people can attend Meet video meetings together. Other participants can join from computers, mobile devices, or other video conferencing systems.

To use Meet hardware, you need a Google Workspace subscription for your organization and a Meet hardware license for each device.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. Google Meet hardware devices often have visual indicators to show their status. These can include LED lights to indicate when the device is in use or on-screen messages. No configuration is needed, though the specific indicators vary depending on the model of the Google Meet hardware. Please refer to your hardware manufacturer's documentation for details.
2. You can use the Google Admin console to remotely connect Google Meet hardware devices to meetings. This allows you to start meetings from your computer, even if you are not physically in the same room as the device. There is no setting that will disable this feature, therefore this should be prohibited via policy.

Supplemental Guidance

- Google Meet Hardware

Control Domain	System & Communications Protection		
Control #	**SC.L2-3.13.15**		
Control Description	Protect the authenticity of communications sessions.		
Google Workspace Enabling Features	DKIM Authentication	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Protecting the authenticity of communications sessions			

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **DKIM Authentication**

A description of each feature and implementation guidance is included below.

DKIM Authentication
As an administrator, you can set up DKIM (also called a DKIM signature) to authenticate your email and help protect your domain against spoofing. Without DKIM, messages sent from your organization or domain are more likely to be marked as spam by receiving mail servers.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. Sender Policy Framework (SPF) helps to prevent senders from impersonating you, blocking spammers and other attackers from sending email that appears to be from your organization. You should set up both SPF and DKIM. Simplified DKIM says you wrote the email. SPF says your server sent the email. So DKIM+SPF sends a stronger signal that the email came from you since you wrote it and sent it.
2. You do not need to do anything in your Google Admin console to set up SPF. Instead, determine your SPF record by following the instructions in the supplemental guidance. Then, log into your domain host and add the SPF record, following the domain host SPF instructions.

Supplemental Guidance

- DKIM Authentication
- Set up SPF

Control Domain	System & Information Integrity		
Control #	**SI.L2-3.14.3**		
Control Description	Monitor system security alerts and advisories and take action in response.		
Google Workspace Enabling Features	Alert Center	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			

Google Workspace Customers are responsible for:

a. Identifying response actions to system security alerts and advisories ;
b. Monitoring system security alerts and advisories; and
c. Taking action in response to system security alerts and advisories

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Alert Center**

A description of each feature and implementation guidance is included below.

Alert Center

The alert center includes two types of pages:

- A list of alerts affecting your domain—This page is displayed after you sign in to the Google Admin console and navigate to the alert center. This list can span several pages, depending on the number of alerts that are active.
- A details page that provides more information about each alert—You can access the details by clicking any item on the list of alerts.

To access the alert center:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the **Admin** console, go to **Menu** and then **Security** and then **Alert center**.

Additional Considerations

1. You should disseminate security alerts, advisories, and directives to established roles. You should implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.
2. You should report security incident information to designated authorities, including their Google support contacts, when a security incident is suspected.
3. You should periodically check the Google Workspace Status dashboard for service alerts.

Supplemental Guidance

- Alert Center
- Service Alerts

Control Domain	System & Information Integrity		
Control #	**SI.L2-3.14.6**		
Control Description	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.		
Google Workspace Enabling Features	Security Center Dashboard Apps Report	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Monitoring the system to detect attacks and indicators of potential attacks;
b. Monitoring inbound communications traffic to detect attacks and indicators of potential attacks; and
c. Monitoring outbound communications traffic to detect attacks and indicators of potential attacks.

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Security Center Dashboard**
- **Apps Report**

A description of each feature and implementation guidance is included below.

Security Center Dashboard
As an administrator, you can use the security dashboard to see an overview of different security reports. By default, each security report panel displays data from the last month. Some of the security reports include:

- User login attempts
- Suspicious attachments
- OAuth grant activity
- Suspicious device activities

You can use the dashboard to quickly view trends—for example, to see at a glance whether external file sharing has increased or decreased during a specific time period.

To view and use the dashboard:

1. Sign in with an administrator account to the **Google Admin** console.

2. In the **Admin** console, go to **Menu** and then **Security** and then **Security center** and then **Dashboard**.
3. To view more details about any of the reports, click **View Report** in the bottom-right corner of any panel.

Apps Report

As your organization's administrator, you can use Apps reports to review trends or see an overview of administrative information. The reports generate a series of charts and graphs that display information for all users in your domains. Each app has its own page and series of graphs. For example, the Apps Report for Gmail includes the following graphs:

- Total number of emails stored by all users in your domains
- Total number of inbound messages (delivered, rerouted, rejected) received by your users from senders outside your organization's associated domains
- Number of inbound messages tagged as spam, shown as a fraction of total inbound messages
- Number of inbound-encrypted messages, shown as a fraction of total inbound messages
- Number of outbound-delivered messages (delivered, rerouted, rejected), shown as a fraction of total outbound messages
- Number of outbound-Transport Layer Security (TLS)-encrypted messages, shown as a fraction of total outbound messages

To view Apps reports on your organization:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the **Admin** console, go to **Menu** and then **Reporting** and then **Apps Reporting** and then choose an app

You can also change the data you see in the chart, change the data you see in reports, and export your report data. Please refer to the supplemental guidance for more information.

Additional Considerations

1. Before you get started with these reports, you should familiarize yourself with the security dashboard and the reports by systematically going over each of the reports. As you view the reports, read the information in the Help Center instructions to better understand what the data is saying about your domain. Click each report, zoom in, and drill down to learn more about how the reports work, and to gain a better understanding of how the reports provide insights about your domain.

Supplemental Guidance

- Security Center Dashboard
- Apps Report

Control Domain	Systems & Information Integrity		
Control #	**SI.L2-3.14.7**		
Control Description	Identify unauthorized use of organizational systems.		
Google Workspace Enabling Features	Security Investigation Tool	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Defining authorized use of the system; and b. Identifying unauthorized use of the system. When configured correctly, the following feature(s) in Google Workspace may be used to support this control: • **Security Investigation Tool** A description of each feature and implementation guidance is included in IR.L2-3.6.1.			
Supplemental Guidance			
• Security Investigation Tool			

Controls Natively Implemented by Google Workspace

Control Domain	Access Control		
Control #	**AC.L2-3.1.13**		
Control Description	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			

Google Workspace is responsible for:

a. Identifying cryptographic mechanisms to protect the confidentiality of remote access sessions
b. Implementing cryptographic mechanisms to protect the confidentiality of remote access sessions

Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.

Supplemental Guidance

- N/A

Control Domain	**Access Control**		
Control #	**AC.L2-3.1.14**		
Control Description	Route remote access via managed access control points.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer

Customer Implementation Description

Google Workspace is responsible for:

a. Implementing managed access control points are identified and
b. Routing remote access through managed network access control points.

Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.

Supplemental Guidance

- N/A

Control Domain	Access Control		
Control #	**AC.L2-3.1.16**		
Control Description	Authorize wireless access prior to allowing such connections.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Identifying Wireless access points; and b. Authorizing Wireless access prior to allowing such connections. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	Access Control		
Control #	**AC.L2-3.1.17**		
Control Description	Protect wireless access using authentication and encryption.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. authenticating wireless access to the system; and b. protecting wireless access to the system using encryption.			

Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.
Supplemental Guidance
• N/A

Control Domain	**Audit & Accountability**		
Control #	**AU.L2-3.3.2**		
Control Description	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Defining the content of the audit records needed to support the ability to uniquely trace users to their actions is defined; and b. Ensuring audit records, once created, contain the defined content. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	**Audit & Accountability**

Control #	AU.L2-3.3.4		
Control Description	Alert in the event of an audit logging process failure.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Identifying personnel or roles to be alerted in the event of an audit logging process failure; b. Defining types of audit logging process failures for which alert will be generated; and c. Alerting the identified personnel or roles in the event of an audit logging process failure. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	Audit & Accountability		
Control #	**AU.L2-3.3.7**		
Control Description	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Using internal system clocks to generate time stamps for audit records;			

b. Specifying an authoritative source with which to compare and synchronize internal system clocks; and
c. Comparing and synchronizing internal system clocks used to generate time stamps for audit records with the specified authoritative time source.

Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.

Supplemental Guidance

- N/A

Control Domain	**Identification & Authentication**		
Control #	**IA.L2-3.5.4**		
Control Description	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer

Customer Implementation Description

Google Workspace is responsible for:

a. Implementing replay-resistant authentication mechanisms for network account access to privileged and non-privileged accounts.

Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.

Supplemental Guidance

- N/A

Control Domain	Identification & Authentication		
Control #	**IA.L2-3.5.10**		
Control Description	Store and transmit only cryptographically-protected passwords.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Cryptographically protecting passwords in storage; and b. Cryptographically protecting passwords in transit. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	Identification & Authentication		
Control #	**IA.L2-3.5.11**		
Control Description	Obscure feedback of authentication information.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Obscuring authentication information during the authentication process. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include*			

systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.
Supplemental Guidance
• N/A

Control Domain	**Maintenance**		
Control #	**MA.L2-3.7.1**		
Control Description	Perform maintenance on organizational systems.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Performing system maintenance. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	**Maintenance**		
Control #	**MA.L2-3.7.2**		
Control Description	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google

			☐ Shared ☐ Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Controlling tools used to conduct system maintenance; b. Controlling techniques used to conduct system maintenance; c. Controlling mechanisms used to conduct system maintenance; and d. Controlling personnel used to conduct system maintenance. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	**Maintenance**		
Control #	**MA.L2-3.7.3**		
Control Description	Ensure equipment removed for off-site maintenance is sanitized of any CUI.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	☒ Google ☐ Shared ☐ Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Sanitizing equipment to be removed from organizational spaces for off-site maintenance of any CUI. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			

Supplemental Guidance
• N/A

Control Domain	Maintenance		
Control #	**MA.L2-3.7.4**		
Control Description	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Checking media containing diagnostic and test programs for malicious code before being used in organizational systems that process, store, or transmit CUI. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control #	MA.L2-3.7.5		
Control Description	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared

			☐ Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Using multifactor authentication to establish nonlocal maintenance sessions via external network connections; and b. Terminating nonlocal maintenance sessions established via external network connections when nonlocal maintenance is complete. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	**Maintenance**		
Control #	**MA.L2-3.7.6**		
Control Description	Supervise the maintenance activities of maintenance personnel without required access authorization.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	☒ Google ☐ Shared ☐ Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Supervising maintenance personnel without required access authorization during maintenance activities. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			

- N/A

Control Domain	Media Protection		
Control #	**MP.L1-3.8.3**		
Control Description	Sanitize or destroy system media containing CUI before disposal or release for reuse.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Sanitizing system media containing CUI before disposal; and b. Sanitizing system media containing CUI before it is released for reuse. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	Media Protection		
Control #	**MP.L2-3.8.5**		
Control Description	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer

Customer Implementation Description			
Google Workspace is responsible for: a. Controlling access to media containing CUI; and b. Maintaining accountability for media containing CUI during transport outside of controlled areas. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	**Media Protection**		
Control #	**MP.L2-3.8.6**		
Control Description	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Protecting the confidentiality of CUI stored on digital media during transport using cryptographic mechanisms or alternative physical safeguards. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			

- N/A

Control Domain	Media Protection		
Control #	**MP.L2-3.8.7**		
Control Description	Control the use of removable media on system components.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Controlling the use of removable media on system components. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	Media Protection		
Control #	**MP.L2-3.8.8**		
Control Description	Prohibit the use of portable storage devices when such devices have no identifiable owner.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer

Customer Implementation Description
Google Workspace is responsible for: a. Prohibiting the use of portable storage devices is prohibited when such devices have no identifiable owner. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*
Supplemental Guidance
• N/A

Control Domain	Media Protection		
Control #	**MP.L2-3.8.9**		
Control Description	Protect the confidentiality of backup CUI at storage locations.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Protecting the confidentiality of backup CUI at storage locations. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	Physical Protection		
Control #	**PE.L1-3.10.1**		
Control Description	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Identifying authorized individuals allowed physical access; b. Limiting physical access to organizational systems to authorized individuals; c. Limiting physical access to equipment to authorized individuals; and d. Limiting physical access to operating environments to authorized individuals. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	Physical Protection		
Control #	**PE.L1-3.10.2**		
Control Description	Protect and monitor the physical facility and support infrastructure for organizational systems.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer

Control Domain	Physical Protection		
Control #	**PE.L1-3.10.3**		
Control Description	Escort visitors and monitor visitor activity.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Escorting visitors; and b. Monitoring visitor activity. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	Physical Protection		
Control #	**PE.L1-3.10.4**		
Control Description	Maintain audit logs of physical access.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Maintaining audit logs of physical access *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	Physical Protection		
Control #	**PE.L1-3.10.5**		
Control Description	Control and manage physical access devices.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Identifying physical access devices;			

b. Controlling physical access devices; and
c. Managing physical access devices.

Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.

Supplemental Guidance

- N/A

Control Domain	**Risk Assessment**		
Control #	**RA.L2-3.11.2**		
Control Description	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer

Customer Implementation Description

Google Workspace is responsible for:

a. Defining the frequency to scan for vulnerabilities in organizational systems and applications;
b. Performing vulnerability scans on organizational systems with the defined frequency;
c. Performing vulnerability scans on applications with the defined frequency;
d. Performing vulnerability scans on organizational systems when new vulnerabilities are identified; and
e. Performing vulnerability scans on applications when new vulnerabilities are identified.

Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.

Supplemental Guidance

- N/A

Control Domain	Risk Assessment		
Control #	**RA.L2-3.11.3**		
Control Description	Remediate vulnerabilities in accordance with risk assessments.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Identifying vulnerabilities; and b. Remediating vulnerabilities in accordance with risk assessments. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required. .*			
Supplemental Guidance			
• N/A			

Control Domain	System & Communications Protection		
Control #	**SC.L2-3.13.4**		
Control Description:	Prevent unauthorized and unintended information transfer via shared system resources.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			

Google Workspace is responsible for:

a. Preventing unauthorized and unintended information transfer via shared system resources

Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.

Supplemental Guidance

- N/A

Control Domain	**System & Communications Protection**		
Control #	**SC.L2-3.13.5**		
Control Description	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer

Customer Implementation Description

Google Workspace is responsible for:

a. Identifying publicly accessible system components; and

b. Physically or logically separating subnetworks for publicly accessible system components from internal networks.

Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.

Supplemental Guidance

- N/A

Control Domain	System & Communications Protection		
Control #	**SC.L2-3.13.6**		
Control Description	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Denying network communications traffic by default; and b. Allowing network communications traffic by exception. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	System & Communications Protection		
Control #	**SC.L2-3.13.7**		
Control Description	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			

Google Workspace is responsible for:

a. Preventing remote devices from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling).

Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.

Supplemental Guidance

- N/A

Control Domain	**System & Communications Protection**		
Control #	**SC.L2-3.13.10**		
Control Description	Establish and manage cryptographic keys for cryptography employed in organizational systems.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer

Customer Implementation Description

Google Workspace is responsible for:

a. Establishing cryptographic keys whenever cryptography is employed; and
b. Managing cryptographic keys whenever cryptography is employed

Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.

Additional Considerations

1. With Google Workspace Client-side encryption (CSE), you can add another layer of encryption to your organization's data—like files and emails—in addition to the default encryption that Google Workspace provides. CSE helps to keep your organization's data private with end-to-end encryption that Google servers and third parties can't decrypt, giving your organization greater control over access to its data. CSE is especially beneficial for organizations that store sensitive or regulated data, like

intellectual property, healthcare records, or financial data. Please refer to the supplemental guidance for additional information about this feature.
    a. If this feature is enabled, then this control may be in scope of your CUI boundary.
2. Additionally, with Meet Client-side Encryption (CSE), all media is encrypted by each participant's browser using keys only made available to the participants. Only the meeting participants can decrypt the call media while it remains unreadable to Google's servers or any other service provider. Please refer to the supplemental guidance for additional information about this feature.
    a. If this feature is enabled, then this control may be in scope of your CUI boundary.

Supplemental Guidance

- Client Side Encryption (CSE)
- Meet Client Side Encryption (CSE)

Control Domain	**System & Communications Protection**		
Control #	**SC.L2-3.13.11**		
Control Description	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer

Customer Implementation Description

Google Workspace is responsible for:
    a. Employing FIPS-validated cryptography to protect the confidentiality of CUI

Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.

Additional Considerations

1. With Google Workspace Client-side encryption (CSE), you can add another layer of encryption to your organization's data—like files and emails—in addition to the default

encryption that Google Workspace provides. CSE helps to keep your organization's data private with end-to-end encryption that Google servers and third parties can't decrypt, giving your organization greater control over access to its data. CSE is especially beneficial for organizations that store sensitive or regulated data, like intellectual property, healthcare records, or financial data. Please refer to the supplemental guidance for additional information about this feature.
    a. If this feature is enabled, then this control may be in scope of your CUI boundary.
2. Additionally, with Meet Client-side Encryption (CSE), all media is encrypted by each participant's browser using keys only made available to the participants. Only the meeting participants can decrypt the call media while it remains unreadable to Google's servers or any other service provider. Please refer to the supplemental guidance for additional information about this feature.
    a. If this feature is enabled, then this control may be in scope of your CUI boundary.

Supplemental Guidance

- Client Side Encryption (CSE)
- Meet Client Side Encryption (CSE)

Control Domain	**System & Communications Protection**		
Control #	**SC.L2-3.13.13**		
Control Description	Control and monitor the use of mobile code.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer

Customer Implementation Description

Google Workspace is responsible for:
a. Controlling the use of mobile code; and
b. Monitoring the use of mobile code.

Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include

systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.
Supplemental Guidance
• N/A

Control Domain	System & Communications Protection		
Control #	**SC.L2-3.13.14**		
Control Description	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			

Google Workspace is responsible for:

a. Controlling use of Voice over Internet Protocol (VoIP) technologies; and
b. Monitoring use of Voice over Internet Protocol (VoIP) technologies.

Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.

Additional Considerations

1. Google Voice is an add-on service that is compatible with Google Workspace. If used, Google Voice traffic is secured and encrypted, so there's no need to restrict traffic to the Google IPs. You can monitor Voice usage in the Apps Report page, including:
    a. Total active users
    b. Total licensed users
    c. Total call duration
    d. Total outbound calls
    e. Total inbound calls
    f. Total calls
    g. Total outbound messages
    h. Total inbound messages
    i. Total messages

2. Please refer to supplemental guidance for additional information about this service and how it is managed in Google Workspace.
Supplemental Guidance
• Google Voice

Control Domain	System & Communications Protection		
Control #	**SC.L2-3.13.16**		
Control Description	Protect the confidentiality of CUI at rest.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Protecting the confidentiality of CUI at rest *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	System & Information Integrity		
Control #	**SI.L1-3.14.1**		
Control Description	Identify, report, and correct system flaws in a timely manner.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer

Customer Implementation Description
Google Workspace is responsible for: a. Specifying the time within which to identify system flaws; b. Identifying system flaws within the specified time frame; c. Specifying the time within which to report system flaws; d. Reporting system flaws within the specified time frame; e. Specifying the time within which to correct system flaws; and f. Correcting system flaws within the specified time frame. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.* **Additional Considerations** 1. You can contact Google Workspace support for additional help from a specialist or to report an issue. Make sure you include the following information: a. A description of the problem, and the behavior you expected instead. b. A list of steps and a small snippet of sample code that can be used to reproduce the problem. c. A description of the output you expect and what actually occurred. Include any error messages you receive. d. Information about your development environment, including programming language, library versions, etc. 2. Additionally, Google has a Bug Hunter program that you can use to report security vulnerabilities to Google's vulnerability reward program (VRP). Please refer to the supplemental guidance for additional information.
Supplemental Guidance
• Google Workspace Support • Google Bug Hunters

Control Domain	System & Information Integrity		
Control #	**SI.L1-3.14.2**		
Control Description	Provide protection from malicious code at designated locations within organizational systems.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google

			☐ Shared ☐ Customer

Customer Implementation Description

Google Workspace is responsible for:

a. Identifying designated locations for malicious code protection; and
b. Providing protection from malicious code at designated locations.

Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.

Additional Considerations

1. Google scans all messages to protect against malware, whether or not attachment security settings are turned on. However, you can enforce extra, specific actions for certain types of files with the Advanced Security Settings. These settings protect against senders with no prior Gmail history or with a low sender reputation. Please refer to the supplemental guidance for additional information.
2. Attachments in Gmail messages you send and receive are automatically scanned for viruses. However, you can also set up rules to detect harmful attachments in Google Security Sandbox. Security Sandbox scans files directly attached to messages and files inside archive attachments, for example zip or rar files. Supported attachment types in Security Sandbox include Microsoft executables (.exe), Microsoft Office, and PDF. Security Sandbox scanning can delay message delivery by up to 3 minutes, although scans might be completed in less time. Customers interested in using this feature can use the link in the supplemental guidance for more information.
3. Additionally, as an administrator, you can increase Gmail's ability to identify suspicious content with enhanced pre-delivery message scanning. Typically, when Gmail identifies a possible phishing message, a warning is displayed and the message might be moved to spam. With the Enhanced pre-delivery message scanning option, when Gmail detects suspicious content, message delivery is slightly delayed so that Gmail can do additional security checks on the message. Please refer to the supplemental guidance for additional information.

Supplemental Guidance

- Advanced Security Settings
- Security Sandbox
- Pre-delivery message scanning

Control Domain	System & Information Integrity		
Control #	**SI.L1-3.14.4**		
Control Description	Update malicious code protection mechanisms when new releases are available.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Updating malicious code protection mechanisms when new releases are available. *Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.*			
Supplemental Guidance			
• N/A			

Control Domain	System & Information Integrity		
Control #	**SI.L1-3.14.5**		
Control Description	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			
Google Workspace is responsible for: a. Defining the frequency for malicious code scans; b. Performing malicious code scans with the defined frequency; and			

c. Performing real-time malicious code scans of files from external sources as files are downloaded, opened, or executed.

Based on the scope of this implementation guide, you do not need to configure any Google Workspace features to implement this control. Please note your CUI Boundary may include systems, applications, facilities, or tools outside of Google Workspace, therefore, additional control implementation responsibility may be required.

Supplemental Guidance

- N/A

Controls Requiring Implementation outside of Google Workspace

Control Domain	**Access Control**		
Control #	**AC.L2-3.1.9**		
Control Description	Provide privacy and security notices consistent with applicable CUI rules.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer

Customer Implementation Description

Google Workspace Customers are responsible for:

a. Identifying privacy and security notices required by CUI-specified rules consistent with the specific CUI category; and
b. Displaying privacy and security notices

Google Workspace does not natively offer any features that, if configured, will address this control. Google Workspace is compatible with many third party authentication services. You should consider using your SSO solution to display your approved system use notification and ensuring all Google login pages are configured to point to your SSO portal using SSO Profiles.

Additional Considerations

1. If using your own SSO solution to implement a privacy notice, you will need to set up SSO Profiles to access Google Workspace services. Google Workspace supports SSO

from third-party identity providers (IdPs). Please refer to AC.L1-3.1.1 for more details about this service.
Supplemental Guidance
• N/A

Control Domain	**Access Control**		
Control #	**AC.L2-3.1.10**		
Control Description	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Defining the period of inactivity after which the system initiates a session lock b. Preventing access to the system and viewing of data by initiating a session lock after the defined period of inactivity c. Concealing previously visible information via a pattern-hiding display after the defined period of inactivity *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should consider configuring your authorized endpoints with access to Google Workspace to use a session lock with pattern-hiding displays to prevent access and viewing of data after a defined period of inactivity.*			
Supplemental Guidance			
• N/A			

Control Domain	Access Control		
Control #	**AC.L2-3.1.21**		
Control Description	Limit use of organizational portable storage devices on external systems.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[ ] Google [ ] Shared [X] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Identifying and documenting the use of portable storage devices containing CUI on external systems; b. Defining the use of portable storage devices containing CUI on external systems; and c. Limiting the use of portable storage devices containing CUI on external systems is limited as defined. *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*			
Supplemental Guidance			
• N/A			

Control Domain	Awareness & Training		
Control #	**AT.L2-3.2.1**		
Control Description	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description
Google Workspace Customers are responsible for: a. Identifying security risks associated with organizational activities involving CUI; b. Identifying policies, standards, and procedures related to the security of the system; c. Informing managers, systems administrators, and users of the system of the security risks associated with their activities; and d. Informing managers, systems administrators, and users of the system of the applicable policies, standards, and procedures related to the security of the system. *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*
Supplemental Guidance
• N/A

Control Domain	**Awareness & Training**		
Control #	**AT.L2-3.2.2**		
Control Description	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Defining information security-related duties, roles, and responsibilities; b. Assigning information security-related duties, roles, and responsibilities to designated personnel; and c. Adequately training personnel to carry out their assigned information security related duties, roles, and responsibilities. *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*			

Supplemental Guidance
• N/A

Control Domain	Awareness & Training		
Control #	**AT.L2-3.2.3**		
Control Description	Provide security awareness training on recognizing and reporting potential indicators of insider threat.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Identifying potential indicators associated with insider threats; and b. Providing security awareness training on recognizing and reporting potential indicators of insider threat to managers and employees. *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*			
Supplemental Guidance			
• N/A			

Control Domain	Configuration Management		
Control #	**CM.L2-3.4.4**		
Control Description	Analyze the security impact of changes prior to implementation.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			

Google Workspace Customers are responsible for: a. Analyze the security impact of changes to the system prior to implementation *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*
Supplemental Guidance
• N/A

Control Domain	**Identification & Authentication**		
Control #	**IA.L2-3.5.5**		
Control Description	Prevent reuse of identifiers for a defined period.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Defining a period within which identifiers cannot be reused; and b. Preventing the reuse of identifiers within the defined period. *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*			
Supplemental Guidance			
• N/A			

Control Domain	**Incident Response**
Control #	**IR.L2-3.6.2**
Control Description	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

Google Workspace Enabling Features	N/A	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Tracking incidents; b. Documenting incidents; c. Identifying authorities to whom incidents are to be reported; d. Identifying organizational officials to whom incidents are to be reported; e. Notifying the identified authorities of incidents; and f. Notifying the identified organizational officials of incidents. *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*			
Supplemental Guidance			
• N/A			

Control Domain	**Incident Response**		
Control #	**IR.L2-3.6.3**		
Control Description	Test the organizational incident response capability		
Google Workspace Enabling Features	N/A	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Testing the incident response capability *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*			

Supplemental Guidance
• N/A

Control Domain	Media Protection		
Control #	**MP.L2-3.8.1**		
Control Description	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Physically controlling paper media containing CUI; b. Physically controlling digital media containing CUI; c. Securely storing paper media containing CUI; and d. Securely storing digital media containing CUI. *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*			
Supplemental Guidance			
• N/A			

Control Domain	Media Protection		
Control #	**MP.L2-3.8.2**		
Control Description	Limit access to CUI on system media to authorized users.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer

Customer Implementation Description
Google Workspace Customers are responsible for: a. Limiting access to CUI on system media to authorized users. *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*
Supplemental Guidance
• N/A

Control Domain	Media Protection		
Control #	**MP.L2-3.8.4**		
Control Description	Mark media with necessary CUI markings and distribution limitations.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Marking media containing CUI with applicable CUI markings; and b. Marking media containing CUI with distribution limitations. *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*			
Supplemental Guidance			
• N/A			

Control Domain	Personnel Security
Control #	**PS.L2-3.9.1**

Control Description	Screen individuals prior to authorizing access to organizational systems containing CUI.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[ ] Google [x] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Screening individuals prior to authorizing access to organizational systems containing CUI. *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*			
Supplemental Guidance			
• N/A			

Control Domain	**Physical Protection**		
Control #	**PE.L2-3.10.6**		
Control Description	Enforce safeguarding measures for CUI at alternate work sites.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Defining safeguarding measures for CUI for alternate work sites; and b. Enforcing safeguarding measures for CUI for alternate work sites *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*			

Supplemental Guidance
• N/A

Control Domain	Risk Assessment		
Control #	**RA.L2-3.11.1**		
Control Description	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Defining the frequency to assess risk to organizational operations, organizational assets, and individuals; and b. Assessing risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI with the defined frequency. *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*			
Supplemental Guidance			
• N/A			

Control Domain	Security Assessment
Control #	**CA.L2-3.12.1**
Control Description	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

Google Workspace Enabling Features	N/A	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Defining the frequency of security control assessments; and b. Assessing security controls with the defined frequency to determine if the controls are effective in their application. *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*			
Supplemental Guidance			
• N/A			

Control Domain	**Security Assessment**		
Control #	**CA.L2-3.12.2**		
Control Description	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	[ ] Google [X] Shared [ ] Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Identifying deficiencies and vulnerabilities to be addressed by the plan of action; b. Developing a plan of action to correct the identified deficiencies and reduce or eliminate identified vulnerabilities; and c. Implementing the plan of action to correct the identified deficiencies and reduce or eliminate identified vulnerabilities.			

Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.
Supplemental Guidance
• N/A

Control Domain	Security Assessment		
Control #	**CA.L2-3.12.3**		
Control Description	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.		
Google Workspace Enabling Features	N/A	**Control Responsibility**	☐ Google ☒ Shared ☐ Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Monitoring security controls on an ongoing basis to ensure the continued effectiveness of those controls. *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*			
Supplemental Guidance			
• N/A			

Control Domain	Security Assessment
Control #	**CA.L2-3.12.4**
Control Description	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Google Workspace Enabling Features	N/A	**Control Responsibility**	☐ Google ☒ Shared ☐ Customer
Customer Implementation Description			
Google Workspace Customers are responsible for: a. Developing a system security plan; b. Describing and documenting the system boundary in the system security plan; c. Describing and documenting the system environment of operation in the system security plan; d. Identifying the security requirements identified and approved by the designated authority as non-applicable; e. Describing and documenting the method of security requirement implementation in the system security plan; f. Describing and documenting the relationship with or connection to other systems in the system security plan; g. Defining the frequency to update the system security plan; and h. Updating the system security plan with the defined frequency. *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*			
Supplemental Guidance			
• N/A			

Control Domain	**System & Communications Protection**		
Control #	**SC.L2-3.13.2**		
Control Description	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.		
Google Workspace Enabling Features	N/A	Control Responsibility	☐ Google ☒ Shared ☐ Customer

Customer Implementation Description
Google Workspace Customers are responsible for: a. Identifying architectural designs that promote effective information security; b. Identifying software development techniques that promote effective information security; c. Identifying systems engineering principles that promote effective information security; d. Employing identified architectural designs that promote effective information security; e. Employing identified software development techniques that promote effective information f. security; and g. Employing identified systems engineering principles that promote effective information security. *Google Workspace does not natively offer any features that, if configured correctly, will address this control. You should implement this control outside of Google Workspace, in accordance with your CUI boundary.*
Supplemental Guidance
• N/A

Appendix

Chrome Browser & Chrome OS

This Appendix provides additional features which may be used to secure your CUI boundary on Chrome Browsers, ChromeOS endpoints, iOS, and Android devices. Please refer to links in the supplemental guidance to learn more about each feature, including which devices or endpoints the feature can be applied.

Most of the features listed below require Chrome Enterprise or Chrome Enterprise Premium. These licenses must be purchased separately from Workspace Enterprise.

Control Domain	Access Control
Control #	**AC.L1-3.1.1**
Control Description	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

Google Workspace Enabling Features	SAML SSO for ChromeOS devices SAML SSO for Chrome apps Chrome Policy: Guest Mode Managed Guest Sessions Context Aware Access	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer

Customer Implementation Description

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **SAML SSO for ChromeOS devices**
- **SAML SSO for Chrome apps**
- **Chrome Policy: Disable Guest Mode**
- **Managed Guest Sessions**
- **Context Aware Access**

A description of each feature and implementation guidance is included below.

SAML SSO for ChromeOS devices
Security Assertion Markup Language (SAML) single sign-on (SSO) support for ChromeOS devices allows users to sign in to a device with the same authentication mechanisms that you use within the rest of your organization. Their passwords can remain within your organization's Identity Provider (IdP). Signing in is very similar to signing in to a Google Workspace account from a browser via SAML SSO. However, because a user is signing in to a device, there are several additional considerations.

Additionally, you can choose to sync ChromeOS device local passwords with users' SAML SSO passwords. By default, the local password is updated every time users sign in online. You can configure how often users are required to sign in online using the SAML single sign-on login frequency or SAML single sign-on unlock frequency settings. However, some users might change their SAML SSO password before they are required to sign in online again. If that happens, users continue to use their old local ChromeOS password until the next time they sign in online. To keep the local ChromeOS password in sync with their SAML SSO password, you can force them to sign in online as soon as their SAML SSO password changes. That way, they update their ChromeOS password almost immediately.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

SAML SSO for Chrome apps

You can use the SAML SSO for Chrome Apps extension when you need to configure SAML SSO for Chrome apps. Users can sign in to a Chrome app with the same authentication mechanisms that you use within the rest of your organization. Their passwords can remain within your organization's IdP.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Chrome Policy: Guest Mode
Guest mode is a feature in Chrome that allows someone to use your Chromebook without signing in to a Google account. Controls guest browsing on managed ChromeOS devices. If you select Allow guest mode, the main sign-in screen offers the option for a user to sign in as a guest. If you select Disable guest mode, a user must sign in using a Google Account or Google Workspace account. When a user signs in using guest mode, your organization's policies are not applied.

To disable this feature:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the Admin console, go to **Menu** and then **Devices** and then **Chrome** and then **Settings** and then **Device settings.**
3. (Optional) To apply the setting only to some users and enrolled browsers, at the side, select an organizational unit (often used for departments) or configuration group (advanced).
4. Click **Guest mode** under Sign-in Settings.
5. Next to configuration, select **Disable guest mode.**
6. Click **Save.**

Managed Guest Sessions
With managed guest sessions, multiple users can share the same device running Chrome OS without having to sign in to their Google Account. For example, use managed guest sessions to configure Chrome devices as loaner devices or shared computers. Before a device can host managed guest sessions, you must enroll the devices that you want to let users run managed guest sessions and place devices that users will use to run managed guest sessions in an organizational unit.

To disable Managed Guest Sessions in Chrome devices:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the Admin console, go to **Menu** and then **Devices** and then **Chrome** and then **Settings** and then **Managed guest sessions**.
3. To apply the setting to everyone, leave the top organizational unit selected. Otherwise, select a child organizational unit.
4. Next to configuration, choose **Do not allow managed guest sessions**
5. Click **Save**.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Context Aware Access
Context-Aware Access gives you control over which apps a user can access based on their context (e.g., whether their device complies with your IT policy.) Using Context-Aware Access, you can create granular access control policies to authenticate devices. For example, you can create a policy that only if a device has a serial number that matches one that's in the company's asset management system, or if a device has a valid enterprise certificate that is issued by the company, then the device may access Google Workspace data.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Supplemental Guidance

- SAML SSO for ChromeOS devices
- SAML SSO for Chrome apps
- Chrome Policy: Guest Mode
- Managed Guest Sessions
- Context Aware Access

Control Domain	Access Control		
Control #	**AC.L1-3.1.2**		
Control Description	Limit system access to the types of transactions and functions that authorized users are permitted to execute.		
Google Workspace Enabling Features	Admin Roles ChromeOS Policies Chrome Policies	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer
Customer Implementation Description			
When configured correctly, the following feature(s) in Google Workspace may be used to support this control: • **Admin Roles**			

- **ChromeOS Policies**
- **Chrome Policies**

A description of each feature and implementation guidance is included below.

Admin Roles
When you specify privileges in the Admin Console, you can also grant corresponding Chrome Management privileges. For example, if a role is assigned the Chrome Management, then admins can manage your organization's Chrome devices and policies, including:

- User settings
- Device settings
- Chrome and Managed Google Play apps and extensions on Chrome devices

Customers interested in using this feature can use the link in the supplemental guidance for more information.

ChromeOS Policies
As a Chrome Enterprise admin, you can manage policies and settings for Chromebooks and other devices that run ChromeOS from the cloud-based Google Admin console. You should use the policies and settings to determine what functions and features in the Chrome OS or Chrome Browser that you want users to access.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Chrome Policies
As an IT admin for a business or school, you can deploy Chrome browser to users across Microsoft Windows, Apple Mac, and Linux computers. You can then manage 200+ policies that govern their use of Chrome browser, such as the apps and extensions they can use, data security and privacy, their browsing experience, and more.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Supplemental Guidance

- Admin Roles
- ChromeOS Policies
- Chrome Policies

Control Domain	Access Control		
Control #	**AC.L2-3.1.3**		
Control Description	Control the flow of CUI in accordance with approved authorizations.		
Google Workspace Enabling Features	DLP with Chrome	**Control Responsibility**	[ ] Google [ ] Shared [X] Customer
Customer Implementation Description			
When configured correctly, the following feature(s) in Google Workspace may be used to support this control: • **DLP with Chrome** A description of each feature and implementation guidance is included below. **DLP with Chrome** Using Chrome Enterprise Premium threat and data protection, you can integrate Data Loss Prevention (DLP) features to use with Chrome to implement sensitive data detection for files that are uploaded and downloaded and for content that is pasted or dragged and dropped. The DLP integration with Chrome scans and reports findings from up to 10MB of the text content extracted from each file. ***Note: Chrome Enterprise Premium threat and data protection features are available only for customers who have purchased Chrome Enterprise Premium*** *Customers interested in using this feature can use the link in the supplemental guidance for more information.*			
Supplemental Guidance			
• DLP with Chrome			

Control Domain	Access Control
Control #	**AC.L2-3.1.9**
Control Description	Provide privacy and security notices consistent with applicable CUI rules.

Google Workspace Enabling Features	Chrome Policy: Custom Terms of Service	Control Responsibility	[ ] Google [ ] Shared [X] Customer
Customer Implementation Description			
When configured correctly, the following feature(s) in Google Workspace may be used to support this control: • **Chrome Policy: Custom Terms of Service** A description of each feature and implementation guidance is included below. **Chrome Policy: Custom Terms of Service** You can upload a custom privacy or security notice that users must accept before they can sign in to start a session. *Customers interested in using this feature can use the link in the supplemental guidance for more information.* **Additional Considerations:** • Only available on ChromeOS devices.			
Supplemental Guidance			
• Chrome Policy: Custom Term of Service			

Control Domain	Access Control		
Control #	**AC.L2-3.1.10**		
Control Description	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.		
Google Workspace Enabling Features	Chrome Policy: Browser Idle Timeout Chrome Policy: Idle Settings	**Control Responsibility**	[ ] Google [ ] Shared [X] Customer
Customer Implementation Description			

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Chrome Policy: Browser Idle Timeout**
- **Chrome Policy: Idle Settings**

A description of each feature and implementation guidance is included below.

Chrome Policy: Browser Idle Timeout
You can select what actions the browser performs when idle for a specified period of time. This feature is available on iOS devices and Chrome browser for Windows, Mac, and Linux.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Chrome Policy: Idle Settings
This Chrome Policy controls actions performed when the user closes the Chromebook lid or when the AC/Battery is idle.

To configure the idle settings:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the Admin console, go to **Menu** and then **Devices** and then **Chrome** and then **Settings**.
    a. If you signed up for Chrome Enterprise Core, go to **Menu** and then **Chrome browser** and then **Settings**.
3. (Optional) To apply the setting only to some users and enrolled browsers, at the side, select an organizational unit (often used for departments) or configuration group (advanced).
4. Click Idle Settings
    a. Select if you want a user's device to go to sleep, sign them out, shut down, or do nothing, when they idle when connected to AC power or battery power. The default is Sleep.
    b. Select if you want a user's device to go to sleep, sign them out, shut down, or do nothing, when they close the device lid. The default for user sessions is Sleep and the default for managed guest sessions is Logout.
5. Click **Save**. Or, you might click **Override** for an organizational unit .

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Supplemental Guidance

- Chrome Policy: Browser Idle Timeout
- Chrome Policy: Idle Settings

Control Domain	Access Control		
Control #	**AC.L2-3.1.11**		
Control Description	Terminate (automatically) a user session after a defined condition.		
Google Workspace Enabling Features	Chrome Policy: Maximum user session length	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer
Customer Implementation Description			
When configured correctly, the following feature(s) in Google Workspace may be used to support this control: • **Chrome Policy: Maximum user session length** A description of each feature and implementation guidance is included below. **Maximum user session length** This Chrome Policy controls how long user sessions last. The remaining session time is shown on a countdown timer in the user's system tray. After the specified time, users are automatically signed out and the session ends. Enter a value between 1 and 1440 minutes (24 hours). For unlimited sessions, do not enter a value. *Customers interested in using this feature can use the link in the supplemental guidance for more information.*			
Supplemental Guidance			
• Chrome Policy: Maximum user session length			

Control Domain	Access Control		
Control #	**AC.L2-3.1.12**		
Control Description	Monitor and control remote access sessions.		
Google Workspace Enabling Features	Chrome Remote Desktop ChromeOS Remote Access	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer

Customer Implementation Description

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:
• **Chrome Remote Desktop**
• **ChromeOS Remote Access**
 	
A description of each feature and implementation guidance is included below.
 	
Chrome Remote Desktop
Chrome Remote Desktop allows your users to use a computer or mobile device to access files and applications on another computer with Chrome Remote Desktop. As an administrator, you can control whether users can use Chrome Remote Desktop.
 	
1. Sign in with an administrator account to the **Google Admin** console.
2. In the **Admin** console, go to **Menu** and then **Apps** and then **Additional Google services**.
3. Click **Chrome Remote Desktop**.
4. Click **Service status**.
5. To turn a service on or off for everyone in your organization, click **On for everyone** or **Off for everyone**, and then click **Save**.
6. To change the Service status, select **On** or **Off**.
7. Choose one:
  • If the Service status is set to Inherited and you want to keep the updated setting, even if the parent setting changes, click **Override**.
  • If the Service status is set to Overridden, either click Inherit to revert to the same setting as its parent, or click Save to keep the new setting, even if the parent setting changes.
 	
ChromeOS Remote Access
As a Chrome Enterprise administrator, you can remotely access and troubleshoot ChromeOS devices, including kiosk devices, by starting a Chrome Remote Desktop session from the Google Admin console. All remote connection sessions are logged in the Admin audit log under ChromeOS Device Command.
 	
Customers interested in using this feature can use the link in the supplemental guidance for more information.

Supplemental Guidance
• Chrome Remote Desktop • ChromeOS Remote Access

Control Domain	Access Control		
Control #	**AC.L2-3.1.15**		
Control Description	Authorize remote execution of privileged commands and remote access to security-relevant information.		
Google Workspace Enabling Features	Admin Roles	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer
Customer Implementation Description			
When configured correctly, the following feature(s) in Google Workspace may be used to support this control: • **Admin Roles** A description of each feature and implementation guidance is included below. **Admin Roles** When you specify privileges in the Admin Console, you can also grant remote access to managed ChromeOS devices. For example, if a role is assigned the Chrome Management privileges, then users with this role can manage your organization's Chrome devices and policies, including: • Start Remote Desktop *Customers interested in using this feature can use the link in the supplemental guidance for more information.*			
Supplemental Guidance			
• Admin Roles			

Control Domain	Access Control		
Control #	**AC.L2-3.1.16**		
Control Description	Authorize wireless access prior to allowing such connections.		
Google Workspace Enabling Features	Device Networks	**Control Responsibility**	☐ Google ☐ Shared

			[X] Customer
Customer Implementation Description			
When configured correctly, the following feature(s) in Google Workspace may be used to support this control: • **Device Networks** A description of each feature and implementation guidance is included below. **Device Networks** As an administrator, you can automatically add configured Wi-Fi networks to company-managed mobile and ChromeOS devices. However, you will still need to configure and manage the Wi-Fi network outside of Google Workspace. *Customers interested in using this feature can use the link in the supplemental guidance for more information.*			
Supplemental Guidance			
• Device Networks			

Control Domain	**Access Control**		
Control #	**AC.L2-3.1.17**		
Control Description	Protect wireless access using authentication and encryption.		
Google Workspace Enabling Features	Device Networks	**Control Responsibility**	[ ] Google [ ] Shared [X] Customer
Customer Implementation Description			
When configured correctly, the following feature(s) in Google Workspace may be used to support this control: • **Device Networks** A description of each feature and implementation guidance is included below. **Device Networks**			

As an administrator, you can automatically add configured Wi-Fi networks to company-managed mobile and ChromeOS devices. However, you will still need to configure and manage the Wi-Fi network outside of Google Workspace. *Customers interested in using this feature can use the link in the supplemental guidance for more information.*
Supplemental Guidance
• Device Networks

Control Domain	**Access Control**		
Control #	**AC.L1-3.1.20**		
Control Description	Verify and control/limit connections to and use of external systems.		
Google Workspace Enabling Features	Chrome URL Blocklist or Allowlist Chrome Enterprise Connectors Framework	**Control Responsibility**	[ ] Google [ ] Shared [X] Customer
Customer Implementation Description			

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Chrome URL Blocklist or Allowlist**
- **Chrome Enterprise Connectors Framework**
- **Local and Network Printers**

A description of each feature and implementation guidance is included below.

Chrome URL Blocklist or Allowlist
As a Chrome Enterprise admin, you can block and allow URLs so that users can only visit certain websites. Restricting users' internet access can increase productivity and protect your organization from viruses and malicious content found on some websites.

To configure a URL Blocklist or Allowlist:

1. In the **Admin** console, go to **Menu** and then **Devices** and then **Chrome** and then **Settings**.
    a. If you signed up for Chrome Enterprise Core, go to **Menu** and then **Chrome browser** and then **Settings**.

2. (Optional) To apply the setting only to some users and enrolled browsers, at the side, select an organizational unit (often used for departments) or configuration group.
3. Go to **Content**.
4. Click **URL Blocking** and enter URLs as needed:
    a. **Blocked URLs**—URLs that you want to prevent users from accessing.
    b. **Blocked URL exceptions**—URLs that you want to allow users to access (allowlist). **Access is allowed even if the URLs are also defined in Blocked URLs.**
5. You can block and allow up to 1,000 URLs.
6. Click **Save**.

Chrome Enterprise Connectors Framework
Chrome Enterprise Connectors Framework offers a collection of connectors and APIs that simplify the steps needed to integrate Chrome browser and ChromeOS with solution providers. As an admin, you can use the Google Admin console to get Chrome to report events to third-party service providers. For example, you can configure Chrome to report security events such as malware transfer, unsafe site visits, and password reuse. You can let Chrome report events using multiple service providers and configurations at the same time.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Local and Network Printers
As an administrator, you can use Common UNIX Printing System (CUPS) printers with your organization's ChromeOS devices. CUPS uses an Internet Printing Protocol (IPP) to print to local and network printers. You can also track print jobs and printer usage in your organization. You can add and specify a printer for everyone, or for users or devices in certain groups or departments.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. Alternatively, you can use Google Workspace to configure the networks that company-managed mobile devices, ChromeOS devices, and Google meeting room hardware use. You can control Wi-Fi, Ethernet, and Virtual Private Network (VPN) access, and set up network certificates. When you add a network configuration, you can apply the same network settings for your entire organization, or enforce specific network settings for different organizational units. Customers interested in using this feature can use the link in the supplemental guidance for more information.

Supplemental Guidance

- Chrome URL Blocklist or Allowlist
- Chrome Enterprise Connectors Framework
- Network Management
- Local and Network Printers

Control Domain	Audit & Accountability		
Control #	**AU.L2-3.3.1**		
Control Description	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.		
Google Workspace Enabling Features	Chrome browsers log events Chrome log events Chrome Sync log events Chrome Management Telemetry API	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer
Customer Implementation Description			

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Chrome browsers log events**
- **Chrome log events**
- **Chrome Sync log events**
- **Chrome Management Telemetry API**

A description of each feature and implementation guidance is included below.

Chrome browsers log events
As an administrator, you can use the security investigation tool to view and investigate live-state data about Chrome browsers in your organization. For example:

- Investigate if a browser update has reached all devices in your organization.
- Inspect the details of browser devices where phishing events often occur. The report can help identify if a bad extension is responsible for the unsafe events.
- View which devices have a specific user signed in, and assess the potential damage made to different devices and browsers.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Chrome log events
As your organization's administrator, you can run searches and take action on security issues related to Chrome log events in Google Workspace. For example, you can view a record of actions to track events related to managed Chrome browsers and ChromeOS devices. You can also see when there has been an unsafe site visit.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Chrome Sync log events
As your organization's administrator, you can run searches and take action on security issues related to Chrome Sync log events in Google Workspace. You can view a record of actions taken by users who have Chrome Sync enabled—for example, if a user deleted a bookmark, installed a new Chrome extension, or logged into Chrome on a new device.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Chrome Management Telemetry API
As a Chrome administrator, you can use the Chrome Telemetry API to monitor the operation and health of Chrome OS devices, including:

- CPU information and telemetry

- Memory information and telemetry
- Graphics information and telemetry
- Battery information and telemetry
- Storage information and telemetry
- Network information
- OS update status

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Supplemental Guidance

- Chrome browsers log events
- Chrome log events
- Chrome Sync log events
- Chrome Management Telemetry API

Control Domain	Audit & Accountability		
Control #	**AU.L2-3.3.4**		
Control Description	Alert in the event of an audit logging process failure.		
Google Workspace Enabling Features	Security Investigation Tool Chrome Management Telemetry API notifications	**Control Responsibility**	[ ] Google [ ] Shared [X] Customer

Customer Implementation Description

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Security investigation tool**
- **Chrome Management Telemetry API notifications**

A description of each feature and implementation guidance is included below.

Security Investigation Tool
As an administrator, you can create an activity rule that alerts you or takes action based on any search that you configure in the investigation tool. After you configure the activity rule,

Google will continuously perform a search that you have specified in the rule. If the number of results returned by that search exceeds the threshold that you have set up, then Google will perform the actions that you specify. For example, you can set up a rule to send email notifications to certain administrators if Drive documents are shared outside the company.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Chrome Management Telemetry API notifications
As a Chrome administrator, you can use the Chrome Telemetry API to monitor the operation and health of ChromeOS devices, helping you with root cause analysis and troubleshooting. Using Chrome Management Telemetry API notifications, you can subscribe to and receive Telemetry API event notifications using Google Cloud Pub/Sub.

Using Google Cloud Pub/Sub, you can create a system of event producers and consumers, called publishers and subscribers. This system streams analytics and data integration pipelines to receive and distribute data. Publishers communicate with subscribers asynchronously by broadcasting events. You can create notifications when the Chrome Management Telemetry API stops sending event notifications.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

- Chrome Management Telemetry API notifications requires a Google Cloud Platform (GCP) account

Supplemental Guidance

- Security Investigation Tool
- Chrome Management Telemetry API notifications

Control Domain	Audit & Accountability
Control #	AU.L2-3.3.5
Control Description	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

Google Workspace Enabling Features	Device Reports Chrome Browser and Profile reporting Chrome Insights report Chrome Enterprise reporting connectors	Control Responsibility	[ ] Google [ ] Shared [X] Customer

Customer Implementation Description

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Device Reports**
- **Chrome Browser and Profile reporting**
- **Chrome Insights report**
- **Chrome Enterprise reporting connectors**

A description of each feature and implementation guidance is included below.

Device Reports
As your organization's administrator, you can use device reports to see trends or an overview of information about devices running Chrome OS and mobile devices that are used in your organization. You can also change the data you see in reports and export your report data.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Chrome Browser and Profile reporting
As an administrator, you can view reports in the Google Admin console to review managed Chrome browser and profile information in your organization. You can turn on managed browser reporting to get a detailed view of Chrome browsers and extensions used in your organization. You can turn on managed profile reporting to view profile-level information, browser-level information, and limited device information. Finally, you can turn on browser event reporting to report browser events such as password reuse, malware downloads, extension installs, and make these available in the Admin console.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Chrome Insights report
As an admin, you can use the Google Admin console to see insights about the ChromeOS devices and Chrome browsers in your organization. On the Chrome Insights Report page, you can see the following reports:

- Devices receiving their last automatic update

- Devices That Need Attention
- Device Fleet Hardware Report
- Browsers that need attention

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Chrome Enterprise reporting connectors
As an admin, you can use the Google Admin console to get Chrome to report events to third-party service providers. For example, you can configure Chrome to report security events such as malware transfer, unsafe site visits, and password reuse. You can let Chrome report events using multiple service providers and configurations at the same time.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Supplemental Guidance

- Device Reports
- Chrome Browser and Profile reporting
- Chrome Insights report
- Chrome Enterprise reporting connectors

Control Domain	Configuration Management		
Control #	**CM.L2-3.4.1**		
Control Description	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.		
Google Workspace Enabling Features	Chrome Policies for Users or Browsers ChromeOS Device Policies	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer

Customer Implementation Description

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Chrome Policies for Users or Browsers**
- **ChromeOS Device Policies**

A description of each feature and implementation guidance is included below.

Chrome Policies for Users or Browsers
Administrators who choose to use Chrome Policies for Users or Browsers should establish a baseline configuration for their users or browsers.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

As an administrator, you can use your Google Admin console to find details about enrolled Chrome browsers. You can review information such as enrollment dates, installed extensions, applied policies, and more.

To view browser information:

1. Sign in with an administrator account to the Google Admin console.
2. In the Admin console, go to Menu and then Devices and then Chrome and then Managed browsers.
    a. If you signed up for Chrome Enterprise Core, go to Menu and then Chrome browserand thenManaged browsers.
3. (Optional) On the left, select an organizational unit. By default, all browsers are shown.

ChromeOS Policies
As a Chrome Enterprise admin, you should establish a baseline configuration for devices that run ChromeOS. You can manage policies and settings for Chromebooks and other devices that run ChromeOS from the cloud-based Google Admin console. You can control settings that apply when people use a managed ChromeOS device, such as a Chromebook. Device-level settings apply for anyone who uses the device, even if they sign in as a guest or with a personal Gmail account. On the Device settings page, you can set policies that apply to anyone who uses a managed ChromeOS device, even if they sign in as a guest or with a personal Gmail account.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

As an administrator, you can find details about the ChromeOS devices in your domain in the Google Admin console. To view the device list page, go to Menu and then Devices and then Chrome and then Devices. Click the serial number of any device to view device details. You can also create organizational units to apply settings to different groups of devices.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations
1. The Center for Internet Security (CIS) is a nonprofit that promotes best practices for securing IT systems and data. They publish a variety of materials including CIS Benchmarks. The CIS Benchmarks are security guidelines that institutions across industries can use to assist in the configuration of their environments. You can access the CIS Benchmarks for configuration of Chrome Browser and ChromeOS on the CIS website. Please refer to the supplemental guidance for a direct link.
Supplemental Guidance
• Chrome Policies for Users or Browsers • View Chrome browser details • ChromeOS Device Policies • View ChromeOS device list and details • CIS Benchmarks for Google Chrome

Control Domain	Configuration Management		
Control #	**CM.L2-3.4.2**		
Control Description	Establish and enforce security configuration settings for information technology products employed in organizational systems.		
Google Workspace Enabling Features	Chrome Policies for Users or Browsers ChromeOS Device Policies	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer
Customer Implementation Description			
When configured correctly, the following feature(s) in Google Workspace may be used to support this control: • **Chrome Policies for Users or Browsers** • **ChromeOS Device Policies** A description of each feature and implementation guidance is included below. **Chrome Policies for Users or Browsers** Administrators who choose to deploy Chrome browsers across corporate Windows, Mac, or Linux computers have two options to manage Chrome browsers from the Google Admin console: Chrome Enterprise Core (recommended), or through signed-in user based policies.			

You can enforce Chrome policies from your Admin console that apply to:

- User accounts to sync policies and preferences across a user's devices. Settings apply whenever the user signs in to Chrome browser with their managed account on any device.
- Enrolled browsers to enforce policies when users open Chrome browser on managed Microsoft Windows, Apple Mac, or Linux computers. Signing in is not required.

Administrators who choose to use Chrome Policies for Users or Browsers should establish a baseline configuration for their users or browsers.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

As an administrator, you can use your Google Admin console to find details about enrolled Chrome browsers. You can review information such as enrollment dates, installed extensions, applied policies, and more.

To view browser information:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the Admin console, go to **Menu** and then **Devices** and then **Chrome** and then **Managed browsers**.
    a. If you signed up for Chrome Enterprise Core, go to **Menu** and then **Chrome** browser and then **Managed browsers**.
3. (Optional) On the left, select an organizational unit. By default, all browsers are shown.

ChromeOS Policies

As a Chrome Enterprise admin, you can manage policies and settings for Chromebooks and other devices that run ChromeOS from the cloud-based Google Admin console. You can control settings that apply when people use a managed ChromeOS device, such as a Chromebook. Device-level settings apply for anyone who uses the device, even if they sign in as a guest or with a personal Gmail account. On the Device settings page, you can set policies that apply to anyone who uses a managed ChromeOS device, even if they sign in as a guest or with a personal Gmail account.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

As an administrator, you can find details about the ChromeOS devices in your domain in the Google Admin console. To view the device list page, go to Menu and then Devices and then Chrome and then Devices. Click the serial number of any device to view device details. You can also create organizational units to apply settings to different groups of devices.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. The Center for Internet Security (CIS) is a nonprofit that promotes best practices for securing IT systems and data. They publish a variety of materials including CIS Benchmarks. The CIS Benchmarks are security guidelines that institutions across industries can use to assist in the configuration of their environments. You can access the CIS Benchmarks for configuration of Chrome Browser and ChromeOS on the CIS website. Please refer to the supplemental guidance for a direct link.

Supplemental Guidance

- Chrome Policies for Users or Browsers
- View Chrome browser details
- ChromeOS Device Policies
- View ChromeOS device list and details
- CIS Benchmarks for Google Chrome

Control Domain	Configuration Management		
Control #	**CM.L2-3.4.6**		
Control Description	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.		
Google Workspace Enabling Features	Apps & Extensions ChromeOS Device Policies	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer

Customer Implementation Description

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Apps & Extensions**
- **ChromeOS Device Policies**

A description of each feature and implementation guidance is included below.

Apps & Extensions

As a Chrome Enterprise admin, you can use your Admin console to apply app and extension policies across several apps at a time. These app or extension policies can apply for signed-in users on any device or enrolled browsers on Windows, Mac, or Linux. You can also control which apps or extensions users can install on managed Chrome browsers or ChromeOS devices.

Customers interested in using this feature can use the links in the supplemental guidance for more information.

ChromeOS Device Policies
As a Chrome Enterprise admin, you should employ the principle of least functionality when configuring Chrome policies for managed Chromebooks and other ChromeOS devices and set common policies. You can manage policies and settings for Chromebooks and other devices that run ChromeOS from the cloud-based Google Admin console.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Supplemental Guidance

- View and configure apps and extensions
- Allow or block apps and extensions
- Managing ChromeOS device policies

Control Domain	Configuration Management		
Control #	**CM.L2-3.4.7**		
Control Description	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.		
Google Workspace Enabling Features	Apps & Extensions ChromeOS Device Policies	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer
Customer Implementation Description			
When configured correctly, the following feature(s) in Google Workspace may be used to support this control: • **Apps & Extensions**			

- **ChromeOS Device Policies**

A description of each feature and implementation guidance is included below.

Apps & Extensions
As a Chrome Enterprise admin, you can control which apps or extensions users can install on managed Chrome browsers or ChromeOS devices.

To block or allow an app:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the Admin console, go to **Menu** and then **Devices** and then **Chrome** and then **Apps & extensions** and then **Users & browsers**.
    a. If you signed up for Chrome Browser Cloud Management, go to **Menu** and then **Chrome browser** and then **Apps & extensions** and then **Users & browsers**.
3. (Users only) To apply the setting to a group, do the following:
    a. Select **Groups**.
    b. Select the group to which you want to apply the setting.
4. To apply the setting to all users and enrolled browsers, leave the top organizational unit selected. Otherwise, select a child organizational unit.
5. Find the app that you want to configure policies for.
6. Under Installation policy, choose **Block**.
7. Click **Save**.

ChromeOS Device Policies
As a Chrome Enterprise admin, you should employ the principle of least functionality when configuring Chrome policies for managed Chromebooks and other ChromeOS devices and set common policies. You can manage policies and settings for Chromebooks and other devices that run ChromeOS from the cloud-based Google Admin console.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Supplemental Guidance

- View and configure apps and extensions
- Allow or block apps and extensions
- Managing ChromeOS device policies

Control Domain	Configuration Management		
Control #	**CM.L2-3.4.8**		
Control Description	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.		
Google Workspace Enabling Features	Apps & Extensions	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer

Customer Implementation Description

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Apps & Extensions**

A description of each feature and implementation guidance is included below.

Apps & Extensions

As a Chrome Enterprise admin, you can control which apps or extensions users can install on managed Chrome browsers or ChromeOS devices within the Play Store or the Chrome Web Store.

1. If you signed up for Chrome Browser Cloud Management, go to **Menu** and then **Chrome browser** and then **Apps & extensions** and then **Users & browsers**.
2. (Users only) To apply the setting to a group, do the following:
    a. Select **Groups**.
    b. Select the group to which you want to apply the setting.
3. To apply the setting to all users and enrolled browsers, leave the top organizational unit selected. Otherwise, select a child organizational unit.
4. On the right, click **Additional settings**.
5. Go to Allow/block mode.
6. Click **Edit**.
7. For Play Store apps, select one of the following options:
    a. Allow all apps, admin manages blocklist—Users can install all apps and extensions from the Google Play Store, except the ones that you block.
    b. Block all apps, admin manages allowlist—Users can only install the apps and extensions from the Google Play Store that you allow.
8. For Chrome Web Store apps, select one of the following options:
    a. Allow all apps, admin manages blocklist—Users can install all apps and extensions from the Chrome Web Store, except the ones that you block.

b. Block all apps, admin manages allowlist—Users can only install the apps and extensions from Chrome Web Store that you allow.
c. Block all apps, admin manages allowlist, users may request extensions—Users can only install the apps and extensions from the Chrome Web Store that you allow, but they can also request the extensions that they need. Then, you can allow, block, or automatically install extensions that users request. See the link in the supplemental guidance for more details.

9. Click **Save**.

Supplemental Guidance

- Allow or block apps and extensions

Control Domain	Configuration Management		
Control #	**CM.L2-3.4.9**		
Control Description	Control and monitor user-installed software.		
Google Workspace Enabling Features	Apps & Extensions	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer

Customer Implementation Description

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Apps & Extensions**

A description of each feature and implementation guidance is included below.

Apps & Extensions
From your Admin console, you can list all apps and extensions you've set policies for in an organizational unit.

1. Sign in with an administrator account to the **Google Admin** console.
2. In the Admin console, go to **Menu** and then **Devices** and then **Chrome** and then **Apps & extensions**. The Overview page opens by default.
3. If you signed up for **Chrome Enterprise Core**, go to **Menu** and then **Chrome browser** and then **Apps & extensions**.
4. At the top, click the type of app or extension you want to view:
   a. **Users & browsers**

b. **Kiosks**
c. **Managed guest sessions**

5. On the left, choose your search:
   a. **Users**—search for apps for a specific user
   b. **Groups**—Search for apps within a specific group
   c. **Organizational units**—Search for apps within a specific organizational unit
6. At the top, click Search or add a filter and search by:
   a. **Full-text**—Enter the app or extension name or ID.
   b. **Title**—Enter the app or extension name.
   c. **ID**—Enter the app or extension ID.
   d. **Type**—Choose whether to display Android, Chrome, web apps, or IWAs.
   e. **Installation policy**—Choose whether to display apps, depending on their installation policy.
7. Click **Apply**.

Supplemental Guidance

- Apps & Extensions

Control Domain	Identification & Authentication		
Control #	**IA.L1-3.5.1**		
Control Description	Identify system users, processes acting on behalf of users, and devices.		
Google Workspace Enabling Features	SAML SSO for ChromeOS devices SAML SSO for Chrome apps Chrome Enterprise Connectors ChromeOS Device Management	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer

Customer Implementation Description

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **SAML SSO for ChromeOS devices**
- **SAML SSO for Chrome apps**
- **Chrome Enterprise Connectors**
- **ChromeOS Device Management**

A description of each feature and implementation guidance is included below.

SAML SSO for ChromeOS devices

SAML SSO support for ChromeOS devices allows users to sign in to a device with the same authentication mechanisms that you use within the rest of your organization. Their passwords can remain within your organization's IdP. Signing in is very similar to signing in to a Google Workspace account from a browser via SAML SSO. However, because a user is signing in to a device, there are several additional considerations.

Additionally, You can choose to sync ChromeOS device local passwords with users' SAML SSO passwords. By default, the local password is updated every time users sign in online. You can configure how often users are required to sign in online using the SAML single sign-on login frequency or SAML single sign-on unlock frequency settings. However, some users might change their SAML SSO password before they're required to sign in online again. If that happens, users continue to use their old local ChromeOS password until the next time they sign in online. To keep the local ChromeOS password in sync with their SAML SSO password, you can force them to sign in online as soon as their SAML SSO password changes. That way, they update their ChromeOS password almost immediately.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

SAML SSO for Chrome apps
You can use the SAML SSO for Chrome Apps extension when you need to configure SAML SSO for Chrome apps. Users can sign in to a Chrome app with the same authentication mechanisms that you use within the rest of your organization. Their passwords can remain within your organization's IdP.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Chrome Enterprise device trust connectors
As an admin, you can configure Chrome Enterprise device trust connectors to share context-aware signals from managed Chrome browsers, managed Chrome profiles and ChromeOS devices with third-party IdPs. This integration allows device trust signals as inputs in authentication and authorization policies. This solution provides enhanced security and less dependence on the network as a trust factor.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

ChromeOS Device Management
As an administrator, you can find details about the ChromeOS devices in your domain in the Google Admin console.

To view the device list page:

1. Go to **Menu** and then **Devices** and then **Chrome** and then **Devices**. 2. Click the serial number of any device to view device details. You can also create organizational units to apply settings to different groups of devices.
Supplemental Guidance
• SAML SSO for ChromeOS devices • SAML SSO for Chrome apps • Chrome Enterprise Connectors • ChromeOS device management

Control Domain	**Identification & Authentication**		
Control #	**IA.L1-3.5.2**		
Control Description	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.		
Google Workspace Enabling Features	SAML SSO for ChromeOS devices SAML SSO for Chrome apps Chrome Enterprise Connectors ChromeOS Device Management	**Control Responsibility**	[ ] Google [ ] Shared [X] Customer
Customer Implementation Description			

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **SAML SSO for ChromeOS devices**
- **SAML SSO for Chrome apps**
- **Chrome Enterprise Connectors**
- **ChromeOS Device Management**

A description of each feature and implementation guidance is included below.

Configure SAML single sign-on for ChromeOS devices
SAML SSO support for ChromeOS devices allows users to sign in to a device with the same authentication mechanisms that you use within the rest of your organization. Their passwords can remain within your organization's IdP. Signing in is very similar to signing in to a Google Workspace account from a browser via SAML SSO. However, because a user is signing in to a device, there are several additional considerations.

Additionally, You can choose to sync ChromeOS device local passwords with users' SAML SSO passwords. By default, the local password is updated every time users sign in online. You can configure how often users are required to sign in online using the SAML single sign-on login frequency or SAML single sign-on unlock frequency settings. However, some users might change their SAML SSO password before they're required to sign in online again. If that happens, users continue to use their old local ChromeOS password until the next time they sign in online. To keep the local ChromeOS password in sync with their SAML SSO password, you can force them to sign in online as soon as their SAML SSO password changes. That way, they update their ChromeOS password almost immediately.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Configure SAML single sign-on for Chrome apps
You can use the SAML SSO for Chrome Apps extension when you need to configure SAML SSO for Chrome apps. Users can sign in to a Chrome app with the same authentication mechanisms that you use within the rest of your organization. Their passwords can remain within your organization's IdP.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Chrome Enterprise device trust connectors
As an admin, you can configure Chrome Enterprise device trust connectors to share context-aware signals from managed Chrome browsers, managed Chrome profiles and ChromeOS devices with third-party IdPs. This integration allows device trust signals as inputs in authentication and authorization policies. This solution provides enhanced security and less dependence on the network as a trust factor.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

ChromeOS Device Management
As an administrator, you can find details about the ChromeOS devices in your domain in the Google Admin console.

To view the device list page:

1. Go to **Menu** and then **Devices** and then **Chrome** and then **Devices**.
2. Click the serial number of any device to view device details. You can also create organizational units to apply settings to different groups of devices.

Supplemental Guidance

- SAML SSO for ChromeOS devices
- SAML SSO for Chrome apps
- Chrome Enterprise Connectors
- ChromeOS device management

Control Domain	Identification & Authentication		
Control #	**IA.L2-3.5.3**		
Control Description	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.		
Google Workspace Enabling Features	2–Step Verification	**Control Responsibility**	[ ] Google [ ] Shared [X] Customer
Customer Implementation Description			
When configured correctly, the following feature(s) in Google Workspace may be used to support this control: • **2-Step Verification** A description of each feature and implementation guidance is included below. **2-Step Verification** As a Chrome enterprise admin, you can implement 2-Step Verification (2-SV) or Multi-Factor Authentication (MFA) in your organization and force users to regularly sign in to their ChromeOS devices. This means that your users must regularly sign in to their account in two or more steps and provides additional security for your organization. *Customers interested in using this feature can use the link in the supplemental guidance for more information.*			
Supplemental Guidance			
• 2-Step Verification			

Control Domain	IA.L2-3.5.11		
Control #	**IA.L2-3.5.8**		
Control Description	Obscure feedback of authentication information.		
Google Workspace Enabling Features	Chrome Policy: Display password button	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer
Customer Implementation Description			
When configured correctly, the following feature(s) in Google Workspace may be used to support this control: • **Chrome Policy: Display password button** A description of each feature and implementation guidance is included below. **Chrome Policy: Display password button** By default, password data is obscured in Chrome, but users may choose to select the eye icon next to the password field to reveal their password. You can change this using a Chrome policy. If you select **Do not show the display password button on the login and lock screen**, users don't see the icon. *Customers interested in using this feature can use the link in the supplemental guidance for more information.*			
Supplemental Guidance			
• Chrome Policy: Display password button			

Control Domain	Incident Response		
Control #	**IR.L2-3.6.1**		
Control Description	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.		
Google Workspace Enabling Features	Chrome Enterprise Connectors Framework	**Control Responsibility**	☐ Google ☐ Shared

			[X] Customer
Customer Implementation Description			
While Chrome does not natively offer any features that, if configured correctly, will address this control, the following features may support your ability to meet the control: • **Chrome Enterprise Connectors Framework** A description of each feature and implementation guidance is included below. **Chrome Enterprise Connectors Framework** Chrome Enterprise Connectors Framework offers a collection of connectors and APIs that simplify the steps needed to integrate Chrome browser and ChromeOS with solution providers, including security providers including Splunk, Crowdstrike, and Palo Alto Networks. You can also allow third-party providers to monitor potential threats by reporting ChromeOS telemetry events. Events are sent directly from Google with no additional agents needed. As an admin, you can use the Google Admin console to get Chrome to report events to third-party service providers. For example, you can configure Chrome to report security events such as malware transfer, unsafe site visits, and password reuse. You can let Chrome report events using multiple service providers and configurations at the same time. *Customers interested in using this feature can use the link in the supplemental guidance for more information.*			
Supplemental Guidance			
• Chrome Enterprise Connectors Framework			

Control Domain	**Media Protection**		
Control #	**MP.L2-3.8.7**		
Control Description	Control the use of removable media on system components.		
Google Workspace Enabling Features	ChromeOS Policy: USB Access	**Control Responsibility**	[ ] Google [ ] Shared [X] Customer
Customer Implementation Description			

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **ChromeOS Policy: USB Access**

A description of each feature and implementation guidance is included below.

ChromeOS Policy: USB Access
You can use this policy to specify a list of USB devices that can be accessed directly by apps, such as Citrix Receiver. You can list devices, such as keyboards, signature pads, printers and scanners, as well as other USB devices.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Supplemental Guidance

- ChromeOS Policy: USB Access

Control Domain	Maintenance		
Control #	**MA.L2-3.7.1**		
Control Description	Perform maintenance on organizational systems.		
Google Workspace Enabling Features	Chrome Browser Updates ChromeOS Updates	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer

Customer Implementation Description

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Chrome Browser Updates**
- **ChromeOS Updates**

A description of each feature and implementation guidance is included below.

Chrome Browser Updates
As an administrator, you can manage Chrome browser updates for users in your organization. Chrome releases a full browser update about every 6 weeks. Minor updates, such as security fixes and software updates, happen every 2–3 weeks. To keep Chrome browser secure and up to date, Google recommends using automatic updates instead of manual updates. If your

organization deploys Chrome browser to thousands of devices or if you have bandwidth restrictions, you might need to customize how updates are deployed.

By default, Chrome browser updates to the latest version of Chrome when it is available. We recommend that you keep the default auto-update settings. That way, your users' devices will automatically update to new versions of Chrome browser as they're released on the Stable channel. Your users will get critical security fixes and new features as they become available.

To configure automatic updates:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the Admin console, go to **Menu** and then **Devices** and then **Chrome** and then **Settings**. The User & browser settings page opens by default.
    a. If you signed up for Chrome Enterprise Core, go to **Menu** and then **Chrome browser** and then **Settings.**
3. To apply the setting to all enrolled browsers, leave the top organizational unit selected. Otherwise, select a child organizational unit.
4. Go to **Chrome updates**.
5. Click **Chrome browser updates**.
6. Select **Allow updates**.
7. Click **Save**.

ChromeOS Updates

As a Chrome administrator, you can manage ChromeOS updates for devices in your organization. Chrome releases a full OS update about every 4 weeks. Minor updates, such as security fixes and software updates, happen every 2–3 weeks. By default, ChromeOS devices update to the latest version of Chrome when it is available. Google recommends that you keep the default auto-update settings. That way, your users' devices will automatically update to new versions of ChromeOS as they're released on the Stable channel. Your users will get critical security fixes and new features as they become available.

8. Sign in with an administrator account to the **Google Admin** console.
9. In the Admin console, go to **Menu** and then **Devices** and then **Chrome** and then **Settings** and then **Device settings**.
10. To apply the setting to all devices, leave the top organizational unit selected. Otherwise, select a child organizational unit.
11. Go to **Device update** settings.
12. Click **Auto-update** settings.
13. Select **Allow updates**.
14. Click **Save**.

Supplemental Guidance

- Chrome Browser Updates

- ChromeOS Updates

Control Domain	System & Communications Protection		
Control #	**SC.L2-3.13.4**		
Control Description	Prevent unauthorized and unintended information transfer via shared system resources.		
Google Workspace Enabling Features	Chrome Policy: Guest Mode Managed Guest Sessions	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer

Customer Implementation Description

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Chrome Policy: Guest Mode**
- **Managed Guest Sessions**

A description of each feature and implementation guidance is included below.

Chrome Policy: Guest Mode
Guest mode is a feature in Chrome that allows someone to use a Chromebook without signing in to a Google account. This policy controls guest browsing on managed ChromeOS devices. If you select **Allow guest mode**, the main sign-in screen offers the option for a user to sign in as a guest. If you select **Disable guest mode**, a user must sign in using a Google Account or Google Workspace account. When a user signs in using guest mode, your organization's policies are not applied.

To disable this feature:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the Admin console, go to **Menu** and then **Devices** and then **Chrome** and then **Settings** and then **Device settings.**
3. (Optional) To apply the setting only to some users and enrolled browsers, at the side, select an organizational unit (often used for departments) or configuration group (advanced).
4. Click **Guest mode** under Sign-in Settings.
5. Next to configuration, select **Disable guest mode.**
6. Click **Save.**

Managed Guest Sessions
With managed guest sessions, multiple users can share the same device running Chrome OS without having to sign in to their Google Account. For example, use managed guest sessions to configure Chrome devices as loaner devices or shared computers. Before a device can host managed guest sessions, you must enroll the devices that you want to let users run managed guest sessions and place devices that users will use to run managed guest sessions in an organizational unit.

To disable Managed Guest Sessions in Chrome devices:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the Admin console, go to **Menu** and then **Devices** and then **Chrome** and then **Settings** and then **Managed guest sessions**.
3. To apply the setting to everyone, leave the top organizational unit selected. Otherwise, select a child organizational unit.
4. Next to configuration, choose **Do not allow managed guest sessions**
5. Click **Save**.

Supplemental Guidance

- Chrome Policy: Guest Mode
- Managed Guest Sessions

Control Domain	System & Communications Protection		
Control #	**SC.L2-3.13.6**		
Control Description	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).		
Google Workspace Enabling Features	Chrome URL Blocklist or Allowlist Chrome Enterprise Connectors Framework Local and Network Printers	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer

Customer Implementation Description

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Chrome URL Blocklist or Allowlist**
- **Chrome Enterprise Connectors Framework**
- **Local and Network Printers**

A description of each feature and implementation guidance is included below.

Chrome URL Blocklist or Allowlist
As a Chrome Enterprise admin, you can block and allow URLs so that users can only visit certain websites. Restricting users' internet access can increase productivity and protect your organization from viruses and malicious content found on some websites.

To configure a URL blocklist:

1. In the **Admin** console, go to **Menu** and then **Devices** and then **Chrome** and then **Settings**.
    a. If you signed up for Chrome Enterprise Core, go to **Menu** and then **Chrome browser** and then **Settings**.
2. (Optional) To apply the setting only to some users and enrolled browsers, at the side, select an organizational unit (often used for departments) or configuration group
3. Go to **Content**.
4. Click **URL Blocking** and enter URLs as needed:
    a. **Blocked URLs**—URLs that you want to prevent users from accessing.
    b. **Blocked URL exceptions**—URLs that you want to allow users to access (allowlist). **Access is allowed even if the URLs are also defined in Blocked URLs.**
5. You can block and allow up to 1,000 URLs.
6. Click **Save**.

Chrome Enterprise Connectors Framework
Chrome Enterprise Connectors Framework offers a collection of connectors and APIs that simplify the steps needed to integrate Chrome browser and ChromeOS with solution providers. As an admin, you can use the Google Admin console to get Chrome to report events to third-party service providers. For example, you can configure Chrome to report security events such as malware transfer, unsafe site visits, and password reuse. You can let Chrome report events using multiple service providers and configurations at the same time.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Local and Network Printers
As an administrator, you can use Common UNIX Printing System (CUPS) printers with your organization's ChromeOS devices. CUPS uses an Internet Printing Protocol (IPP) to print to local and network printers. You can also track print jobs and printer usage in your organization. You can add and specify a printer for everyone, or for users or devices in certain groups or departments.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. Alternatively, you can use Google Workspace to configure the networks that company-managed mobile devices, ChromeOS devices, and Google meeting room hardware use. You can control Wi-Fi, Ethernet, and Virtual Private Network (VPN) access, and set up network certificates. When you add a network configuration, you can apply the same network settings for your entire organization, or enforce specific network settings for different organizational units. Customers interested in using this feature can use the link in the supplemental guidance for more information.

Supplemental Guidance

- Chrome URL Blocklist or Allowlist
- Chrome Enterprise Connectors Framework
- Network Management
- Local and Network Printers

Control Domain	System & Communications Protection		
Control #	**SC.L2-3.13.10**		
Control Description	Establish and manage cryptographic keys for cryptography employed in organizational systems.		
Google Workspace Enabling Features	Google Cloud Certificate Connector Certificate Enrollment for ChromeOS extension HTTPS Certificate Authority Certificate Enrollment for ChromeOS via SCEP	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer

Customer Implementation Description

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Google Cloud Certificate Connector**
- **Certificate Enrollment for ChromeOS extension**
- **HTTPS Certificate Authority**
- **Certificate Enrollment for ChromeOS via SCEP**

A description of each feature and implementation guidance is included below.

Google Cloud Certificate Connector
You can control user access to your organization's Wi-Fi networks, internal apps, and internal websites on ChromeOS devices by using a connector to distribute device certificates from your on-premises Certificate Authority (CA). The Google Cloud Certificate Connector is a Windows service that securely distributes certificates and authentication keys from your Simple Certificate Enrollment Protocol (SCEP) server to users' devices. For ChromeOS devices, private keys for certificates are generated on the device. The corresponding public key is stored temporarily on Google servers and deleted after the certificate is installed.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Certificate Enrollment for ChromeOS extension
As an administrator you can use the Certificate Enrollment for ChromeOS extension to enable a user to get a user or device certificate either manually or automatically. You can also set up the automatic renewal of existing certificates that are expiring. Before using the extension, ensure that users have access, and that the extension and associated managed policy are properly configured. For more help with setting up the extension, see the Extension deployment guide section.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

HTTPS Certificate Authority
You will need to set up a CA to manage networks and monitor traffic for your ChromeOS devices. It's important to set up a CA to ensure that your users can access websites that have digital certificates that can be validated by a specific CA. This should be done early during your deployment to ensure that users can access websites without issues.

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Certificate Enrollment for ChromeOS via SCEP
You may choose to set up ChromeOS Certificate Enrollment with SCEP. The Configuring Certificate Enrollment for ChromeOS via SCEP with Microsoft NDES guide is for IT administrators with Active Directory expertise who want to set up ChromeOS Certificate Enrollment with SCEP. It provides steps for configuring the Microsoft Network Device Enrollment Service (NDES) to allow enrollment and issuance of certificates used to authenticate ChromeOS devices and users to WiFi access points.

Customers interested in using this feature can use the link in the supplemental guidance for more information.
Supplemental Guidance
• Google Cloud Certificate Connector • Certificate Enrollment for ChromeOS extension • HTTPS Certificate Authority • Certificate Enrollment for ChromeOS via SCEP

Control Domain	**System & Information Integrity**		
Control #	**SI.L1-3.14.2**		
Control Description	Provide protection from malicious code at designated locations within organizational systems.		
Google Workspace Enabling Features	Chrome Safe Browsing	**Control Responsibility**	[X] Google [ ] Shared [ ] Customer
Customer Implementation Description			

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Chrome Safe Browsing**

Chrome Safe Browsing
To keep your data private, Google Chrome uses Safe Browsing to protect you against:

- Abusive websites and extensions
- Malicious and intrusive ads
- Malware
- Phishing
- Social engineering

Chrome Safe Browsing comes in two flavors: Standard Protection and Enhanced Protection

Customers interested in using this feature can use the link in the supplemental guidance for more information.

Additional Considerations

1. If you wish to use Chrome Safe Browsing to implement this control on your endpoints, you should consider restricting the browsers which are installed on those endpoints, or ensuring that all browsers installed on endpoints provide similar features.

Supplemental Guidance

- Chrome Safe Browsing

Control Domain	System & Information Integrity		
Control #	**SI.L1-3.14.4**		
Control Description	Update malicious code protection mechanisms when new releases are available.		
Google Workspace Enabling Features	Chrome Browser Updates	**Control Responsibility**	☐ Google ☐ Shared ☒ Customer

Customer Implementation Description

When configured correctly, the following feature(s) in Google Workspace may be used to support this control:

- **Chrome Browser Updates**
- **ChromeOS Updates**

A description of each feature and implementation guidance is included below.

Chrome Browser Updates
As an administrator, you can manage Chrome browser updates for users in your organization. Chrome releases a full browser update about every 6 weeks. Minor updates, such as security fixes and software updates, happen every 2–3 weeks. To keep Chrome browser secure and up to date, Google recommends using automatic updates instead of manual updates. If your organization deploys Chrome browser to thousands of devices or if you have bandwidth restrictions, you might need to customize how updates are deployed.

By default, Chrome browser updates to the latest version of Chrome when it's available. We recommend that you keep the default auto-update settings. That way, your users' devices will automatically update to new versions of Chrome browser as they are released on the Stable channel. Your users will get critical security fixes and new features as they become available.

To configure automatic updates:

1. Sign in with an administrator account to the **Google Admin** console.
2. In the Admin console, go to **Menu** and then **Devices** and then **Chrome** and then **Settings**. The User & browser settings page opens by default.
    a. If you signed up for Chrome Enterprise Core, go to **Menu** and then **Chrome browser** and then **Settings.**
3. To apply the setting to all enrolled browsers, leave the top organizational unit selected. Otherwise, select a child organizational unit.
4. Go to **Chrome updates**.
5. Click **Chrome browser updates**.
6. Select **Allow updates**.
7. Click **Save**.

ChromeOS Updates
As a Chrome administrator, you can manage ChromeOS updates for devices in your organization. Chrome releases a full OS update about every 4 weeks. Minor updates, such as security fixes and software updates, happen every 2–3 weeks. By default, ChromeOS devices update to the latest version of Chrome when it's available. Google recommends that you keep the default auto-update settings. That way, your users' devices will automatically update to new versions of ChromeOS as they're released on the Stable channel. Your users will get critical security fixes and new features as they become available.

1. Sign in with an administrator account to the **Google Admin** console.
2. In the Admin console, go to **Menu** and then **Devices** and then **Chrome** and then **Settings** and then **Device settings**.

3. To apply the setting to all devices, leave the top organizational unit selected. Otherwise, select a child organizational unit. 4. Go to **Device update** settings. 5. Click **Auto-update** settings. 6. Select **Allow updates**. 7. Click **Save**.
Supplemental Guidance
• Chrome Browser Updates • ChromeOS Updates

Security audits and certifications

The Cyber AB does not issue certifications for CMMC compliance for Cloud Service Providers (CSPs), but rather requires CSPs be a minimum of FedRAMP Moderate or equivalent to support customers CMMC compliance. Google Workspace is FedRAMP High compliant (see FedRAMP Marketplace), and makes other certifications, like ISO/IEC certificates and SOC audit reports, available for download via Compliance Reports Manager.[1]

Learn more about Google Workspace by visiting our compliance offerings website.[2]

Additional resources

These additional resources may help you understand how Google services are designed with privacy, confidentiality, integrity, and availability of data in mind.

- Google Workspace Help Center[3]
- Google Workspace security page[4]
- Google Cloud Compliance Resource Center[5]
- How Google Workspace uses encryption to protect your data[6]

This CMMC implementation guide is for informational purposes only. Google does not intend the information or recommendations in this guide to constitute legal advice. Each customer should independently evaluate its own particular use of the services as appropriate to support its legal compliance obligations.

[1] https://cloud.google.com/security/compliance/compliance-reports-manager
[2] https://cloud.google.com/security/compliance/offerings
[3] https://support.google.com/a/
[4] https://www.google.com/work/our-approach.html
[5] https://cloud.google.com/security/compliance
[6] https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf

Key terms, acronyms & definitions

Term	Definition
Assured Controls Plus	Assured Controls Plus for Google Workspace are specialized features that provide organizations with advanced tools and support
CMMC	The Cybersecurity Maturity Model Certification (CMMC) is a program which verifies that companies in the Defense Industry Base (DIB) have adequate cybersecurity safeguards in place
CUI	Controlled Unclassified Information (CUI) is a category of federal information that is not classified but still requires protection to ensure national security
CUI Boundary	The Controlled Unclassified Information (CUI) boundary is the defined organizational systems, facilities in which CUI is stored, processed, and transmitted
Customer	User of Google Workspace, including but not limited to: the DCMA, members of the DIB, federal contractors and subcontractors, OSAs, etc.
DCMA	The Defense Contract Management Agency (DCMA) is a federal agency that manages contracts for the Department of Defense and other federal agencies
DFARS	The Defense Federal Acquisition Regulation Supplement (DFARS) is a set of regulations that apply to a United States Department of Defense (DoD) contracts
DIB	The Defense Industry Base (DIB) is a network of organizations, facilities, and resources that support the United States military with services, resources, and equipment
Enterprise Plus Edition	Google Workspace Enterprise Plus Edition to a subscription that provides premium security and collaboration features for customers
FAR	The Federal Acquisition Regulation (FAR) is a set of regulations that govern how the federal govern provisions goods and services
NIST	The National Institute of Standards and Technology (NIST) is a United States federal agency that develops measurement

	standards, including several cybersecurity frameworks such as NIST 800-171 and NIST 800-53.
OSA	Organizations seeking assessment (OSAs) are organizations aiming to comply with CMMC and/or organizations considering bidding on future Department of Defense (DoD) contracts with CMMC obligations.