CONFIDENTIAL

JAMORIE

GOOGLE WORKSPACE

Security Assessment Report

Client: Société Patrimoniale Jacques GmbH

Assessment Date: 17 March 2026

Auditor: Edouard Jacques

Standard: CIS Google Workspace Benchmark

Scope: L1+L2 Controls

Jamorie Consulting GmbH · Mergenthalerallee 15-22, 65760 Eschborn · edouard.jacques@jamorie.eu · +49 171 35 61623

1. Management Summary

On behalf of Jamorie Consulting GmbH, we conducted a comprehensive security assessment of Société Patrimoniale Jacques GmbH's Google Workspace environment against the CIS Google Workspace Benchmark, encompassing both Level 1 and Level 2 controls. The assessment evaluated 89 controls in total, of which 26 passed, 53 failed, and 5 require further manual review. This yields an overall compliance score of 32.9%, which falls significantly below the threshold considered acceptable for a securely configured enterprise environment and indicates that the organisation's Google Workspace deployment presents a materially elevated risk profile that warrants prompt and structured remediation.

The most critical risk areas identified span several functional domains, with Login & Identity representing the most severe concern: all eight assessed controls in this category failed, indicating that foundational identity security mechanisms — including multi-factor authentication enforcement and account lifecycle controls — are not adequately configured. The Drive category similarly presents substantial risk, with 10 of 12 controls failing, exposing the organisation to potential data exfiltration through unrestricted external sharing, uncontrolled file publishing, and insufficient access governance. Calendar controls also showed a high failure rate, with four of six controls failing, raising concerns around the inadvertent disclosure of sensitive scheduling and organisational information to external parties. Additionally, the failure of control 1.1.1 — confirming that fewer than two Super Admin accounts are properly configured — represents a significant operational and security resilience gap, as it creates a single point of failure for administrative access and recovery.

Access Management and administrative controls require prioritised attention, particularly the absence of external directory data restrictions (control 1.2.1.1) and the inadequate configuration of Super Admin redundancy. These deficiencies, if exploited, could result in unauthorised access to sensitive corporate and personal data, potentially triggering regulatory obligations under applicable data protection legislation. Remediation efforts should be sequenced to address identity and access controls first, followed by data sharing governance within Drive and Calendar, as these represent the highest likelihood of real-world impact and the broadest potential exposure.

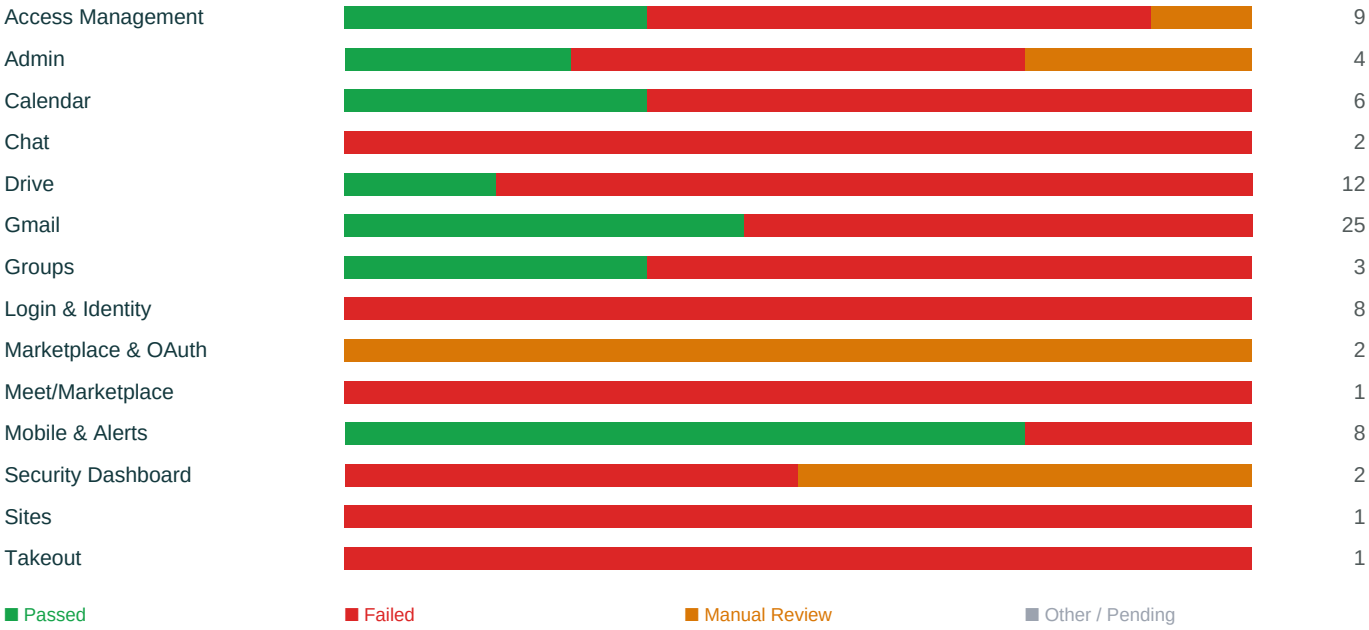
Despite the overall compliance posture, it is noteworthy that the Mobile & Alerts category demonstrated a relatively strong result, with six of eight controls passing, suggesting that the organisation has invested meaningful effort in endpoint visibility and alerting configurations. Similarly, Gmail showed the highest absolute number of passing controls at 11, reflecting a degree of maturity in email security hardening, even though 14 controls in that category still require remediation. These results indicate that the organisation possesses the operational capacity to implement and maintain security controls effectively, and they provide a constructive foundation upon which a broader remediation programme can be built.

Jamorie Consulting GmbH strongly recommends that Société Patrimoniale Jacques GmbH treat the findings of this assessment as a matter of operational urgency. A structured remediation roadmap should be developed prioritising the Login & Identity and Drive categories, with clear ownership assigned to each remediation action and a target timeline established for re-assessment. Engagement with Google Workspace administrators and relevant stakeholders will be essential to ensure that configuration changes are implemented in a controlled and documented manner. Jamorie Consulting GmbH remains available to support the remediation planning process and to conduct a follow-up assessment to validate progress against the identified findings.

84	26	53	5
Total Controls	**Passed**	**Failed**	**Manual Review**
assessed	31%	63%	6%

Compliance Score **32.9%**

Category Breakdown



2. Compliance Overview

Metric	Count	%
Total Controls	84	100%
Passed	26	31.0%
Failed	53	63.1%
Manual Review	5	6.0%
Other / Pending	0	0.0%
Compliance Score	32.9%	—

3. Findings — Failed Controls

53 control(s) with status: Failed

Access Management

4.2.1.1 · L2 **FAILED**

Ensure application access to Google services is restricted

Description
Prevent unrestricted application access to Google services.

Rationale
You can restrict (or leave unrestricted) access to most Workspace services, including Google Cloud Platform services such as Machine Learning. For Gmail and Google Drive, you can specifically restrict access to high-risk scopes (for example, sending Gmail or deleting files in Drive). While users are prompted to consent to apps, if an app uses restricted scopes and you haven't specifically trusted it, users can't add

it.

Impact
The potential impact associated with implementation of this setting is that any previously installed apps that you haven't trusted stop working and tokens are revoked. When a user tries to install an app that has a restricted scope, they're notified that it's blocked.

Assessment

Observed Value
All visible Google services (Drive, Gmail, Calendar, Contacts, Google Workspace Admin, Vault, Cloud Platform, Cloud Billing, Cloud Machine Learning, Apps Script Runtime) show 'Unrestricted' in the Access column.

Expected Value
All applicable Google Services should have 'Restricted' in the Access column.

Reasoning
The screenshot clearly shows the Google Services list under App Access Control, and every service visible (all 10 listed on of 1, covering 18 Google services total) has 'Unrestricted' access. The audit procedure requires all applicable Google Services to show 'Restricted' in the Access column, which is not the case here.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Security 3. Select Access and Data Control 4. Select API Controls, then select App access control 5. Under Overview, select MANAGE GOOGLE SERVICES 6. Select ALL applicable Google Services 7. Click Change access 8. Select Restricted: Only trusted apps can access a service

4.2.2.1 · L1 **FAILED**

Ensure blocking access from unapproved geographic locations

Description
Restrict access to selected Google applications by geographic location.

Rationale
Restricting access to known/approved geographic locations is a simple way to limit where attacks can originate from. Especially for smaller organizations that do not need global access to applications.

Impact
Valid/approved users traveling to a geographic region outside of those defined in the Access Level will not be able to access their applications.

Assessment

Observed Value
Context-Aware Access is only available for users with specific enterprise licenses.

Expected Value
An appropriate Access Level with geographic restrictions defined and assigned to Admin Console, Drives and Docs, Gmail, and Google Vault.

Reasoning
The screenshot displays the message 'Context-Aware Access is only available for users with specific enterprise licenses,' indicating the organization's license level is insufficient to use Context-Aware Access. As per the special instructions, this constitutes a FAIL because the required functionality is not available due to the license tier.

Remediation

To configure this setting via the Google Workspace Admin Console: Create an appropriate Access Level

1. Log in to https://admin.google.com as an administrator 2. Select Security 3. Select Access and Data Control 4. Select Context-Aware Access 5. Select Access levels 6. Select Create Access Level 7. Under Details - Name the Access Level (Suggested using a clear name - ex. "Restrict to USA") 8. Under Conditions - Select Basic 9. Under Condition 1 - Select Meet attributes 10. Under Condition 1 - Select Add Attribute 11. Click on the Add Attribute drop-down box and select Geographic origin 12. Click on the far right drop-down box and select the region, or regions, to be allowed (ex. United States) 13. Click Save

Assign the defined Access Level has been assigned to the application(s) that need the restriction

1. Log in to https://admin.google.com as an administrator 2. Select Security 3. Select Access and Data Control 4. Select Context-Aware

Access 5. Select Assign access levels 6. For each application listed that needs this restriction, select Assign 7. Under, Access is granted when a user meets conditions in at least one of the selected access levels, ensure the previously named Access Level (ex. "Restrict to USA") is checked 8. Also, ensure Apply to Google desktop and mobile apps is checked

NOTE: CIS recommends geographically restricting assess to the following Google applications at minimum:

1. Admin Console 2. Drives and Docs 3. Gmail 4. Google Vault

4.2.3.1 · L1 **FAILED**

Ensure DLP policies for Google Drive are configured

Description
Enabling Data Loss Prevention (DLP) policies for Google Drive allows organizations to control the content that users can share in Google Drive files outside the organization.

Rationale
Enabling DLP policies alerts users and administrators that specific types of data should not be exposed, helping to protect the data from accidental exposure. DLP gives you control over what users can share, and prevents unintended exposure of sensitive information such as credit card numbers or identity numbers

Impact
Configuring a DLP policy for Google Drive will detect or block sensitive information.

Assessment

Observed Value
Upgrade to Enterprise editions for access to automated data protection and more. (with 'GO TO SUBSCRIPTIONS' button visible, indicating DLP rules are not available at current subscription level)

Expected Value
Data protection rules exist and are enabled for Google Drive

Reasoning
The screenshot displays the message 'Upgrade to Enterprise editions for access to automated data protection and more.' along with a 'GO TO SUBSCRIPTIONS' button, which per the special instructions indicates the subscription level is insufficient to configure DLP rules, resulting in a FAIL.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Security 3. Select Access and Data Control 4. Select Data protection 5. Select Manage Rules 6. Select ADD RULE, then select either New rule or New rule from template

New rule Examples can be found here.

1. Set the rule Name 2. Optionally - Set the rule Description 3. Set the Scope as appropriate 4. Select Continue 5. Set Triggers by checking - File modified under Google Drive 6. Select ADD CONDITION and configure values (Field, Comparison Operator, Content to match) - Repeat as appropriate 7. Select Continue 8. Under Actions, select the desired action to take for each incident 9. Under Alerting, select the desired severity level 10. Under Alerting, Select - Send to alert center 11. Select Continue 12. Select Create

New rule from template

1. Select the desired rule template 2. Optionally set the Name as desired 3. Optionally set the `Description as desired 4. Set the Scope as appropriate 5. Select Continue 6. Modify preconfigured Conditions as desired, or add additional conditions 7. Select Continue 8. Under Alerting, Select - Send to alert center 9. Select Continue 10. Select Create

4.2.4.1 · L1 **FAILED**

Ensure Google session control is configured

Description
Configure Google Workspace's session control to strengthen session expiration.

Rationale

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. How the settings work on mobile devices varies by device and app.

Impact
The potential impact associated with implementation of this setting are:

• When a web session expires for a user, they see the Verify it's you page and must sign in again. • When you change the session length, users need to sign out and in again for settings to take effect. • If you set the session to never expire, users never have to sign in again. • If you need some users to sign in more frequently than others, place them in different organizational units. Then, apply different session lengths to them. That way, certain users won't be interrupted to sign in when it isn't necessary. • If a Google Meet meeting starts within 2 hours of a session's scheduled expiration, the user is forced to sign in again before the start of the meeting. This helps avoid an interruption to the meeting while in-progress. • If you're using a third-party identity provider (IdP), such as Okta or Ping, and you set web session lengths for your users, you need to set the IdP session length parameter to expire before the Google session expires. That way, your users will be forced to sign in again. If the third-party IdP session is still valid when the Google session expires, the Google session might be renewed automatically without the user signing in again.

Assessment

Observed Value
Enable DBSC checkbox is unchecked (disabled)

Expected Value
DBSC (Device Bound Session Credentials) must be enabled

Reasoning
The screenshot shows the Google Session Control page with the 'Enable DBSC' checkbox unchecked, meaning Device Bound Session Credentials are not enabled for the 'Edouard Jacques' organizational unit. Per the special instructions, DBSC must be enabled to pass this control.

Remediation

To verify this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Security 3. Select Access and Data Control 4. Select Google session control 5. Set Web session duration to 12 hours or less 6. Select Save

4.2.5.1 · L2 **FAILED**

Ensure Google Cloud session control is configured

Description
Configure Google cloud session control to strengthen session expiration.

Rationale
As an administrator, you can control how long different users can access the Google Cloud console and Cloud SDK without having to re-authenticate. For example, you might want users with elevated privileges, like project owners, billing administrators, or others with administrator roles, to re-authenticate more frequently than regular users. If you set a session length, they're prompted to sign in again to start a new session.

Impact
The potential impact associated with implementation of this setting are:

• When a Google cloud session expires for a user, they see the Verify it's you page and must sign in again. • If you require a security key, users who do not have one cannot use the GCP Console or Cloud SDK until they set it up. Once they have a security key, they can switch to using their password instead if they want.

If you're using a third-party identity provider (IdP):

• With the GCP Console—If you require a user to re-authenticate using their password, they're redirected to the identity provider (IdP). The IdP might not require the user to re-enter their password to start another console session, if the user already has a session active with the IdP—because they are using another application that caused the session to remain active. If a user must re- authenticate by touching their security key, they can do this while using the console. They will not be redirected to the IdP. • With the Cloud SDK—If a password is required for re-authentication, gcloud will require the user to execute the gcloud auth login command to renew the session. This will bring up a browser window, and the user will be taken to the IdP, where they may be prompted for credentials if there's no active session with the IdP. If a user must reauthenticate by touching their security key, they can do this on the Cloud SDK. They will not be redirected to the IdP.

Assessment

Observed Value
Reauthentication policy: 'Require reauthentication' is selected; Exempt Trusted apps: unchecked; Reauthentication frequency: 16 hours (recommended); Reauthentication method: Password (selected, not Security key)

Expected Value
Require reauthentication selected, Exempt Trusted apps unchecked, Reauthentication frequency: 16 hours (recommended), Reauthentication method: Security key

Reasoning
While 'Require reauthentication' is correctly selected, 'Exempt Trusted apps' is unchecked, and the frequency is correctly set to 16 hours (recommended), the Reauthentication method is set to 'Password' rather than the required 'Security key'. Since all conditions must be met for a PASS, this configuration fails.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Security 3. Select Access and Data Control 4. Select Google Cloud session control 5. Under Reauthentication policy, set Require reauthentication to selected and Exempt Trusted apps is unchecked 6. Set Reauthentication frequency to 16 hours (recommended) 7. Set Reauthentication method to Security key 8. Select Override

Admin

1.1.1 · L1 **FAILED**

Ensure more than one Super Admin account exists

Description
Having more than one Super Admin account is needed primarily so that a single point of failure can be avoided. Also, for larger organizations, having multiple Super Admins can be useful for workload balancing purposes.

Rationale
From a security point of view, having only a single Super Admin Account can be problematic if this user were unavailable for an extended period of time. Also, Super Admin accounts should never be shared amongst multiple users.

Impact
There should be no user impact, but Administrators should have a normal (low privilege) and an Administrative (high privilege) account.

Assessment

Observed Value
1 active Super Admin account found (superadmin@edouard-jacques.co)

Expected Value
More than 1 (at least 2) active Super Admin accounts must exist

Reasoning
The API evidence shows only 1 active Super Admin account exists in the organization. The CIS benchmark requires more than one Super Admin account to eliminate a single point of failure. The organization does not meet this requirement.

Remediation

Create at least one additional account with a Super Admin role. NOTE: A new account should be created vs adding this role to an existing account since Administration tasks should be done through separate Admin accounts.

1.2.1.1 · L1 **FAILED**

Ensure directory data access is externally restricted

Description
Configure Google Workspace's external directory sharing to prevent unrestricted directory data access.

Rationale
If your organization uses third-party apps that integrate with your Google services, you control how much Directory information the external apps can access. If you allow directory access, your users have a better experience with external apps. For example, when they use a third-party mail app, they want to find domain contacts and have email addresses automatically complete. The app needs access to Directory

data to make this happen. However, this has the ability to share ALL domain AND public data with the connected third-party app.

• Public data and authenticated user basic profile fields — Share publicly visible domain profile data with external apps and APIs. Also share the authenticated user's name, photo, and email address to enable Google Sign-In if the appropriate scopes are granted. Other non-public profile fields for the authenticated user aren't shared. All the non-public profile information of other users in the domain aren't shared. • Domain and public data — (Default) Share all Directory information that's shared with your domain and public data. This information includes profile information for users in your domain, shared external contacts, and Google+ profile names and photos.

Impact
The External directory sharing setting applies only to the following APIs and the Apps Scripts or third-party Marketplace apps that use those APIs:

• Google People API • Google CardDAV API • Google Contacts API v3

The setting applies only to third-party apps, such as iOS Mail and iOS Contacts (when enrolled on an iOS device via Add Account and then Google), third-party Contacts apps (on Android). The setting doesn't apply to Google products, including mobile apps, such as the following

• Gmail, Contacts (on Android), Inbox, Meet, and other Google mobile apps • iOS Mail and iOS Contacts using Google Sync (when enrolled on an iOS device through Add Account and then Exchange) • Workspace Sync for Microsoft Outlook

Assessment

Observed Value
Organization data and authenticated user basic profile fields (selected)

Expected Value
Public data and authenticated user basic profile fields (i.e., 'Domain and public data' must NOT be selected; the more restrictive option must be chosen)

Reasoning
The screenshot shows 'Organization data and authenticated user basic profile fields' is selected (blue radio button), which shares all Directory information within the organization including profile information and shared external contacts. The audit procedure requires that 'Domain and public data' is not selected and that the more restrictive 'Public data and authenticated user basic profile fields' (or equivalent) option is chosen instead. The currently selected option is broader than what the benchmark requires.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Open the collapsed menu via "hamburger button \ 3 horizontal lines" 3. Under Directory, select Directory settings 4. Under Sharing settings, select External Directory sharing 5. Select Public data and authenticated user basic profile fields

Calendar

3.1.1.1.2 · L2 **FAILED**

Ensure internal sharing options for primary calendars are configured

Description
Control how much calendar information users in your organization can share internally.

Rationale
In general, not everyone in the organization needs to know the schedule details of everyone else (operational security). Free/busy indication is enough for most people.

Impact
This will be the default for the user's primary calendar. The user can override this setting to allow other specific users greater visibility of their calendar.

Assessment

Observed Value
Share all information

Expected Value
Only free/busy information (hide event details)

Reasoning
The screenshot clearly shows the 'Internal sharing options for primary calendars' section with the radio button for 'Share all information' selected (filled blue circle), while 'Only free/busy information (hide event details)' is not selected. This does not meet the CIS Benchmark requirement.

Remediation
To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Calendar 5. Under Sharing settings, select Internal sharing options for primary calendars 6. Select Only free/busy information (hide event details) 7. Select Save

3.1.1.2.1 · L1 **FAILED**

Ensure external sharing options for secondary calendars are configured

Description
Control how much calendar information users in your organization can share externally.

Rationale
Prevent data leakage by restricting the amount of information is externally viewable when a user shares their calendar with someone external to your organization.

Impact
• Once you limit external sharing for your organization, users can't exceed these limits when sharing individual events. For example, if you limit your organization's external sharing to Free/Busy, events with Public visibility are only shared as Free/Busy. • External mobile users who previously synced events may keep seeing restricted details. That access stops when their device is wiped and re-synced. • If you lower the external sharing level, people outside your organization may lose access to calendars they could previously see.

Assessment

Observed Value
Share all information, but outsiders cannot change calendars

Expected Value
Only free/busy information (hide event details)

Reasoning
The screenshot clearly shows that 'Share all information, but outsiders cannot change calendars' is the selected radio button (filled blue circle) under External sharing options for secondary calendars. The required setting per the audit procedure is 'Only free/busy information (hide event details)', which is not selected.

Remediation
To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Calendar 5. Under General settings, select External sharing options for secondary calendars 6. Select Only free/busy information (hide event details) 7. Select Save

3.1.1.2.2 · L2 **FAILED**

Ensure internal sharing options for secondary calendars are configured

Description
Control how much calendar information users in your organization can share internally.

Rationale
In general, not everyone in the organization needs to know the schedule details of everyone else (operational security). Free/busy indication is enough for most people.

Impact
This will be the default for the user's secondary calendars. The user can override this setting to allow other specific users greater visibility of their calendars.

Assessment

Observed Value
Share all information

Expected Value

Only free/busy information (hide event details)

Reasoning
The screenshot clearly shows the 'Internal sharing options for secondary calendars' section with the radio button for 'Share all information' selected (filled blue circle), while 'Only free/busy information (hide event details)' is not selected. This does not meet the CIS benchmark requirement.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Calendar 5. Under General settings, select Internal sharing options for secondary calendars 6. Select Only free/busy information (hide event details) 7. Select Save

3.1.1.3.1 · L2 **FAILED**

Ensure calendar web offline is disabled

Description
Limit who is allowed offline calendar access.

Rationale
When enabled, users can turn on offline use for each computer they use. Data is stored on the computer until offline use is turned off by the user. In this case, the organization can lose control of where its data is stored (for this user). Care should be taken regarding which users and groups have this capability enabled.

Impact
Users will not be able to access their calendars offline.

Assessment

Observed Value
Allow using Calendar on the web when offline is checked (enabled)

Expected Value
Allow using Calendar on the web when offline is unchecked (disabled)

Reasoning
The screenshot clearly shows the 'Allow using Calendar on the web when offline' checkbox is checked (blue checkmark visible) under Calendar web offline in Advanced settings. The benchmark requires this checkbox to be unchecked to prevent offline calendar access.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Calendar 5. Under Advanced settings, select Calendar web offline 6. Set Allow using Calendar on the web when offline to unchecked 7. Select Save

Chat

3.1.4.4.1 · L1 **FAILED**

Ensure allow users to install Chat apps is disabled

Description
Control the use of Chat apps in spaces or direct messages to connect to services in Google Chat and look up information, schedule meetings, or complete tasks. Apps are accounts created by Google, users in your organization, or third parties.

Rationale
When a user interacts with an app in Chat, the app can see the user's email address, avatar, other basic user information, user locale, timezone, and interaction information. The app can also see the basic user information of other people in the chat, but it can't see their email address or avatar unless they also interact directly with the app. Chat apps that you install from the Google Workspace Marketplace can be made by developers from outside of your organization. Using these Chat app need to be carefully controlled (vetted and approved) since a malicious Chat app could allow the exfiltration of company proprietary information.

Impact
By default users will not be able to install Chat apps.

Assessment

Observed Value
Allow users to install Chat apps is ON

Expected Value
Allow users to install Chat apps is OFF

Reasoning
The screenshot clearly shows the 'Allow users to install Chat apps' setting with the 'ON' radio button selected (filled/blue), meaning users can install and run Chat apps created by Google, the organization, and third-party developers. The benchmark requires this setting to be OFF.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Chat and classic Hangouts 4. Select Chat apps 5. Under Chat apps access settings, set Allow users to install Chat apps to OFF 6. Select Save

3.1.4.4.2 · L1 **FAILED**

Ensure allow users to add and use incoming webhooks is disabled

Description
Allow users to configure incoming webhooks and developers to call incoming webhooks to post content. Incoming webhooks let you send asynchronous messages into Google Chat from applications that aren't Chat apps.

Rationale
Webhook usage should be carefully controlled (vetted and approved) since a malicious application could send bogus information to exposed webhooks and ultimately these users.

Impact
By default users will have exposed webhooks.

Assessment

Observed Value
Allow users to add and use incoming webhooks is ON

Expected Value
Allow users to add and use incoming webhooks is OFF

Reasoning
The screenshot clearly shows the 'Allow users to add and use incoming webhooks' setting with the ON radio button selected (filled blue circle), meaning users can add and use incoming webhooks. The benchmark requires this setting to be OFF.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Chat and classic Hangouts 4. Select Chat apps 5. Under Chat apps access settings, set Allow users to add and use incoming webhooks to OFF

Drive

3.1.2.1.1.2 · L1 **FAILED**

Ensure users cannot publish files to the web or make visible to the world as public or unlisted

Description
You should control the publishing of documents to the web or making them visable to the world as public or unlisted.

Rationale
Attackers will often attempt to expose sensitive information to external entities through sharing, and restricting the methods that your users can share documents with will reduce that surface area. This setting is only applicable if ON - Files owned by users in can be shared outside of . This applies to files in all shared drives as well is selected, but should be configured as described below to prevent unintentional document publishing.

Impact

Enabling this feature will prevent users from publishing documents on the web or making them visible to the world as public or unlisted files.

Assessment

Observed Value
The checkbox 'When sharing outside of Edouard Jacques is allowed, users in Edouard Jacques can make files and published web content visible to anyone with the link' is CHECKED (enabled).

Expected Value
The checkbox 'When sharing outside of is allowed, users in can make files and published web content visible to anyone with the link' must be UNCHECKED.

Reasoning
The screenshot clearly shows the 'ON - Files owned by users or shared drives in Edouard Jacques can be shared outside of Edouard Jacques' radio button is selected, and beneath it the checkbox for making files and published web content visible to anyone with the link is checked (blue checkbox). The audit procedure requires this checkbox to be unchecked to prevent users from publishing files to the web or making them publicly visible.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Drive and Docs 5. Under Sharing settings, select Sharing options 6. Under Sharing outside of - ON - Files owned by users in can be shared outside of . This applies to files in all shared drives as well, set When sharing outside of is allowed, users in can make files and published web content visible to anyone with the link to unchecked 7. Select Save

3.1.2.1.1.3 · L2 **FAILED**

Ensure document sharing is being controlled by domain with allowlists

Description
You should control sharing of documents to external domains by either blocking domains or only allowing sharing with specific named domains.

Rationale
Attackers will often attempt to expose sensitive information to external entities through sharing, and restricting the domains that your users can share documents with will reduce that surface area.

Impact
Enabling this feature will prevent users from sharing documents with domains outside of the organization unless allowed.

Assessment

Observed Value
ON - Files owned by users or shared drives in Edouard Jacques can be shared outside of Edouard Jacques (radio button selected). The ALLOWLISTED DOMAINS option is not selected.

Expected Value
ALLOWLISTED DOMAINS - Files owned by users in can be shared with Google Accounts in compatible allowlisted domains must be selected, AND 'Warn when files owned by users or shared drives in are shared with users in allowlisted domains' must be checked.

Reasoning
The screenshot clearly shows the 'ON' radio button is selected for sharing outside of the organization, not the 'ALLOWLISTED DOMAINS' option as required by the benchmark. The ALLOWLISTED DOMAINS radio button is unselected, meaning sharing is not being controlled by an allowlist. This fails the primary requirement of the control.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Drive and Docs 5. Under Sharing settings, select Sharing options 6. Under Sharing outside of , select ALLOWLISTED DOMAINS - Files owned by users in can be shared with Google Accounts in compatible allowlisted domains. 7. Set Warn when files owned by users or shared drives in are shared with users in allowlisted domains to checked 8. Select Save

3.1.2.1.1.4 · L2 **FAILED**

Ensure users are warned when they share a file with users in an allowlisted domain

Description
Warn the user when they try and share a file and/or shared drive with users in an allowlisted domain.

Rationale
The user may not realize the potential account is external to the organization. Providing a warning allows the user an opportunity to know this and possibly reassess this sharing.

Impact
None, except an additional warning. Sharing can still occur.

Assessment

Observed Value
ALLOWLISTED DOMAINS radio button is NOT selected (ON is selected instead). The 'Warn when files owned by users or shared drives in Edouard Jacques are shared with users in allowlisted domains' checkbox under ALLOWLISTED DOMAINS appears checked, but the ALLOWLISTED DOMAINS option itself is not the active/selected radio button.

Expected Value
ALLOWLISTED DOMAINS option must be selected AND the sub-setting 'Warn when files owned by users or shared drives in are shared with users in allowlisted domains' must be checked.

Reasoning
The audit procedure requires that the ALLOWLISTED DOMAINS radio button is selected and the warn sub-setting beneath it is checked. In the screenshot, the 'ON' radio button is selected (not ALLOWLISTED DOMAINS), meaning the ALLOWLISTED DOMAINS option is not the active sharing level. Although the warn checkbox under ALLOWLISTED DOMAINS appears checked, the primary ALLOWLISTED DOMAINS option is not selected, which means this control is not configured as required.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Drive and Docs 4. Select Sharing Settings 5. Select Sharing Options 6. Under Sharing outside of 7. Set ALLOWLISTED DOMAINS - Files owned by users or shared drives in BMDT-Group can be shared with Google accounts in compatible allowlisted domains. to checked. Also, set the sub-setting Warn when files owned by users or shared drives in are shared with users in allowlisted domains to checked. 8. Select Save

3.1.2.1.1.5 · L1 **FAILED**

Ensure Access Checker is configured to limit file access

Description
When a user shares a file via a Google product other than Docs or Drive (e.g. by pasting a link in Gmail), Google can check that the recipients have access. If not, when possible, Google will ask the user to pick how they want to share the file.

Rationale
In general, access should be restricted to the smallest group possible. In this case recipients only.

Impact
Only recipients can access files. Recipients cannot share access with others by forwarding the email/link.

Assessment

Observed Value
Recipients only, Edouard Jacques, or public (no Google account required). is selected

Expected Value
Recipients only. is checked

Reasoning
The Access Checker section shows the most permissive option 'Recipients only, Edouard Jacques, or public (no Google account required).' is selected (radio button filled), while the required setting is 'Recipients only.' which is visible but not selected. This does not meet the CIS benchmark requirement.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Drive and Docs 4. Select Sharing Settings 5. Select Sharing Options 6. Under Access Checker 7. Set Recipients only. to checked 8. Select Save

3.1.2.1.1.6 · L1 **FAILED**

Ensure only users inside your organization can distribute content externally

Description
You should control who is allowed to distribute organizational content to shared drives owned by another organization.

Rationale
Sharing and collaboration are key; however, only your users should have the authority over where company content is shared with to prevent unauthorized disclosures of information.

Impact
Only people in your organization with Manager access to a shared drive can move files from that shared drive to a Drive location in a different organization. In addition, users in the selected organizational unit or group can copy content from their My Drive to a shared drive owned by a different organization.

Assessment

Observed Value
Anyone is selected under 'Distributing content outside of Edouard Jacques'

Expected Value
Only users in (i.e., 'Only users in Edouard Jacques') should be selected

Reasoning
The screenshot clearly shows the 'Distributing content outside of Edouard Jacques' section with the 'Anyone' radio button selected, rather than the required 'Only users in Edouard Jacques' option. This does not meet the CIS Benchmark requirement.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Drive and Docs 5. Under Sharing settings, select Sharing options 6. Under Distributing content outside of , select - Only users in 7. Select Save

3.1.2.1.2.2 · L1 **FAILED**

Ensure manager access members cannot modify shared drive settings

Description
Only administrators should be able to modify shared drive settings.

Rationale
Allowing manager access members to override or modify shared drive settings can allow intentional and unintentional data access by unauthorized users.

Impact
Disabling this feature will prevent manager access members from modifying shared drive settings, requiring administrators to perform settings modifications as required.

Assessment

Observed Value
Allow members with manager access to override the settings below is checked (enabled)

Expected Value
Allow members with manager access to override the settings below is unchecked (disabled)

Reasoning
The screenshot clearly shows the checkbox for 'Allow members with manager access to override the settings below' is checked (blue checkbox), whereas the CIS benchmark requires this setting to be unchecked to prevent manager access members from modifying shared drive settings.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Drive and Docs 5. Select Sharing settings 6. Under Shared drive creation, set Allow members with manager access to override the settings below to unchecked 7. Select Save

3.1.2.1.2.3 · L1 **FAILED**

Ensure shared drive file access is restricted to members only

Description
Shared drive file access should be restricted to that shared drive's members

Rationale
Preventing unauthorized users from access sensitive data is paramount in preventing unauthorized or unintentional information disclosures.

Impact
Disabling this feature will prevent shared drive non-members from accessing content in shared drives where they are not a member.

Assessment

Observed Value
Allow people who aren't shared drive members to be added to files is checked (enabled)

Expected Value
Allow people who aren't shared drive members to be added to files is unchecked (disabled)

Reasoning
The screenshot clearly shows the checkbox for 'Allow people who aren't shared drive members to be added to files' is checked (blue checkmark visible), whereas the CIS benchmark requires this setting to be unchecked to restrict shared drive file access to members only.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Drive and Docs 5. Select Sharing settings 6. Under Shared drive creation, set Allow people who aren't shared drive members to be added to files to unchecked 7. Select Save

3.1.2.1.2.4 · L2 **FAILED**

Ensure viewers and commenters ability to download, print, and copy files is disabled

Description
limit what viewers/commenters on a shared document can do with it.

Rationale
In many cases when sharing a document it might be fine for the users to do what they want with the document on the shared drive (Download, Print, etc.). In more restricted environments these capabilities may need to be prevented (Protected Intellectual property, Personally Identifiable Information, etc.).

Impact
Users of this shared drive will be restricted to only reading and commenting on the existing files.

Assessment

Observed Value
Download, print, and copy is enabled for: 'Everyone (Managers, content managers, contributors, commenters and viewers)' is selected

Expected Value
Allow viewers and commenters to download, print, and copy files is unchecked (i.e., only Managers, content managers, and contributors or Managers only should be selected)

Reasoning
The screenshot shows the 'Download, print, and copy is enabled for' section with 'Everyone (Managers, content managers, contributors, commenters and viewers)' selected. This means viewers and commenters are allowed to download, print, and copy files, which violates the CIS benchmark requirement that this capability be restricted (unchecked/disabled) for viewers and commenters.

Remediation

To verify this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Drive and Docs 5. Select Sharing settings 6. Under Shared drive creation, set Allow viewers and commenters to download, print, and copy files to unchecked 7. Select Save

3.1.2.2.1 · L1 **FAILED**

Ensure offline access to documents is disabled

Description
Prevent documents from being locally accessible on an unconnected device.

Rationale
This setting prevents an organization's files from being stored locally, thus limiting data loss issues if the device is lost or stolen.

Impact
Copies of recent files are only synced and saved on devices if you've defined a managed policy to do so. NOTE: All users will lose access to offline documents on all devices if managed devices policies are not set. NOTE: Setting up policies to control offline access on individual devices is outside the scope of this Benchmark. Additional information om doing this for various device types can be found here.

Assessment

Observed Value
'Allow users to enable offline access (recommended)' is selected (radio button filled), while 'Control offline access using device policies' is unselected.

Expected Value
'Control offline access using device policies' should be checked/selected.

Reasoning
The screenshot clearly shows two radio button options under Offline settings. The second option 'Allow users to enable offline access (recommended)' is currently selected (blue filled radio button), while the first option 'Control offline access using device policies' is unselected (empty radio button). The benchmark requires 'Control offline access using device policies' to be selected, which is the opposite of what is observed.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Drive and Docs 5. Select Features and Applications 6. Select Offline 7. Set Control offline access using device policies. to checked 8. Select Save

3.1.2.2.2 · L1 **FAILED**

Ensure desktop access to Drive is disabled

Description
Prevent documents from being locally accessible on an unconnected device.

Rationale
This setting prevents an organization's files from being stored locally, thus limiting data loss issues if the device is lost or stolen. NOTE: The Google Drive desktop application has its own way of handling "Offline" files and does not obey the Drive and Doc > Offline > Control offline access using divide policies setting. Not allowing Google Drive for desktop on the device will prevent this channel.

Impact
The end user will not be able to use Google Drive for desktop and its convenient integration into the Windows file explorer.

Assessment

Observed Value
Allow users to access Google Drive with the Drive SDK API is checked (enabled)

Expected Value
Allow users to access Google Drive with the Drive SDK API is unchecked (disabled)

Reasoning
The screenshot clearly shows the Drive SDK checkbox 'Allow users to access Google Drive with the Drive SDK API' is checked (blue checkbox), but the audit procedure requires it to be unchecked to comply with this control.

Remediation

To verify this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Drive and Docs 5. Select Features and Applications 6. Select Google Drive for desktop 7. Set Allow Google Drive for desktop in your organization to unchecked 8.

Select Save

Gmail

3.1.3.2.1 · L1 **FAILED**

Ensure that DKIM is enabled for all mail enabled domains

Description
DKIM adds an encrypted signature to the header of all outgoing messages. Email servers that get signed messages use DKIM to decrypt the message header, and verify the message was not changed after it was sent.

Rationale
Spoofing is a common unauthorized use of email, so some email servers require DKIM to prevent email spoofing.

Impact
There should be no impact of setting up DKIM however, organizations should ensure appropriate setup to ensure continuous mail-flow.

Assessment

Observed Value
Domain 'edouard-jacques.co' has no DKIM TXT record found at 'google._domainkey.edouard-jacques.co'. dkim_found: false, txt_records: [].

Expected Value
A valid DKIM record must exist and be enabled for all mail-enabled domains.

Reasoning
The evidence clearly shows that the only domain ('edouard-jacques.co') has no DKIM DNS TXT record configured, with dkim_found set to false and an explicit error stating no DNS record was found. This means DKIM authentication is not enabled for the organization's mail-enabled domain, failing the benchmark requirement.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Gmail 5. Under Authenticate email, select - Generate new record 6. Under Select DKIM key bit length, select the appropriate key bit length 2048 is recommended if supported 7. Under Prefix selector (optional), enter the appropriate prefix selector 8. Use the text at TXT record value to update the DNS record at your domain host 9. Select Start Authentication

3.1.3.2.3 · L1 **FAILED**

Ensure the DMARC record is configured for all mail enabled domains

Description
For all email domains configured in Google Workspace, a corresponding Domain-Based Message Authentication, Reporting and Conformance (DMARC) record should be created. NOTE: There are a number of ways DMARC can be configured, this document presents a most basic method. For more information on setting up DMARC for Google Workspace please refer to the Google documentation.

• Help prevent spoofing and spam with DMARC • Tutorial: Recommended DMARC rollout

Rationale
DMARC works with Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) to authenticate mail senders and ensure that destination email systems trust messages sent from your domain. Spammers can spoof your domain or organization to send fake messages that impersonate your organization. DMARC tells receiving mail servers what to do when they get a message that appears to be from your organization, but doesn't pass authentication checks, or doesn’t meet the authentication requirements in your DMARC policy record. Messages that aren't authenticated might be impersonating your organization, or might be sent from unauthorized servers.

Impact
There should be minimal impact of setting up DMARC records however, organizations should ensure proper DMARC record setup as email could be flagged as spam if DMARC is not set up appropriately.

Assessment

Observed Value
No DMARC record found for domain 'edouard-jacques.co'. DNS lookup at '_dmarc.edouard-jacques.co' returned no record.

Expected Value

A TXT record with at minimum 'v=DMARC1; p=none; rua=mailto:' must exist at '_dmarc.' for all mail-enabled domains.

Reasoning
The API evidence confirms that the sole domain 'edouard-jacques.co' has no DMARC record configured (dmarc_found: false). The audit procedure requires a valid DMARC TXT record to exist for every mail-enabled domain, and this domain is listed in 'domains_without_dmarc', making this a clear failure.

Remediation

Configure the DNS record for each domain.

1. If all email in your domain is sent from and received by Google Gmail, add the following TXT record for the domain:

v=DMARC1; p=none; rua=mailto:

NOTE: This will likely need to be configured at your domain registrar (Godaddy, etc.).

3.1.3.3.1 · L1 **FAILED**

Enable quarantine admin notifications for Gmail

Description
Quarantines can help prevent spam, minimize data loss, and protect confidential information. They can also help moderate message attachments so users don’t send, open, or click something they shouldn’t.

Rationale
Admins should be notified periodically when messages are quarantined so they can take the appropriate actions.

Impact
Admins will begin receiving quarantine notifications as emails are quarantined.

Assessment

Observed Value
Notify periodically when messages are quarantined is unchecked

Expected Value
Notify periodically when messages are quarantined is checked for each quarantine

Reasoning
The screenshot shows the 'Edit quarantine' dialog for the Default quarantine, and the 'Notify periodically when messages are quarantined' checkbox is clearly unchecked. The audit procedure requires this checkbox to be checked for each quarantine.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Gmail 5. Under Manage quarantines, set Notify periodically when messages are quarantined to checked

As required, give appropriate users the Access Admin Quarantine and\or Access restricted quarantine roles

3.1.3.4.1.3 · L1 **FAILED**

Ensure protection against anomalous attachment types in emails is enabled

Description
As a Google Workspace administrator, you can protect incoming mail against phishing and harmful software (malware). You can also choose what action to take based on the type of threat detected.

Rationale
You should protect your users from potentially malicious attachments.

Impact
Users will be warned when they receive an anomalous attachment.

Assessment

Observed Value

Protect against anomalous attachment types in emails is unchecked

Expected Value
Protect against anomalous attachment types in emails is checked

Reasoning
The screenshot clearly shows the checkbox for 'Protect against anomalous attachment types in emails' is unchecked (empty checkbox), whereas the CIS benchmark requires it to be checked.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Gmail 5. Under Safety - Attachments, set Protect against anomalous attachment types in emails to checked 6. Select Save

3.1.3.4.3.1 · L1 **FAILED**

Ensure protection against domain spoofing based on similar domain names is enabled

Description
Moves domain spoofing emails to spam folder.

Rationale
You should protect your users from domain spoofing emails.

Impact
Domain spoofed emails will be moved to a user's spam folder.

Assessment

Observed Value
Protect against domain spoofing based on similar domain names: checked (ON); Action: Keep email in inbox and show warning (default)

Expected Value
Protect against domain spoofing based on similar domain names is checked AND Action is Move email to spam

Reasoning
While the checkbox for 'Protect against domain spoofing based on similar domain names' is checked, the action selected is 'Keep email in inbox and show warning (default)' rather than the required 'Move email to spam'. Both conditions must be met for a PASS, and the action setting fails to meet the benchmark requirement.

Remediation

To verify this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Gmail 5. Under Safety - Spoofing and authentication, set Protect against domain spoofing based on similar domain names to checked 6. Set Action to Move email to spam 7. Select Save

3.1.3.4.3.2 · L1 **FAILED**

Ensure protection against spoofing of employee names is enabled

Description
Moves employee spoofing emails to spam folder.

Rationale
You should protect your users from employee spoofing emails.

Impact
Employee spoofed emails will be moved to a user's spam folder.

Assessment

Observed Value
Protect against spoofing of employee names = checked; Action = Keep email in inbox and show warning (default)

Expected Value
Protect against spoofing of employee names = checked; Action = Move email to spam

Reasoning

While the 'Protect against spoofing of employee names' checkbox is checked (compliant), the action is set to 'Keep email in inbox and show warning (default)' rather than the required 'Move email to spam'. Since both conditions must be met for a PASS, this control fails.

Remediation

To verify this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Gmail 5. Under Safety - Spoofing and authentication, set Protect against spoofing of employee names to checked 6. Set Action to Move email to spam 7. Select Save

3.1.3.4.3.3 · L1 **FAILED**

Ensure protection against inbound emails spoofing your domain is enabled

Description
Moves inbound emails spoofing your domain to spam folder.

Rationale
You should protect your users from inbound company domain spoofing emails.

Impact
Inbound company domain spoofed emails will be moved to a user's spam folder.

Assessment

Observed Value
Protect against inbound emails spoofing your domain = checked; Action = Keep email in inbox and show warning (default)

Expected Value
Protect against inbound emails spoofing your domain = checked; Action = Move email to spam

Reasoning
While the 'Protect against inbound emails spoofing your domain' checkbox is checked (compliant), the action is set to 'Keep email in inbox and show warning (default)' rather than the required 'Move email to spam'. Since the action does not meet the benchmark requirement, the overall result is FAIL.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Gmail 5. Under Safety - Spoofing and authentication, set Protect against inbound emails spoofing your domain to checked 6. Set Action to Move email to spam 7. Select Save

3.1.3.4.3.4 · L1 **FAILED**

Ensure protection against any unauthenticated emails is enabled

Description
Displays a warning when any message is not authenticated (SPF or DKIM).

Rationale
You should protect your users from any emails that aren't authenticated (SPF or DKIM)

Impact
Emails that aren't authenticated (SPF or DKIM) display a warning message to the recipient.

Assessment

Observed Value
Protect against any unauthenticated emails = unchecked

Expected Value
Protect against any unauthenticated emails = checked

Reasoning
The screenshot clearly shows the 'Protect against any unauthenticated emails' checkbox is unchecked (empty checkbox) in the Spoofing and authentication section. The audit procedure requires this setting to be checked.

Remediation

To verify this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Gmail 5. Under Safety - Spoofing and authentication, set Protect against any unauthenticated emails to checked 6. Select Save

3.1.3.4.3.5 · L1 **FAILED**

Ensure groups are protected from inbound emails spoofing your domain

Description
If a group receives an email that is spoofing your domain it is sent to the spam folder.

Rationale
You should protect your groups from any emails that spoofing your domain.

Impact
Emails that are spoofing your domain and are received by a group are sent to the spam folder.

Assessment

Observed Value
Protect your Groups from inbound emails spoofing your domain: unchecked (checkbox not checked); Action: Keep email in inbox and show warning (default)

Expected Value
Protect your Groups from inbound emails spoofing your domain: checked; Action: Move email to spam

Reasoning
The screenshot shows the 'Protect your Groups from inbound emails spoofing your domain' checkbox is unchecked, and the action is set to 'Keep email in inbox and show warning (default)'. Both conditions fail the audit requirement, which requires the checkbox to be checked and the action set to 'Move email to spam'.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Gmail 5. Under Safety - Spoofing and authentication, set Protect your Groups from inbound emails spoofing your domain to checked 6. Set Action to Move email to spam 7. Select Save

3.1.3.5.1 · L2 **FAILED**

Ensure POP and IMAP access is disabled for all users

Description
POP and IMAP may allow users to access Gmail using legacy or unapproved email clients that do not support modern authentication mechanisms, such as multifactor authentication.

Rationale
Disabling POP and IMAP prevents use of legacy and unapproved email clients with weaker authentication mechanisms that would increase the risk of email account credential compromise.

Impact
If you have Apple iOS or Android device users in your organization and you turn IMAP off, let them know that they’re no longer syncing Google Workspace mail to the iOS or Android Mail app. They might not get a notification on their device. Additionally, new users can’t manually add the Google Account they use for work or school to the device. If your Google Workspace users want to use desktop clients, such as Microsoft Outlook and Apple Mail, to access their Google Workspace mail, you need to enable POP or IMAP access in the Google Admin console. You can enable access for everyone in your organization or only for users in specific organizational units.

Assessment

Observed Value
Enable IMAP access for all users is checked (enabled); Enable POP access for all users is checked (enabled)

Expected Value
Enable IMAP access for all users is unchecked (disabled); Enable POP access for all users is unchecked (disabled)

Reasoning

The screenshot clearly shows both 'Enable IMAP access for all users' and 'Enable POP access for all users' checkboxes are checked (blue checkmarks visible), meaning both POP and IMAP are currently enabled. The benchmark requires both to be unchecked/disabled.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Gmail 5. Under End User Access - POP and IMAP Access 6. Set Enable IMAP access for all users to unchecked 7. Set Enable POP access for all users to unchecked 8. Select Save

3.1.3.5.2 · L1 **FAILED**

Ensure automatic forwarding options are disabled

Description
You should disable automatic forwarding to prevent users from auto-forwarding mail.

Rationale
In the event that an attacker gains control of an end-user account they could create rules to ex-filtrate data from your environment.

Impact
Care should be taken before implementation to ensure there is no business need for case-by-case auto-forwarding. Disabling auto-forwarding to remote domains will affect all users and in an organization.

Assessment

Observed Value
Allow users to automatically forward incoming email to another address: CHECKED (enabled)

Expected Value
Allow users to automatically forward incoming email to another address is unchecked (disabled)

Reasoning
The screenshot clearly shows the 'Automatic forwarding' checkbox under End User Access is checked (blue checkbox), meaning users are allowed to automatically forward incoming email to another address. The benchmark requires this checkbox to be unchecked to prevent potential data exfiltration.

Remediation

To verify this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Gmail 5. Under End User Access - Automatic forwarding, set Allow users to automatically forward incoming email to another address to unchecked 6. Select Save

3.1.3.6.2 · L1 **FAILED**

Ensure spam filters are not bypased for internal senders

Description
You can configure your advanced Gmail settings to bypass, or not bypass, spam filters for messages received from internal senders.

Rationale
Turning off this setting reduces the risk of spoofing and phishing/whaling.

Impact
Your users will be better protected by filtering their email for spam and minimizing the chances for spoofing and phishing/whaling attacks.

Assessment

Observed Value
Bypass spam filters for internal senders. is checked (enabled)

Expected Value
Bypass spam filters for messages received from internal senders. is unchecked

Reasoning
The screenshot clearly shows the 'Bypass spam filters for internal senders.' checkbox is checked (blue checkbox) under 'Options to bypass filters and warning banners'. The CIS benchmark requires this checkbox to be unchecked to ensure spam filters are not bypassed for internal senders.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Gmail 5. Select Spam, phishing, and malware 6. Under Spam, select Configure 7. Set Bypass spam filters for messages received from internal senders. to unchecked 8. Select Save

3.1.3.7.1 · L1 **FAILED**

Ensure comprehensive mail storage is enabled

Description

Comprehensive mail storage ensures messages sent by other core services appear in users' sent folders and are therefore accessible to Vault.

Rationale

As an administrator, you can ensure that a copy of all sent or received messages in your domain—including messages sent or received by non-Gmail mailboxes—is stored in the associated users' Gmail mailboxes.

Impact

There are some important considerations to carefully review before enabling comprehensive mail storage:

• You should not enable comprehensive mail storage if you have compliance routing rules that change the recipient (and don’t want the original recipient to receive a copy of the email). • When you have the SMTP Relay service enabled, user mailboxes will keep a copy of the message in the sent folder (for example, when sending mail from a scanner) if comprehensive mail storage is enabled. This might cause accounts to exceed storage limits if your account's edition has storage limits. Compare editions. • You should enable comprehensive mail storage if you only use Gmail for the Vault feature and forward email to your on-premise mail server or other email provider.

Assessment

Observed Value

Checkbox 'Ensure that a copy of all sent and received mail is stored in associated users' mailboxes' is UNCHECKED (OFF)

Expected Value

Checkbox 'Ensure that a copy of all sent and received mail is stored in associated users' mailboxes' must be CHECKED (ON)

Reasoning

The screenshot clearly shows the Comprehensive mail storage section under Gmail Compliance settings. The checkbox for 'Ensure that a copy of all sent and received mail is stored in associated users' mailboxes' is visibly unchecked, meaning the feature is disabled. The benchmark requires this checkbox to be checked (enabled).

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Gmail 5. Select Compliance 6. Select Comprehensive mail storage 7. Set Ensure that a copy of all sent and received mail is stored in associated users' mailboxes to checked 8. Select Save

3.1.3.7.2 · L1 **FAILED**

Ensure 'Send email over a secure TLS connection' Is Enabled

Description

The default is that Gmail always tries to send messages over a secure TLS connection. If the receiving server doesn't use TLS, Gmail still sends messages with TLS but the connection isn't secure. This setting allows the option to require a CA-signed certificate, verify the hostname associated with the certificate, and test the TLS connection. A padlock image will appear next to the recipient address if the message will be sent with TLS. The padlock shows only for accounts with a Google Workspace subscription that supports S/MIME encryption. Google Workspace supports TLS versions 1.0, 1.1, 1.2, and 1.3.

Rationale

Transport Layer Security (TLS) encrypts email messages for security and privacy and prevents unauthorized access of messages when they're sent over internet connections.

Impact

This should not have an impact on the usage of Gmail.

Assessment

Observed Value
Inbound - all messages: unchecked; Outbound - all messages: unchecked

Expected Value
Inbound - all messages: checked (ON) and Outbound - all messages: checked (ON)

Reasoning
The screenshot shows the 'Add setting' dialog for Secure transport (TLS) compliance. Both 'Inbound - all messages' and 'Outbound - all messages' checkboxes are unchecked, which does not meet the benchmark requirement that both must be enabled (checked/ON).

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Gmail 5. Select Compliance 6. Select Secure transport (TLS) compliance 7. Select Configure 8. Set Inbound - all messages and Outbound - all messages to checked 9. Select Save

Note: Enabling the Inbound - all messages and Outbound - all messages configurations will also, by default, enable Require CA-signed certificate when delivering outbound messages to the TLS-enabled domains specified above. This is not a required configuration, but it is recommended.

Groups

3.1.6.2 · L1 **FAILED**

Ensure creating groups is restricted

Description
Control who is allowed to create Groups in your organization and if they can have external members.

Rationale
The organization should have some control over the organizational groups created and the purpose they are for.

Impact
In a large organization, this may cause too much burden on administrators.

Assessment

Observed Value
Creating groups: 'Anyone in the organization can create groups' is selected; 'Group owners can allow external members / Organization admins can always add external members' is unchecked; 'Group owners can allow incoming email from outside the organization' is unchecked

Expected Value
'Only organization admins can create groups' is selected; 'Group owners can allow external members / Organization admins can always add external members' is unchecked; 'Group owners can allow incoming email from outside the organization' is unchecked

Reasoning
The screenshot shows 'Anyone in the organization can create groups' is selected (filled radio button) instead of the required 'Only organization admins can create groups'. Although the two checkbox settings are correctly unchecked, the primary radio button setting fails the benchmark requirement, resulting in an overall FAIL.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Groups for Business 5. Select Creating groups 6. Select Only organization admins can create groups 7. Set Group owners can allow external members Organization admins can always add external members to unchecked 8. Set Group owners can allow incoming email from outside the organization to unchecked 9. Select Save

3.1.6.3 · L1 **FAILED**

Ensure default for permission to view conversations is restricted

Description
By default, only allow group members to view group conversations.

Rationale
Conversation viewing can always be expanded by exception for certain groups as needed (Need to know), but by default be restricted.

Impact
No practical impact, since Group members can view conversations in the Group.

Assessment

Observed Value
All organization users

Expected Value
All group members

Reasoning
The screenshot clearly shows the 'Default for permission to view conversations' section with 'All organization users' selected (blue radio button), whereas the CIS Benchmark requires 'All group members' to be selected. This is a less restrictive setting than required.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Groups for Business 5. Select Sharing options 6. Set Default for permission to view conversations to All group members 7. Select Save

Login & Identity

4.1.1.1 · L1 **FAILED**

Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users in administrative roles

Description
Enforce 2-Step Verification (Multi-Factor Authentication) for all users assigned administrative roles. These include roles such as:

• Help Desk Admin • Groups Admin • Super Admin • Services Admin • User Management Admin • Mobile Admin • Android Admin • Custom Admin Roles

Rationale
Add an extra layer of security to users accounts by asking users to verify their identity when they enter a username and password. 2-Step Verification (Multi-factor authentication) requires an individual to present a minimum of two separate forms of authentication before access is granted. 2-Step Verification provides additional assurance that the individual attempting to gain access is who they claim to be. With 2- Step Verification, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

Impact
Implementation of 2-Step Verification (multi-factor authentication) for all users in administrative roles will necessitate a change to user routine. All users in administrative roles will be required to enroll in 2-Step Verification using using phone, SMS, or an authentication application. After enrollment, use of 2-Step Verification will be required for future access to the environment.

Assessment

Observed Value
Enforcement is Off; New user enrollment period is None; Allow user to trust the device is present (state unclear but default is checked); Methods is set to 'Any'; settings are shown for the top-level org unit 'Edouard Jacques', not a dedicated admin roles group.

Expected Value
Enforcement is On; New user enrollment period is 2 weeks; Allow user to trust device is unchecked; Methods is 'Any except verification codes via text, phone call'; applied to a group containing ALL ADMIN ROLES.

Reasoning
The page text snippet clearly shows 'Enforcement: Off' for the Edouard Jacques organizational unit, which directly contradicts the requirement for Enforcement to be 'On'. Additionally, the New user enrollment period appears to be 'None' and the Methods setting shows 'Any' rather than 'Any except verification codes via text, phone call'. Furthermore, the settings are being reviewed at the top-level OU rather than a dedicated admin roles group, as the benchmark requires. Multiple required settings are non-compliant.

Remediation

To verify this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Go to Security and click on 2-Step Verification 3. Select the appropriate group with ALL ADMIN ROLES -- Create this group if needed 4. Under Authentication, set Allow users to turn on 2-Step Verification to checked 5. Set Enforcement to On 6. Set New user enrollment period is set to 2 weeks 7. Under Frequency, set Allow user to trust device to unchecked 8. Under Methods, set Any except verification codes via text, phone call to selected 9. Select Save

4.1.1.2 · L2 **FAILED**

Ensure hardware security keys are used for all users in administrative roles and other high-value accounts

Description
A hardware security key connects to a user's device using USB (A & C), Lightning, NFC, or Bluetooth connection. Also, many Android phones and Apple iPhones have built-in security keys accessible via Bluetooth and that can be assigned to a Google Workspace account. The purpose of a physical security key is to provide an additional security layer to high value accounts; in the event of a compromise of a user's credentials (username and password) without the associated security key, the authentication process cannot be successfully completed.

Rationale
The purpose of a physical security key is to provide an additional security layer to high value accounts; in the event of a compromise of a user's credentials (username and password) without the associated security key, the authentication process cannot be successfully completed. Hardware security keys help to protect high value accounts from targeted attacks, including phishing attempts. Adding a hardware security key requirement to your Google privileged accounts adds another layer of depth of protection greater than any other form of two-factor authentication.

Impact
Users with hardware security keys enabled will need to have physical access to the hardware key in order complete the authentication process and this will force users to adopt a practice of making sure that the physical key is available to them at any point in time that they need to be able to log in. If a hardware security key is lost or stolen, the impacted user can gain access to their Google account by using a backup MFA process and then remove the lost/stolen key and add another one. If a hardware security key is stolen, the user's account is not automatically compromised as the hardware key works in conjunction with the user's account credentials (username & password).

Assessment

Observed Value
Allow users to turn on 2-Step Verification: checked; Enforcement: Off; Methods: Any; 2-Step Verification policy suspension grace period: 1 day; Security codes: partially visible (Don't allow users to generate security codes radio button visible but selection unclear)

Expected Value
Allow users to turn on 2-Step Verification: checked; Enforcement: On or On from with valid date; Methods: Only security key; 2-Step Verification policy suspension grace period: 1 day; Security codes: Don't allow users to generate security codes

Reasoning
The Enforcement option is set to 'Off' instead of 'On' or 'On from' with a valid date, which is a clear failure. Additionally, under Methods, 'Any' is selected rather than 'Only security key'. Multiple required settings are not configured as specified by the benchmark.

Remediation
To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Go to Security and click on Authentication 3. Under Authentication, select 2-Step Verification 4. Select the option to Allow users to turn on 2-Step Verification 5. Under Enforcement, enable either 'On' or else 'On from' and configure a valid date 6. Under Methods, select Only security key to force the use of a security key 7. Under 2-Step Verification policy suspension grace period, select 1 day 8. Under Security codes, select Don't allow users to generate security codes 9. Select Save

4.1.1.3 · L1 **FAILED**

Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users

Description
Enforce 2-Step Verification (Multi-Factor Authentication) for all users.

Rationale
Add an extra layer of security to users accounts by asking users to verify their identity when they enter a username and password. 2-Step Verification (Multi-factor authentication) requires an individual to present a minimum of two separate forms of authentication before access is

granted. 2-Step Verification provides additional assurance that the individual attempting to gain access is who they claim to be. With 2- Step Verification, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

Impact
Implementation of 2-Step Verification (multi-factor authentication) for all users will necessitate a change to user routine. All users will be required to enroll in 2-Step Verification using using phone, SMS, or an authentication application. After enrollment, use of 2-Step Verification will be required for future access to the environment.

Assessment

Observed Value
Enforcement: Off; New user enrollment period: not selected (options shown but no selection visible); Allow user to trust the device: shown but state unclear; Methods: options shown but no selection visible. The page text shows the UI with Enforcement showing both 'Off' and 'On' options listed, but the current state appears to be 'Off' based on the UI rendering order and default context.

Expected Value
Allow users to turn on 2-Step Verification: checked; Enforcement: On; New user enrollment period: 2 weeks; Allow user to trust device: unchecked; Methods: Any except verification codes via text, phone call

Reasoning
The page text snippet clearly shows the Enforcement field listing 'Off' before 'On', indicating the current selection is 'Off' (the default), which directly violates the benchmark requirement that Enforcement be set to 'On'. Multiple other required settings (enrollment period, trust device, methods) cannot be definitively confirmed as compliant from the evidence. Since at minimum Enforcement appears to be Off rather than On, the control fails.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Security 3. Select 2-Step Verification 4. Under Authentication, check - Allow users to turn on 2-Step Verification 5. Set Enforcement to On 6. Set New user enrollment period to 2 weeks 7. Under Frequency, uncheck - Allow user to trust device 8. Under Methods, select - Any except verification codes via text, phone call 9. Select Save

4.1.2.1 · L2 **FAILED**

Ensure Super Admin account recovery is disabled

Description
This option allows Super Admin users to recover access to their accounts if their password has been forgotten. The option is not available if either Single Sign On or Password Sync is in use.

Rationale
Allowing Super Admins to recover access to their accounts when they have forgotten their passwords reduces the number of support tickets generated by users, and reduces the amount of down time spent waiting on the account recovery process to initiate and complete.

Impact
The potential impact to Super Admins being allowed to recover their accounts includes:

1. The Super Admins are now empowered to reset their passwords. 2. The Super Admins will no longer need to call a helpdesk or open a support ticket to regain access to their account.

An organization that allows users to recover their account will realize less time spent by administrative staff working on these tasks.

Assessment

Observed Value
Allow super admins to recover their account: ON

Expected Value
Allow super admins to recover their account is unchecked (OFF)

Reasoning
The screenshot clearly shows the 'Super admin account recovery' section with 'Allow super admins to recover their account' set to ON. The CIS benchmark requires this setting to be OFF (unchecked) to prevent super admins from self-recovering their accounts.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator. 2. Select Security. 3. Select Authentication. 4. Under Account recovery select Super admin account recovery. 5. Set Allow super admins to recover their account to unchecked 6. Click Save

4.1.2.2 · L1 **FAILED**

Ensure User account recovery is enabled

Description
This option allows non-Super Admin users to recover access to their accounts if their password has been forgotten. The option is not available if either Single Sign On or Password Sync is in use.

Rationale
Allowing users to recover access to their accounts when they have forgotten their passwords reduces the number of support tickets generated by users, and reduces the amount of down time spent waiting on the account recovery process to initiate and complete.

Impact
The potential impact to users being allowed to recover their accounts includes:

1. The user is now empowered to reset their passwords. 2. The user will no longer need to call a helpdesk or open a support ticket to regain access to their account.

An organization that allows users to recover their account will realize less time spent by administrative staff working on these tasks.

Assessment

Observed Value
Allow users and non-super admins to recover their account: OFF

Expected Value
Allow users and non-super admins to recover their account is checked (ON/enabled)

Reasoning
The screenshot clearly shows the 'User account recovery' section with 'Allow users and non-super admins to recover their account' set to OFF, whereas the CIS benchmark requires this setting to be enabled (ON/checked).

Remediation
To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator. 2. Select Security. 3. Select User account recovery 4. Select either the pencil icon or the setting itself. 5. Set Allow users and non-super admins to recover their account to checked. 6. Select Save.

4.1.3.1 · L2 **FAILED**

Ensure Advanced Protection Program is configured

Description
Enable Google's Advanced Protection Platform for all users and prevent the use of security codes where applicable.

Rationale
Sophisticated phishing tactics can trick the most savvy users into giving their sign-in credentials to attackers. Advanced Protection requires you to use a security key, which is a hardware device or special software on your phone used to verify your identity, to sign in to your Google Account. Unauthorized users won’t be able to sign in without your security key, even if they have your username and password. The Advanced Protection Program includes a curated group of high-security policies that are applied to enrolled accounts. Additional policies may be added to the Advanced Protection Program to ensure the protections are current. Advanced Protection allows you to apply all of these protections at once, and override similar settings you may have configured manually. These policies include:

• Strong authentication with security keys • Use of security codes with security keys (as needed) • Restrictions on third-party access to account data • Deep Gmail scans • Google Safe Browsing protections in Chrome (when users are signed into Chrome using the same identity as their Advanced Protection Program identity) • Account recovery through admin

Impact
User Impact

• You need your security key when you sign in for the first time on a computer, browser, or device. If you stay signed in, you may not be asked to use your security key the next time you log in. • Limits third-party app access to your data, puts stronger checks on suspicious

downloads, and tightens account recovery security to help prevent unauthorized access.

Security Keys - 2 Required

• Android: With an Android 7.0+ phone, you can enroll in a few taps by registering your phone's built-in security key. • iPhone: If you have an iPhone running iOS 10.0+, install the Google Smart Lock app to register your security key first, then enroll. • Two security keys are required for added assurance. If one key is lost or damaged, users can use the second key to regain account access.

Third-Party iDP

• You can use the Advanced Protection Program with accounts that federate from an IdP using SAML. When users with these accounts enroll in the Advanced Protection Program, we'll require security key use after the user signs in on the IdP. Note that SAML users can select Remember the device to avoid challenges on a browser or device.

Security Codes

• Before allowing users to generate security codes, carefully evaluate if your organization needs them. Using security keys with security codes increases the risk of phishing. However, if your organization has important workflows where security keys can't be used directly, enabling security codes for those situations may help improve your security posture overall.

Using 'Sign in with Google' with other apps and services

• You can still sign into apps and services with Google. If they request access to your Gmail or Drive data, access is denied.

Assessment

Observed Value
Enrollment: 'Enable user enrollment' is selected. Security Codes: 'Allow security codes without remote access' is selected.

Expected Value
Enrollment: 'Enable user enrollment' selected AND Security Codes: 'Do not allow users to generate security codes' selected.

Reasoning
While 'Enable user enrollment' is correctly selected, the Security Codes setting shows 'Allow security codes without remote access' is selected instead of the required 'Do not allow users to generate security codes'. Since both settings must be compliant for a PASS and the Security Codes setting fails, the overall result is FAIL.

Remediation

To verify this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Security 3. Select Advanced Protection Program 4. Under Enrollment - Allow users to enroll in the Advanced Protection Program, set Enable user enrollment to selected for the desired organizational unit or group 5. Under Security Codes, set Do not allow users to generate security codes to selected for the desired organizational unit or group 6. Select Save

4.1.4.1 · L2 **FAILED**

Ensure login challenges are enforced

Description
Configure Google Workspace to verify a user's identity post-sso.

Rationale
Many organizations use third-party identity providers (IdPs) to authenticate users who use single sign on (SSO) through SAML. The third-party IdP authenticates users and no additional risk-based challenges are presented to them. Any Google 2-Step Verification (2SV) configuration is ignored. This is the default behavior. You can set a policy to allow additional risk-based authentication challenges and 2SV if it's configured. If Google receives a valid SAML assertion (authentication information about the user) from the IdP during user sign-in, Google can present additional challenges to the user. Login challenges requires users have a recovery phone number or email account associated with their organizational account. If not previously configured, users will be prompted to enter this information periodically until provided. One login challenge option prompts users to enter their employee ID. This method is susceptible to information gathering attacks, should a list of employee IDs ever be leaked.

Impact
The potential impact associated with implementation of this setting is dependent upon the existing 2-Step Verification (2SV) polices.

• If you have existing 2SV policies, such as 2SV enforcement, those policies apply immediately. • Users affected by the new policy and who are enrolled in 2SV get a 2SV challenge at sign-in. • Based on Google sign-in risk analysis, users might see risk-based challenges at sign-in.

Assessment

Observed Value
Post-SSO verification (legacy SSO profile): 'Don't ask users for additional verifications from Google' is selected. Post-SSO verification (other SSO profiles): 'Ask users for additional verifications from Google if a sign-in or session behavior looks suspicious, and always apply 2-Step Verification policies (if configured)' is selected. Login challenges - Use employee ID to keep my users more secure: OFF.

Expected Value
Post-SSO verification: 'Logins using SSO are subject to additional verifications (if appropriate) and 2-Step Verification (if configured)' must be checked (i.e., the 'Ask users for additional verifications' option selected for ALL SSO profile types). Use employee ID to keep my users more secure: unchecked/OFF.

Reasoning
For the legacy SSO profile, 'Don't ask users for additional verifications from Google' is selected, which means post-SSO verification is not enforced for users signing in via the legacy SSO profile. The audit procedure requires that logins using SSO are subject to additional verifications for all applicable configurations. Since at least one SSO profile setting is non-compliant, the overall result is FAIL. The employee ID setting is correctly set to OFF.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Security 3. Select Login Challenges 4. Under Post-SSO verification, set Logins using SSO are subject to additional verifications (if appropriate) and 2-Step Verification (if configured) is checked 5. Select Save 6. Under Login challenges, set Use employee ID to keep my users more secure to unchecked 7. Select Save

4.1.5.1 · L1 **FAILED**

Ensure password policy is configured for enhanced security

Description
Configure Google Workspace Password Policy with a more secure length and is enforced upon next sign-in to protect against the use of common password attacks.

Rationale
Strong password policies protect an organization by prohibiting the use of weak passwords.

Impact
The potential impact associated with implementation of this setting is dependent upon the existing password policies in place in the environment. For environments that have strong password policies in place, the impact will be minimal. For organizations that do not have strong password policies in place, enhancing the password policy may require users to change passwords, and adhere to more stringent requirements than they have been accustomed to. Configuring passwords to expire at a 1 year mark ensures that users are not forced to change passwords so often that easily discerned patterns are used in the creation of the passwords. The day-to-day impact on users will be that they have to manage fewer passwords changing on a frequent basis. NOTE: Password should be changed immediately on any indication of system compromise, when a user role changes, and when a user leaves the organization.

Assessment

Observed Value
Enforce strong password: checked; Minimum length: 8; Enforce password policy at next sign-in: unchecked; Allow password reuse: unchecked; Password reset frequency: Never expires

Expected Value
Enforce strong password: checked; Minimum length: 14+; Enforce password policy at next sign-in: checked; Allow password reuse: unchecked; Password reset frequency: 365 Days

Reasoning
Multiple settings fail the benchmark requirements: the minimum password length is set to 8 (required: 14+), 'Enforce password policy at next sign-in' is unchecked (required: checked), and 'Password reset frequency' is set to 'Never expires' (required: 365 Days). Only 'Enforce strong password' and 'Allow password reuse' are correctly configured.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Security 3. Select Password management 4. Under Strength, set Enforce strong passwords to checked 5. Under Length, set Minimum Length to 14 or greater 6. Under Strength and Length enforcement, set Enforce password policy at next sign-in is checked 7. Under Reuse, set Allow password reuse to unchecked 8. Under Expiration, set Password reset frequency to 365 Days 9. Select Save

Meet/Marketplace

3.1.9.1.1 · L1 **FAILED**

Ensure users access to Google Workspace Marketplace apps is restricted

Description
Restrict what Google Marketplace apps a user can install.

Rationale
Users should only be allowed to install approved and vetted apps. This will limit the overall attack surface for the organization.

Impact
Users can only install approved Google Marketplace apps. This list will have to be created and maintained.

Assessment

Observed Value
Allow users to install and run any app from the Marketplace

Expected Value
Allow users to install and run only selected apps from the Marketplace

Reasoning
The screenshot clearly shows the first radio button 'Allow users to install and run any app from the Marketplace' is selected (filled/blue). The required setting per the benchmark is 'Allow users to install and run only selected apps from the Marketplace' (shown in the UI as 'Allow users to install and run allowlisted apps from the Marketplace'), which is not selected.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace Marketplace apps 4. Select Settings 5. Under Manage Google Workspace Marketplace allowlist access, set Settings to install third-party Google Workspace Marketplace apps: to Allow users to install and run only selected apps from the Marketplace 6. Select Save

Mobile & Alerts

6.1 · L1 **FAILED**

Ensure User's password changed is configured

Description
Configuring and enabling the setting that an alert will be generated when a user's password has changed.

Rationale
Ensuring that administrators are alerted when user passwords are changed provides organizations with the ability to detect and halt potential attacks involving credential compromise and account takeover.

Impact
This setting should have no impact on the end user but will send emails to super administrators when triggered.

Assessment

Observed Value
Alerts: Off, Severity: Low, Email Notifications: Off

Expected Value
Alerts: On, Severity: Medium (or higher), Email Notifications: On, Email notification recipients: All super administrators

Reasoning

The screenshot shows Alerts is set to Off, Severity is Low (below the required Medium), and Email Notifications is Off. All three observed values fail to meet the benchmark requirements.

Remediation

To verify this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator. 2. Select Rules 3. Under Google protects you by default select View list. 4. Scroll to User's password changed and select it. 5. Within the Actions pane, click the edit pencil on the right side of the pane. 6. Select Send to alert center (This will result in the alert being set to On). 7. Set the alert severity to Medium 8. To enable emails when this alert condition is met, select Send email notifications. Once enabled, the All super administrators option is selected by default. 9. Click Review to confirm the values. 10. Click Update Rule. 11. Confirm that the User's password changed shows an Alert status of On in the list.

6.4 · L1 **FAILED**

Ensure User granted Admin privilege is configured

Description
Configuring and enabling the setting that an alert will be generated when a user has been granted an admin privilege.

Rationale
Ensuring that administrators are alerted when a user is given increased privileges could be an indication of compromise unless this access has been approved.

Impact
This setting should have no impact on the end user but will send emails to super administrators when triggered.

Assessment

Observed Value
Alerts: Off, Severity: Low, Email Notifications: Off

Expected Value
Alerts: On, Severity: Medium (or higher), Email Notifications: On, Email notification recipients: All super administrators

Reasoning
The screenshot shows the 'User granted Admin privilege' rule with Alerts set to Off, Severity set to Low, and Email Notifications set to Off. All three visible settings fail to meet the benchmark requirements of Alerts: On, Severity: Medium, and Email Notifications: On.

Remediation

To verify this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator. 2. Select Rules 3. Under Google protects you by default select View list. 4. Scroll to User granted Admin privilege and select it. 5. Within the Actions pane, click the edit pencil on the right side of the pane. 6. Select Send to alert center (This will result in the alert being set to On). 7. Set the alert severity to Medium 8. To enable emails when this alert condition is met, select Send email notifications. Once enabled, the All super administrators option is selected by default. 9. Click Review to confirm the values. 10. Click Update Rule. 11. Confirm that the User granted Admin privilege shows an Alert status of On in the list.

Security Dashboard

4.3.2 · L1 **FAILED**

Ensure the Security health is reviewed regularly for anomalies

Description
As an administrator, the security health page enables you to monitor the configuration of your Admin console settings from one location. For example, you can check the status of settings like automatic email forwarding, device encryption, Drive sharing settings, and much more. Settings reported (Minimum, but could be many more depending on account type):

• Blocking of compromised mobile devices • Mobile management • Mobile password requirements • Device encryption • Mobile inactivity reports • Auto account wipe • Application verification • Installation of mobile applications from unknown sources • External media storage • Two-step verification for users • Two-step verification for admins • Security key enforcement for admins

Details on what each of these report entries mean can be found here. This report should be reviewed weekly. NOTE: The availability of each

individual report on the security dashboard depends on your Google Workspace edition. See Google documentation for more details.

Rationale
The security health page provides visibility into your Admin console settings to help you better understand and manage security risks. If needed, you can make adjustments to your domain's settings based on general security guidelines and best practices, while balancing these guidelines with your organization's business needs and risk management policy.

Impact
No user impact.

Assessment

Observed Value
Security advisor page shows multiple red (critical) anomalies: (1) 'In just a week, Workspace orgs like yours detected 149K+ phishing emails with enhanced security' (red alert icon), and (2) '1 user missing 2SV account protections' (red alert icon). Additionally, blue warning icons are present for 'Check options for improving data protection', 'Enhance app access protection', and 'Improve account security'.

Expected Value
Security Health page should be reviewed regularly and show no red anomalies indicating unresolved critical security issues.

Reasoning
The screenshot shows the Security advisor page with at least two red (critical) alert indicators: one regarding phishing email exposure and one indicating '1 user missing 2SV account protections'. Per the special instructions, red recommendations constitute anomalies that result in a FAIL. These unresolved critical issues indicate the security health is not in a compliant state.

Remediation

The remediation for any anomalies in the various settings varies widely (different sections of the Google Workspace Admin UI). Please refer to Google's documentation for specifics (here). NOTE: Many of these settings will be remedied by implementing other sections of this Benchmark. For example, an Admin not enrolled in 2-Step Verification can be remedied by implementing the Remediation procedure for the recommendation Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users in administrative roles.

Sites

3.1.7.1 · L1 **FAILED**

Ensure service status for Google Sites is set to off

Description
By default turn off Google Sites for all users.

Rationale
There is really no reason for every user within an organization to have access to Google Sites. If this capability is needed, it can be enabled and configured for those users and groups by exception as required by the organization to meet specific needs.

Impact
Users will not be have access to Google Sites.

Assessment

Observed Value
Service status is ON for everyone

Expected Value
Service status is OFF for everyone

Reasoning
The screenshot clearly shows the Service status for Google Sites is set to 'ON for everyone', both in the left panel status indicator and in the main Service status section. The benchmark requires it to be OFF for everyone.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select Sites 5. Select Service status 6. Set Service status to OFF for everyone 7. Select Save

Takeout

3.1.8.1 · L1 **FAILED**

Ensure access to external Google Groups is OFF for Everyone

Description
Control whether users in your organization can access external groups from their Google Workspace account. External groups are created outside your organization and might include a public community group or a group for a club a user belongs to. Control access to external groups by turning on or off the Google Groups additional service — a legacy service in your Admin console that does only one thing: It allows or blocks users from accessing external groups from their Google Workspace account. NOTE: This service has no effect on your organization's internal groups.

Rationale
In general, most of the organization's personnel do not need to assess external groups. They can be allowed by exception as needed by the business.

Impact
Users can't access external groups from their Google Workspace account. However, they do continue to receive email digests from groups they're already subscribed to when you turn off the service.

Assessment

Observed Value
ON for everyone

Expected Value
OFF for everyone

Reasoning
The screenshot shows the Google Groups service status is set to 'ON for everyone', both in the status card on the left and in the Service status section on the right. The CIS benchmark requires this service to be OFF for everyone to prevent users from accessing external Google Groups.

Remediation

To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Apps 3. Select Google Workspace 4. Select `Additional Google services 5. Scroll down to Google Groups 6. Set it to OFF for everyone 7. Select Save

4. Findings — Manual Review Required

5 control(s) with status: Manual Review

Access Management

4.2.1.2 · L2 **MANUAL REVIEW**

Review third-party applications periodically

Description
Weekly review connected applications for potential malicious or unintended access or connections.

Rationale
Performing a periodic review of connected applications and their permission scopes ensures only permitted and required applications can access organizational data or resources. Attackers commonly attempt to persuade or trick users to grant their application access to organizational data resources by asking for their consent.

Impact
None

Assessment

Observed Value
App Access Control page is visible showing: 'Configured apps' tab with an empty list (no apps listed), 'Apps pending review' section, 'Configured apps' section, and '3 Accessed apps' section. The configured apps list shows no entries.

Expected Value
All listed applications have been properly vetted and authorized by the appropriate personnel (periodic manual review required).

Reasoning
This control requires a manual, periodic review process to ensure all connected third-party applications are vetted and authorized — it is not a binary configuration setting. The screenshot shows the App Access Control page at the correct location, with no configured apps listed, but '3 Accessed apps' are noted. A human reviewer must verify whether those accessed apps have been periodically reviewed and authorized; this cannot be determined from the screenshot alone.

Remediation
To configure this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator 2. Select Security 3. Select Access and Data Control 4. Select API Controls, then select App access control 5. Under Overview, select MANAGE THIRD-PARTY APP ACCESS 6. Select Change Access for the application you wish to remove 7. Select Blocked: Can't access any Google service 8. Log in to the Google Cloud Platform - Resource Manager https://console.cloud.google.com/cloud-resource-manager as an administrator 9. Now Delete the desired application

Admin

1.1.3 · L1 **MANUAL REVIEW**

Ensure super admin accounts are used only for super admin activities

Description
Super admin accounts have access to all features in the Google Admin console and Admin API and can manage every aspect of your organization's account. Super admins also have full access to all users' calendars and event details. It is recommended to give each super administrator two accounts. One for their super admin account and a second account for daily activities. Users should only sign in to a super admin account to perform super admin tasks, such as setting up 2-Step Verification (2SV), managing billing and user licenses, or helping another admin recover their account. Super administrators should use a separate, non-admin account for day- to-day activities. Super admins should sign in as needed to do specific tasks and then sign out. Leaving super admin accounts sign-in can increase exposure to phishing attacks.

Rationale
Use the super admin account only when needed. Delegate administrator tasks to user accounts with limited admin roles. Use the least privilege approach, where each user has access to the resources and tools needed for their typical tasks. For example, you could grant an admin permissions to create user accounts and reset passwords, but not let them delete user accounts.

Impact
Super admin users will have to switch accounts as well as utilize login/logout functionality when performing administrative tasks.

Assessment

Observed Value
1 super admin account (superadmin@edouard-jacques.co) with 204 logins in the past 30 days, flagged for high login frequency suggesting routine use rather than task-specific access.

Expected Value
Super admin accounts should be used only for super admin tasks (not routine daily activities), with no user holding both Super Admin and Delegated Admin roles simultaneously. Admins should log in only as needed and log out after completing tasks.

Reasoning
The audit procedure specifically requires checking that no users hold both Super Admin and Delegated Admin roles simultaneously, but the evidence data does not contain role overlap information — it only captures login frequency data. While the high login count (204 in 30 days) strongly suggests the super admin account is being used for routine daily activities (which violates the spirit of the control), this is a behavioral inference, not the direct configuration check specified. A manual review is warranted to verify role assignments and confirm whether a separate non-admin account exists for daily use.

Remediation
For every Super admin that is also a Delegated admin account, either create a Delegated admin account for the user of elevate or their existing non-admin account to a Delegated admin account.

Marketplace & OAuth

5.1.1.1 · L1 **MANUAL REVIEW**

Ensure the App Usage Report is reviewed regularly for anomalies

Description

As an administrator, you can use Apps usage reports to get an in-depth understanding of how your users use Google Workspace apps. Fields Available:

• User • Gmail storage used (MB) • Drive storage used (MB) • Photos storage used (MB) • Total storage used (MB) • Storage used (%) • Classroom - last used time • Classes created • Posts created • Total emails • Emails sent • Emails received • Gmail (IMAP) - last used time • Gmail (POP) - last used time • Gmail (Web) - last used time • Files edited • Files viewed • Drive - last active time • Files added • Other types added • Google Docs added • Google Sheets added • Google Slides added • Google Forms added • Google Drawings added • Posts • +1s • +1s received • Comments • Comments received • Reshares • Reshares received • Search queries

• Search queries from web • Search queries from Android • Search queries from iOS

Details on what each of these fields mean can be found here. This report should be reviewed weekly. NOTE: In larger organizations reviewing this entire report weekly may not be possible. At a minimum, all Administrator and Super Administrator users should be reviewed, since they are a higher risk. These can be filtered from the overall user list.

Rationale

The App usage report can allow administrator to discover user that are potentially using application that they do not have access to and/or using in atypical ways.

Impact

No user impact.

Assessment

Observed Value

The Apps usage report is accessible and displays user data including Gmail storage used, Drive storage used, Photos storage used, Total storage used, Storage used (%), Classroom - last used time, Classes created, Posts created, and more columns for 3 users (Edouard Jacques, Invoice Edouard Jacques, Super Admin).

Expected Value

The App Usage Report should be reviewed regularly (at minimum weekly), with all users and fields displayed and reviewed for anomalies. The audit procedure requires navigating to Reporting > Reports > User Reports > App usage and reviewing displayed users and values for anomalies.

Reasoning

The screenshot confirms the administrator has successfully navigated to the correct App Usage report page (Reporting > User Reports > Apps usage) and the report is displaying user data with the required fields. However, this control requires a *process* determination — whether the report is reviewed regularly/weekly — which cannot be confirmed from a single screenshot. The screenshot only shows the report is accessible and populated, not that it is reviewed on a regular schedule.

Remediation

The remediation for any anomalies in the various fields varies widely (different sections of the Google Workspace Admin UI). Please refer to Google's documentation for specifics (here). NOTE: Many of these settings will be remedied by implementing other sections of this Benchmark. For example, an Admin showing recent Gmail (IMAP) - last used time and/or Gmail (POP) - last used time can be remedied by implementing the Remediation procedure for the recommendation Ensure POP and IMAP access is disabled for all users.

5.1.1.2 · L1 **MANUAL REVIEW**

Ensure the Security Report is reviewed regularly for anomalies

Description

As your organization's administrator, you can monitor your users' exposure to data compromise by reviewing the security report. Fields Available:

• User • External apps • 2-Step verification enrollment • 2-Step verification enforcement • Password length compliance • Password strength • User account status • Admin status • Security keys enrolled • Less secure apps access • Gmail (IMAP) - last used time • Gmail (POP) - last used time • Gmail (Web) - last used time • External shares • Internal shares • Public • Anyone with link • Outside domain • Anyone in domain shares • Anyone in domain with link shares • Within domain shares • Private shares

Details on what each of these fields mean can be found here. This report should be reviewed weekly. NOTE: In larger organizations

reviewing this entire report weekly may not be possible. At a minimum, all Administrator and Super Administrator users should be reviewed, since they are a higher risk. These can be filtered from the overall user list.

Rationale
The Security report provides a comprehensive view of how people share and access data and whether they take appropriate security precautions. For example, you can review who installs external apps, shares numerous files, skips 2-Step Verification, and uses security keys.

Impact
No user impact.

Assessment

Observed Value
The Security report under User Reports is visible and displays users (Edouard Jacques, Invoice Edouard Jacques, Super Admin) with columns including External apps, 2-Step verification enrollment, 2-Step verification enforcement, 2-Step verification protection, Password length compliance, Password strength, User account status, and Passkey. Notable anomaly: 'Invoice Edouard Jacques' shows 'Not enrolled' for 2-Step verification enrollment.

Expected Value
The Security report should be reviewed regularly (at minimum weekly) for anomalies across all listed fields. The audit procedure requires the administrator to review displayed users and values for anomalies.

Reasoning
This control is procedural in nature — it requires that the Security report be reviewed regularly (weekly), not just that it exists or is accessible. The screenshot confirms the report is accessible and being viewed, but there is no way to determine from a screenshot alone whether this review is performed on a regular/weekly basis. Additionally, a potential anomaly is visible (Invoice Edouard Jacques not enrolled in 2-Step verification), which may require follow-up action. A definitive PASS or FAIL cannot be determined from a single screenshot.

Remediation

The remediation for any anomalies in the various fields varies widely (different sections of the Google Workspace Admin UI). Please refer to Google's documentation for specifics (here). NOTE: Many of these settings will be remedied by implementing other sections of this Benchmark. For example, an Admin not enrolled in 2-Step Verification can be remedied by implementing the Remediation procedure for the recommendation Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users in administrative roles.

Security Dashboard

4.3.1 · L1 **MANUAL REVIEW**

Ensure the Dashboard is reviewed regularly for anomalies

Description
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 7 days. You can customize the dashboard to view data from Today, Yesterday, This week, Last week, This month, Last month, or Days ago (up to 180 days). Charts/reports available (Minimum, but could be many more depending on account type):

• DLP incidents • Top policy incidents • Failed device password attempts • Compromised device events • Suspicious device activities • OAuth scope grants by product (beta customers only) • OAuth grant activity • OAuth grants to new apps • User login attempts – Challenge method • User login attempts – Failed • User login attempts – Suspicious

Details on what each of these charts/reports mean can be found here. This report should be reviewed weekly. NOTE: The availability of each individual report on the security dashboard depends on your Google Workspace edition. See Google documentation for more details. NOTE: In larger organizations reviewing this entire report weekly may not be possible. At a minimum, all Administrator and Super Administrator users should be reviewed, since they are a higher risk. These can be filtered from the overall user list.

Rationale
The Security report provides a comprehensive view of how people share and access data and whether they take appropriate security precautions. For example, you can review who installs external apps, shares numerous files, skips 2-Step Verification, and uses security keys.

Impact
No user impact.

Assessment

Observed Value

User Reports > Security page is displayed with 3 users (Edouard Jacques, Invoice Edouard Jacques, Super Admin) showing columns: External apps, 2-Step verification enrollment, 2-Step verification enforcement, 2-Step verification protection, Password length compliance, Password strength, User account status, Passkey. One user (Invoice Edouard Jacques) shows 'Not enrolled' for 2-Step verification and 'Not protected' for 2-Step verification protection.

Expected Value

The Security User Report should be reviewed regularly (weekly) for anomalies across all displayed users and fields. The audit procedure requires a human reviewer to assess the data for anomalies rather than checking a specific configuration value.

Reasoning

This control requires a periodic human review of the security dashboard rather than verifying a specific configuration setting. The screenshot confirms the correct page is being accessed (Reports > User Reports > Security), and the report is displaying user data. However, whether the report is being reviewed 'regularly' (weekly) is a procedural/policy question that cannot be determined from a single screenshot alone — it requires evidence of recurring review practices, making this a MANUAL_REVIEW.

Remediation

The remediation for any anomalies in the various fields varies widely (different sections of the Google Workspace Admin UI). Please refer to Google's documentation for specifics (here). NOTE: Many of these settings will be remedied by implementing other sections of this Benchmark. For example, an Admin not enrolled in 2-Step Verification can be remedied by implementing the Remediation procedure for the recommendation Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users in administrative roles.

5. Compliant Controls

26 control(s) passed.

ID	Title	Category	Level
1.1.2	Ensure no more than 4 Super Admin accounts exist	Admin	L1
3.1.1.1.1	Ensure external sharing options for primary calendars are configured	Calendar	L1
3.1.1.1.3	Ensure external invitation warnings for Google Calendar are configured	Calendar	L1
3.1.2.1.1.1	Ensure users are warned when they share a file outside their domain	Drive	L1
3.1.2.1.2.1	Ensure users can create new shared drives	Drive	L1
3.1.3.1.1	Ensure users cannot delegate access to their mailbox	Gmail	L1
3.1.3.1.2	Ensure offline access to Gmail is disabled	Gmail	L1
3.1.3.2.2	Ensure the SPF record is configured for all mail enabled domains	Gmail	L1
3.1.3.4.1.1	Ensure protection against encrypted attachments from untrusted senders is enabled	Gmail	L1
3.1.3.4.1.2	Ensure protection against attachments with scripts from untrusted senders is enabled	Gmail	L1
3.1.3.4.2.1	Ensure link identification behind shortened URLs is enabled	Gmail	L1
3.1.3.4.2.2	Ensure scan linked images for malicious content is enabled	Gmail	L1
3.1.3.4.2.3	Ensure warning prompt is shown for any click on links to untrusted domains	Gmail	L1
3.1.3.5.3	Ensure per-user outbound gateways is disabled	Gmail	L1
3.1.3.5.4	Ensure external recipient warnings are enabled	Gmail	L1
3.1.3.6.1	Ensure enhanced pre-delivery message scanning is enabled	Gmail	L1
3.1.6.1	Ensure accessing groups from outside this organization is set to private	Groups	L1
4.2.1.3	Ensure internal apps can access Google Workspace APIs	Access Management	L1
4.2.1.4	Review domain-wide delegation for applications periodically	Access Management	L2
4.2.6.1	Ensure less secure app access is disabled	Access Management	L1
6.2	Ensure Government-backed attacks is configured	Mobile & Alerts	L1

6.3	Ensure User suspended due to suspicious activity is configured	Mobile & Alerts	L1
6.5	Ensure Suspicious programmatic login is configured	Mobile & Alerts	L1
6.6	Ensure Suspicious login is configured	Mobile & Alerts	L1
6.7	Ensure Leaked password is configured	Mobile & Alerts	L1
6.8	Ensure Gmail potential employee spoofing is configured	Mobile & Alerts	L1