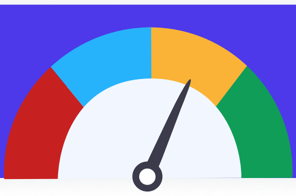
Google Workspace Auditing Task List



This guide outlines key steps to audit and secure your domain, based on our recommended best practices. Remember, each organization has unique needs, so consider this a **starting point.**

Why Audit?

- Maintain security and comply with regulations (e.g., SOC II, ISO 27001, CIPA).
- Gain control and visibility of your Google Workspace environment.

This Guide Will Help You:

- Configure alerts for suspicious activity.
- Take action to address issues.
- Report findings as needed.

1. Access Management Audit:

An Access Management Audit verifies user permissions, removes inactive accounts, and monitors external document sharing for compliance.

□ Review user accounts to ensure that only authorized personnel have access.

□ Verify that former employees or non-active users are suspended, archived or deleted.

□ Check for any external sharing of internal documents and ensure it complies with company policies.

2. Administrator Role Audit:

Ensures only authorized personnel possess elevated access and tracks their activity to maintain security and accountability.

□ Ensure that only a few trusted individuals have administrative access.

□ Review the list of admins periodically and adjust their permissions according to their job requirements.

3. Security Audit:

A Security Audit comprehensively evaluates Google Workspace settings and configurations to identify and address potential vulnerabilities.

□ Check the security dashboard for any suspicious activity.

□ Set up alerts for unusual activities, like an unexpected increase in file sharing or login attempts from unusual locations.

□ Ensure 2-factor authentication is enabled for all users.

□ Regularly update the password policies and enforce strong password requirements.

4. Application Audit:

Scrutinizes third-party and custom apps for authorized use, permissions, compliance, and security risks.

□ Assess third-party apps connected to your Google Workspace and revoke any that are unnecessary or not compliant with your security standards.

□ Regularly review API permissions for any unusual or unauthorized access.

5. Drive and Shared Drives Audit:

Examines file access, ownership, sharing settings, and content compliance for data security and governance.

□ Review sharing settings to ensure sensitive information is not shared with the wrong people or groups.

□ Audit files in Drive to check for proper ownership, especially for users who have left the organization

6. Email Compliance and Security Audit:

Examines routing, authentication, and forwarding to ensure data protection, prevent spoofing, and minimize leakage.

□ Review email routing and delivery settings to ensure compliance with data protection laws.

□ Check for proper email authentication with SPF, DKIM, and DMARC records to prevent email spoofing.

□ Audit any email forwarding rules to prevent data leakage.

7. Compliance Audit:

Evaluates configurations, user activity, and data handling against relevant regulations and internal policies.

□ If your organization is subject to regulations like GDPR, HIPAA, etc., ensure that your Google Workspace settings comply with these standards.

□ Use Google Vault to set up retention policies and legal holds appropriately.

8. Training and Policy Audit:

Verifies effectiveness of security training and assesses employee compliance with security policies, identifying areas for improvement.

□ Ensure that all users are trained on how to use Google Workspace securely.

□ Make sure your organization's policies for data handling are up-to-date and aligned with features and services provided by Google Workspace.

9. Use Google Workspace Audit Logs:

Gain insights into user actions and system events to strengthen security, accountability, and data governance.

□ Utilize the reports and audit logs provided by Google Workspace to get insights into various aspects of your environment, such as login activity, Admin activity, OAuth Token activity, etc.

10. Regular Reviews:

Prevent issues before they arise: Conduct regular reviews of access, activity, and settings.

□ Conduct regular audits to ensure ongoing compliance and security—quarterly or biannually, depending on the size and nature of your organization.

Auditor Name: ______________________ Date: ____________