GAT labs

Annual Auditing Guide

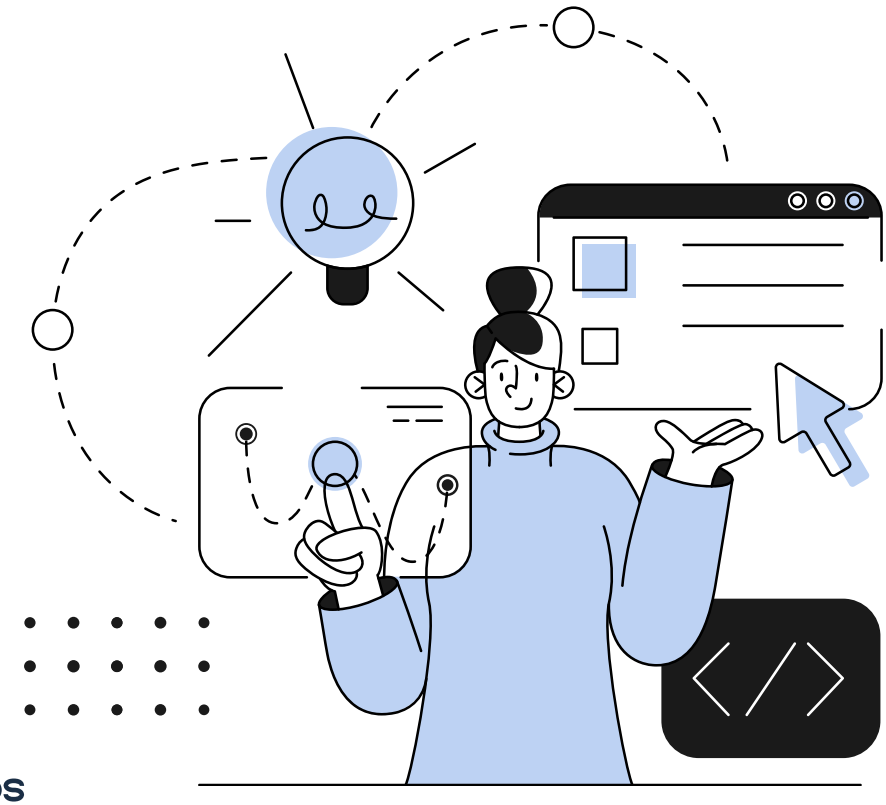
For Enterprises

Audits are an important part of keeping your Google Workspace secure, compliant, and organised. Many organisations choose to conduct audits annually, though the timing often depends on their internal schedules or compliance needs—it could be in April, July, or any other time of the year. No matter when it happens, Google Admins play a key role in protecting their Workspace from risks, meeting regulatory requirements, and ensuring everything runs smoothly.

This guide will help you review your Workspace step-by-step. It includes best practices for compliance, user management (like handling suspended accounts), and data security. You'll also discover how GAT tools can make these tasks faster and easier, so your organisation is ready for the year ahead.

Why Regular Audits Matter (and How a Year-End Review Helps)

Keeping your Workspace secure isn't a one-time task—it's something that needs regular attention throughout the year. Still, setting aside time for a more detailed audit at least once a year is important. It gives you the chance to review everything thoroughly, fix any gaps, and ensure sensitive data is protected while staying compliant with important regulations.



1. Compliance Audits for a Clean Start

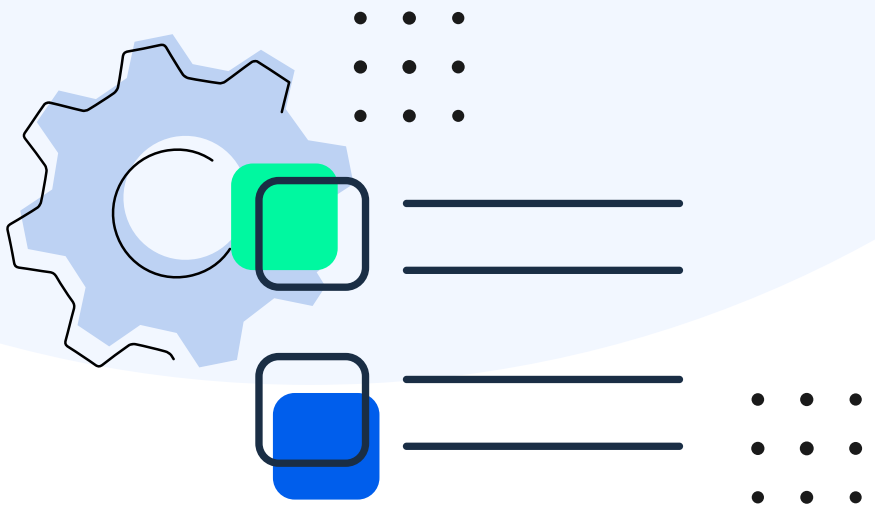
Staying compliant with industry standards like ISO 27001, SOC2, GDPR, HIPAA, and others can be challenging. GAT Labs offers compliance-focused tools that allow you to proactively spot and address vulnerabilities.

- **Compliance Check on Shared Files with GAT+**
  Ensure all shared files comply with your organisation's policies by reviewing permissions across Google Drive. GAT+ enables you to audit file-sharing settings, identify at-risk files, and adjust access to sensitive information.

  Learn How To Find and Take Actions on Externally Shared Files

- **Data Loss Prevention (DLP) for Compliance**
  Set up DLP alerts to monitor user activity and automatically block or alert on attempts to share sensitive information externally, such as credit card numbers or any other data that's important to your organisation with custom rules.

  Learn How to Create a Policy for Any Given File or Folder

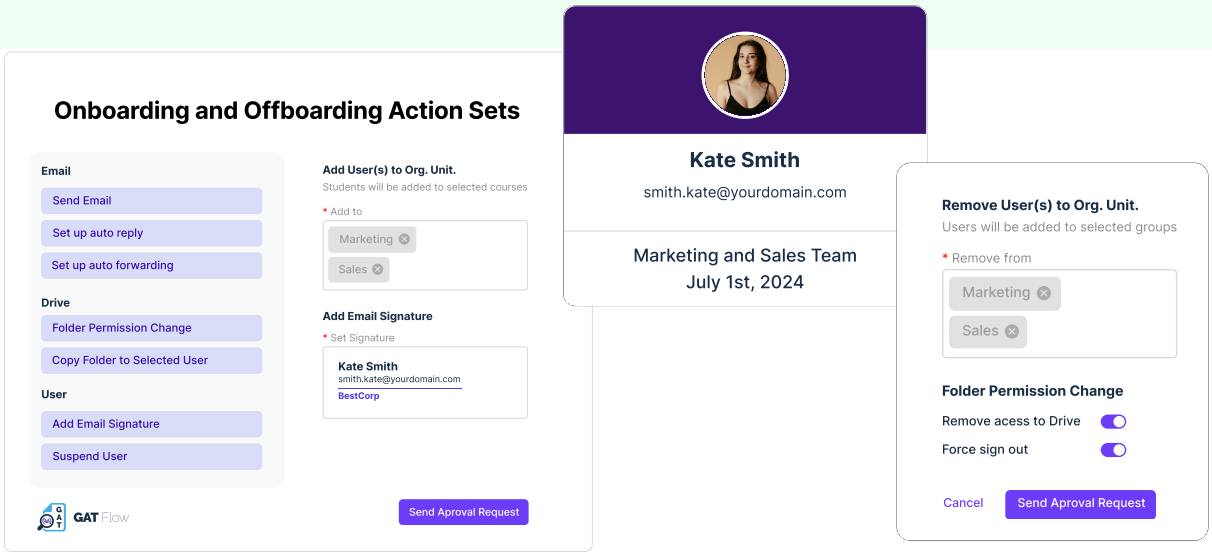


2. Suspended Users: Securing Data & Clean-up Permissions

Although suspended users can no longer access Drive, their sharing permissions and files remain intact. It's good practice to review and clean up unnecessary permissions to keep ACL's (Access Control Lists) current.

- **Transferring Suspended Users Data with GAT Flow**
  To prevent potential data loss when these users are deleted, ensure that any critical files they own are transferred to other users in your organisation. GAT Flow automates offboarding, ensuring your organisation's data is never lost.

  Learn How to Select and Take Actions on Suspended Users



- **Clean-up Suspended Users Permissions with GAT Unlock**
  Unlock lets you quickly change and revoke permissions for suspended users, ensuring your permissions are kept up to date and making it easier for admins and end-users alike to review sharing permissions when required.

  Learn How To Transfer Files Ownership Of A Suspended User

3. Identifying Inactive Accounts

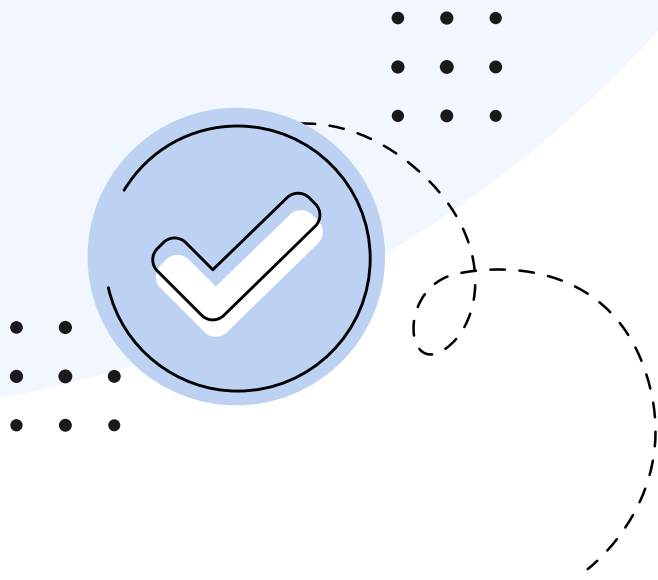
Inactive accounts pose a large risk, as they may be accessible to people who are no longer part of your organisation and slip through the cracks of your regular offboarding processes. It's important to identify these accounts and secure them to prevent any unauthorised access to your data.

- **Review user's last login time**
  Review last login time for all users in your domain and identify any accounts that have not been logged in for more than 30 days. It's important to cross-reference this list with other data sources as some accounts may still be active such as users on annual leave or maternity leave.

  Learn How to Set Up User Login Alerts

- **Cross-reference with Drive/Gmail activity and HR**
  Review users Gmail and Drive activity to determine the last time they were active. Some users may only access these services on mobile or using 3rd party clients, and last login time may not reflect this behaviour. Consider consulting your HR team to verify users current status.

  Learn How To Schedule Report For Email Activity



4. File Ownership and Access Management

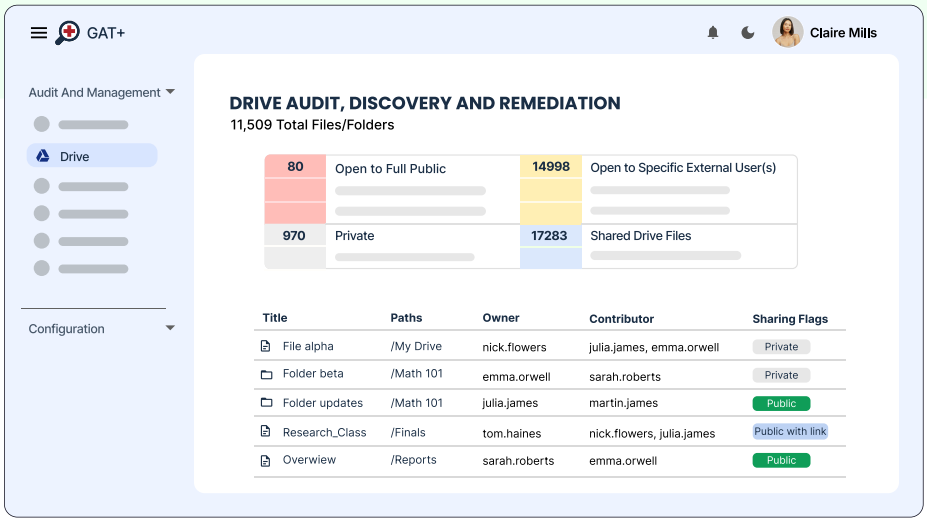
For users who frequently collaborate with external users, it's important to verify your data is being handled correctly. GAT+ helps you ensure all files are managed properly and reduce the risk of data breaches.

- **Review Externally Shared Files**
  Using GAT+ you can run detailed audits to identify files which are shared externally and verify if these permissions are still required. Using Unlock's File Management request you can notify your users of externally shared files they own and revoke permissions when required.

  Learn How To Change Ownership Of A Google Drive File

- **Review Files Shared In**
  Run a comprehensive audit of files shared into your domain using GAT+ and identify files that are accessible to your users but not owned by your domain. You may find files that should not be accessible or identify files that need to be copied into your domain, for example, a user sharing business data from their personal Google Drive account to their Workspace account.

  Learn to Remove External Sharing on Sensitive Files



5. Security Monitoring: Year-End Review and Real-Time Protection

The end of the year is a prime time to review security protocols and monitor for unusual activity that could indicate a breach or risk.

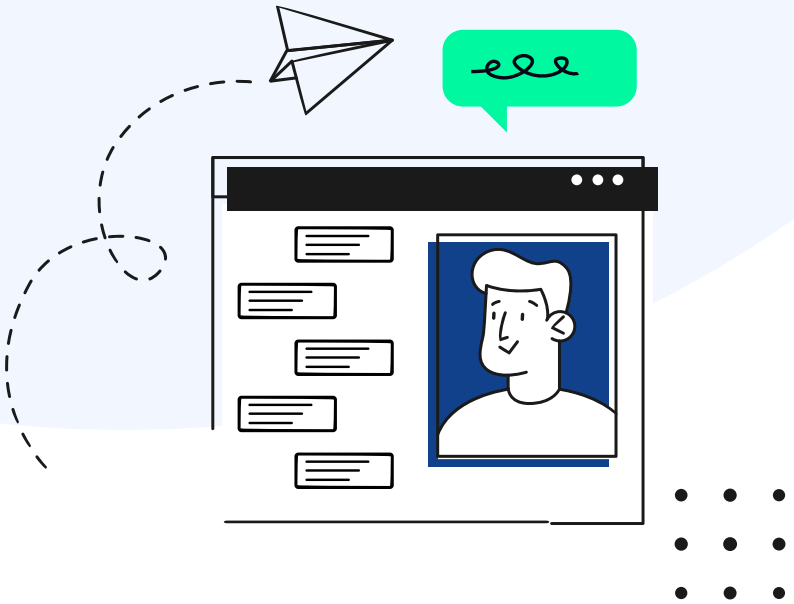
- **Real-Time Security Monitoring with GAT Shield**
  Set up GAT Shield to monitor Chrome activity, detect high-risk actions, and receive alerts to address threats proactively.

  Learn How to Audit Chrome Extensions

- **Setting Up Year-End Audit Reports**
  Compile audit reports on key metrics like file sharing and user access to provide stakeholders with a comprehensive security overview. GAT+ allows you to schedule these reports via the query filter button in any audit menu, automating regular exports based on applied filters.

  For example, in the Files tab of the Drive audit menu, you can schedule reports on externally shared files.

  Lear How to Create Scheduled Reports in Drive Audit



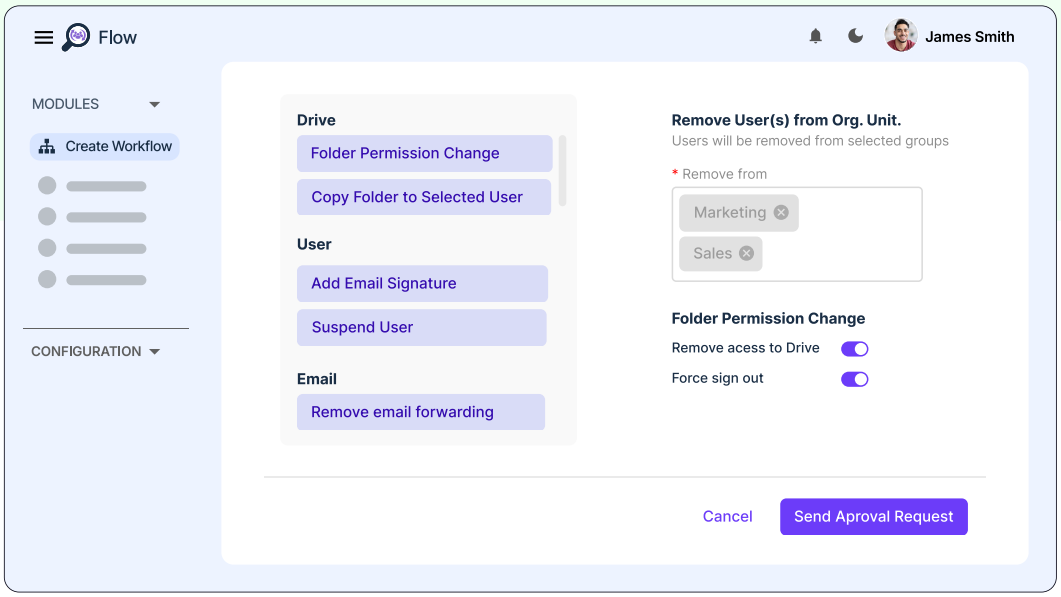
6. Customised Workflows for Data Management

Automate permissions and user updates with GAT Flow, reducing mismanagement risks and streamlining admin tasks.

- **Automate Permissions with GAT Flow**

  Create workflows to manage permission assignments or removals across departments, reducing manual work and ensuring permissions are correctly managed. With Flow roles in GAT Flow, Google Workspace admins can precisely control what non-admin users can do, adding an extra layer of security.

Learn How to Define Flow Role Permissions



Best Practices for Your Annual Auditing in Google Workspace

In addition to tool-based solutions, these best practices help every Google Admin conduct a thorough year-end audit:

- **Configure Sharing Policies**

  Use GAT+ to scan for sensitive or outdated data, helping you clean up unnecessary files. With GAT+, admins can also create policies for specific files or folders, automatically removing external users if files are shared outside the organisation—ensuring data remains secure within your domain.

  Learn How to Create a Policy for Any Given File or Folder

- **Audit and Archive Inactive Accounts**

  Review accounts, especially suspended ones, to determine if they need archiving or deletion. GAT Flow helps automate offboarding while archiving inactive data ensures compliance. With GAT+, admins can also bulk add, update, or remove Google user accounts, streamlining account management through import and export functionalities.

  Learn How to Add-Update-Remove Google User Accounts in Bulk

- **Verify Security and Compliance Policies**

  Use GAT Shield to ensure compliance policies align with the latest regulations and set up alerts for unauthorised activities.

  GAT Shield Overview

Best Practices for Your Annual Auditing in Google Workspace

- **Update Role-Based Permissions**

  Verify that access levels correspond to each employee's role. GAT Unlock enables efficient permission updates to safeguard sensitive data.

  Learn to Replace Sharing Permissions on Google Drive Files

- **Run Regular Reports for Stakeholders**

  Schedule reports to keep stakeholders informed on security metrics, compliance, and risks. GAT+ allows you to automate reporting across all aspects of your Google Workspace domain, saving time and ensuring timely insights. These reports can be set to run automatically, providing comprehensive visibility and supporting proactive security management.

  Learn to Schedule Reports in Google Cloud Storage with GAT+

- **Set Up Automated Alerts for Key Login Activities**

  Use User Login Alerts in GAT+ to receive notifications on critical login events within your chosen scope, enabling vigilant monitoring of your Google Workspace environment. When a login alert rule is deployed, admins are notified instantly if a user logs in from an unusual location or device, helping to secure remote work environments by promptly flagging potential unauthorised access.

  Learn to Setting Up User Login Alerts in GAT+

Useful Resources

In addition to tool-based solutions, these best practices help every Google Admin conduct a thorough annual audit:

- **Guide to Data Breach Prevention:** Essential strategies for preventing data breaches and protecting sensitive information across your organisation.
- **Guide to Securing Files Shared Internally and Externally:** Steps to manage and secure file sharing within and outside your domain, ensuring controlled access.
- **Guide to Google Workspace Automation:** Learn how automation can streamline your workflows, from onboarding to compliance, saving time and reducing risks.
- **Auditing your Google Workspace Guide:** Comprehensive overview of auditing practices to maintain compliance and security across your Workspace environment.

Your Annual Google Workspace Audit Checklist

- Review file-sharing settings and permissions with GAT+
- Audit suspended and inactive accounts using GAT Flow
- Run compliance checks for data-sharing and access policies
- Verify access levels for role-based permissions with GAT Unlock
- Monitor security events with GAT Shield's real-time alerts
- Deliver end-of-year reports to stakeholders

By following these best practices, Google Admins can ensure their environment is fully prepared, compliant, and secure for the coming year.

Remember, We're Here to Help

If you have questions or need support with your year-end audit, our team is ready to assist. Reach out to our support team for personalised guidance.

If you're considering upgrading your plan to access more GAT Labs features, schedule a demo to see how we can further enhance your Google Workspace management.

Ready To Simplify Your Audits?

EXPLORE MORE

VISIT OUR WEBSITE

SCHEDULE A DEMO

15 DAY FREE TRIAL

GAT labs