ENTERPRISE RESOURCES

The Google Admin's Guide To Modern File Sharing Governance

Move beyond one-off audits. Learn how to apply consistent controls across Drive, users, and third-party apps.

GAT labs

1. Modernizing Permission Structures With Zero Trust Access

Traditional Viewer, Commenter, and Editor permissions are no longer enough on their own. In modern Google Workspace environments, **access decisions must consider context, not just role.**

Context-Aware Access allows admins to restrict access to sensitive data based on conditions such as user location, IP reputation, or device security posture. This approach reduces risk without blocking productivity.

For example, finance or legal data can be accessed only from managed devices that meet security requirements.

Authentication is equally important. SMS and push-based verification methods are increasingly targeted by phishing attacks. Admins should enforce phishing-resistant two-step verification, such as hardware security keys or passkeys, especially for privileged accounts.

As AI tools and automated agents begin interacting with Workspace data, permissions must remain tightly scoped. These tools should only access what they need and should never inherit broad Drive permissions by default.

2. Proactive Data Loss Prevention for Shared Files

Data Loss Prevention must evolve alongside new access patterns. DLP should act as a continuous control, not just a passive alerting system.
Admins need visibility into unusual access behavior from both human users and automated tools. Sudden spikes in sharing, bulk downloads, or unexpected access patterns can signal misconfiguration or account compromise.

Where possible, response should be automated. Risky access should trigger immediate action, not just notifications.

How to strengthen DLP controls:

- Identify where sensitive data exists across My Drive and Shared Drives
- Apply DLP rules that trigger when sensitive files are shared externally
- Monitor unusual access patterns, including bulk sharing or downloads

IN THE GOOGLE ADMIN CONSOLE

Create DLP Rules to Match Risk Profiles

Data classification gives you visibility.
DLP rules help you enforce protection.

How to set up rules:

1. In the Google Admin Console, go to: Security → Data Loss Prevention
2. Create rule sets for each sensitive data category (e.g., personal data, financial files, legal docs).
3. Define triggers such as:
   - Shared externally
   - Downloaded outside business hours
   - Copied to public folders

With GAT Shield

Extending DLP with GAT Shield

Enforce controls at the browser level
Native DLP rules alert you to risk.

With Shield, admins can:

- Block downloads of sensitive files
- Receive notification/warning for uploads
- Restrict copy and paste actions
- Revoke public links as soon as policy violations occur
- Monitor real user activity at the browser level

This helps reduce exposure before data leaves the environment, especially in scenarios where alerts alone are not enough.

3. Managing User Lifecycles and File Ownership

File ownership and user lifecycle events are closely tied to data exposure. When users change roles or leave the organization, files are often left behind with unclear ownership or overly broad access.

Without a defined process, sensitive data can remain accessible long after it should not.

How to reduce ownership and lifecycle risk

Admins should focus on:

- Transferring ownership when users leave or change roles
- Ensuring every critical file has a clear business owner
- Removing unnecessary internal access created over time

IN THE GOOGLE ADMIN CONSOLE

Handle ownership and access during offboarding

Google Workspace provides basic tools to manage user offboarding, but many actions require manual follow-up.

What admins can do natively:

1. Suspend or delete the user account
2. Transfer Drive ownership to another user
3. Review Shared Drive access for the departing user
4. Remove domain-wide or group-based sharing where appropriate

These steps work, but they rely on admins remembering to do them every time.

WITH GAT Unlock and Flow

Automate ownership transfer and access cleanup

With GAT Unlock and Flow, lifecycle actions can be built into a standard process.

Admins can:

- Automatically transfer file ownership to a manager or service account
- Remove access to sensitive Shared Drives
- Apply multi-party approval for ownership changes
- Ensure every action is logged for audit purposes

This reduces manual effort and ensures ownership and access changes happen consistently.

4. Why Manual Audits Always Come Too Late

Most file sharing reviews start the same way. Something feels off. A file shows up in the wrong place. Legal or security asks a question. An admin pulls logs and starts digging.
By the time an audit begins, the exposure has usually already happened.

This is the core limitation of manual audits. They are reactive by nature. They tell you what changed, but only after the fact. In fast-moving Google Workspace environments, that gap matters.
What admins need instead is visibility that keeps pace with sharing behavior.

What meaningful visibility actually looks like

Effective file sharing governance is not about running more reports. It is about answering a few key questions at any moment:

- Which files are currently shared outside the domain?
- Which files were shared into the domain from external owners?
- What changed recently, and who made the change?

When visibility is continuous, admins can respond early instead of reconstructing events later.

Auditing with GAT Labs

Extending visibility with GAT+

GAT+ shifts visibility from investigation to monitoring.

Instead of pulling logs manually, admins can:

- View all externally shared files in a single dashboard
- Identify files owned externally but shared into the domain
- Track recent sharing or ownership changes without running reports
- Schedule recurring reports that surface new risks automatically

This makes file sharing visibility part of daily governance rather than a task triggered by concern.

Learn More in our Knowledge Base

5. The Quiet Risk Most Admins Miss: Third-Party Apps and OAuth Access

Most admins focus on users when thinking about access risk. What often gets overlooked is how many apps can read, edit, or delete data in Google Drive without ever logging in like a user.

OAuth access is designed to make work easier. A user clicks “Allow,” and an app can interact with their files. The problem is that this access often remains long after the app is no longer needed, and it rarely gets reviewed.
Over time, these apps become invisible access points into your data.

Why OAuth access is different from user access

Unlike users, apps do not:

- Log in interactively
- Raise obvious access questions
- Leave the company

Once granted, app access persists until it is actively removed.
This creates a situation where an app that was approved for a one-time task can quietly retain broad Drive permissions indefinitely.

What admins should look for

Instead of reviewing every app equally, focus on risk signals:

- Apps with read or edit access to Drive
- Apps that have not been used recently
- Apps installed by users outside IT or security teams

Consent phishing also plays a role here. Malicious apps increasingly rely on user approval prompts rather than stolen credentials, which makes OAuth reviews a critical control.

Strengthen OAuth App Security with GAT

IN THE GOOGLE ADMIN CONSOLE

Review and control app access

Google Workspace provides App Access Control to help admins manage third-party applications.

What admins can do natively:

1. Go to Admin Console → Security → Access and data control → API controls
2. Review apps with domain-wide or user-granted access
3. Block or restrict apps with unnecessary or high-risk scopes
4. Limit app access by organizational unit where appropriate

This provides a baseline level of control, but it does not always show how apps are actually being used.

WITH GAT LABS

Extending OAuth visibility with GAT+

GAT+ adds context to app access decisions.

With GAT+, admins can:

- See which apps have access to Drive data
- Review permission scopes alongside last-used activity
- Identify apps that are dormant but still authorized
- Remove or restrict app access in bulk

This helps admins move from “what is installed” to “what actually represents risk.”

Why this matters

Third-party apps often bypass traditional sharing controls. If an app can read or modify files, it effectively acts as a user with permanent access.
By treating OAuth permissions with the same scrutiny as user permissions, admins close one of the most common and least visible data exposure paths in Google Workspace.

6. External Sharing Feels Obvious. It Rarely Is.

Most Google Workspace admins believe they have external sharing under control. After all, sharing settings exist in the Admin Console, and external access is a known risk.

The problem is not awareness.
The problem is persistence.

Files shared externally tend to stay shared. Public links are created for convenience and rarely reviewed. Ownership changes, but access does not. Over time, exposure becomes invisible.
External sharing is not a single action. It is a lifecycle.

Where external sharing usually breaks down

External exposure often comes from:

- Old shares that were never reviewed
- Public links created for short-term collaboration
- Files owned by users who have since left
- Apps accessing files on behalf of users

Each of these bypasses a different control, which is why external sharing cannot be managed with a single setting.

IN THE GOOGLE ADMIN CONSOLE

Set boundaries, not just permissions

Admins can limit external sharing at the domain or OU level, but these settings define what can happen, not what has already happened.

Native controls help:

- Restrict external sharing by organizational unit
- Limit link sharing options
- Audit sharing activity through Drive logs

These are necessary foundations, but they do not surface existing exposure on their own.

Auditing with GAT Labs

Extending external sharing control with GAT+

GAT+ brings external sharing into focus by showing:

- Files currently shared outside the domain
- Files shared via public links
- Files owned externally but shared into the domain

More importantly, it allows admins to act on this visibility by:

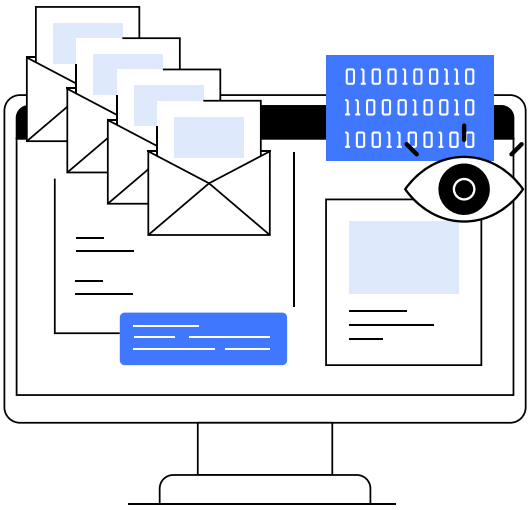
- Removing access in bulk
- Filtering by owner, OU, or sensitivity
- Scheduling recurring reviews instead of one-time cleanups

This turns external sharing into a governed process rather than a recurring surprise.

Why this matters

External sharing is rarely malicious. It is usually forgotten.
By treating external access as something that must be reviewed continuously, rather than configured once, admins can reduce data exposure without slowing collaboration.

This is where permissions, auditing, ownership, DLP, and alerting all come together.



Google Drive Management Features in GAT

7. Putting It All Together: A Practical Governance Model

Securing files in Google Workspace is not about adding more rules. It is about applying the right controls at the right moments, and making them repeatable.
Across this guide, each control addresses a different type of risk. On its own, none of them is enough. Together, they form a governance model that is both practical and sustainable.

Think in lifecycles, not settings

Most file sharing risk does not come from a single misconfiguration. It builds over time.
Files are created, shared, copied, and passed between teams. Users join, change roles, and leave. Apps are approved, forgotten, and replaced. If governance only focuses on settings, these changes will always outpace control.

A practical governance model treats file access as a lifecycle.
It asks the same questions continuously:

- *What is being shared?*
- *Who owns it now?*
- *Who can access it?*
- *What changed recently?*

Use native controls to set boundaries

Google Workspace provides strong foundations. Sharing defaults, organizational units, Context-Aware Access, DLP rules, and App Access Control define what users and apps are allowed to do.
These controls are essential. They set guardrails and reduce obvious risk. But they work best when combined with regular review and enforcement.
Boundaries alone do not provide visibility.

Add visibility where native tools stop

Visibility is what turns boundaries into governance.
Continuous insight into external sharing, internal over-sharing, ownership changes, and third-party app access allows admins to see risk as it develops, not after it has already caused exposure.

This is where tools like **GAT+ and GAT Shield** extend native capabilities, helping admins move from reactive investigation to ongoing oversight.

Automate what should never depend on memory

The biggest gaps appear during routine events. Offboarding. Role changes. Short-term collaborations. These moments happen too often to rely on manual processes.

A practical model builds automation into these workflows:

- Ownership transfers happen automatically
- Risky sharing triggers alerts or action
- Policy violations are corrected early

Automation is not about removing control. It is about making control consistent.

Keep collaboration intact

Good governance does not slow teams down. It removes uncertainty.
When access is clear, ownership is defined, and sharing is reviewed regularly, users can collaborate with confidence. Admins spend less time reacting to surprises and more time maintaining a healthy environment.

The goal is not to restrict collaboration. It is to make it predictable and secure.

The outcome

When these elements work together, file sharing governance becomes part of how Google Workspace operates, not a separate security task.
Admins gain:

- Clear visibility into shared data
- Consistent ownership and access
- Faster response to risk
- Fewer unexpected exposures

That is what a practical governance model looks like.

Want To Learn More?

VISIT OUR WEBSITE

VISIT OUR RESOURCES PAGE

TRAINING SESSIONS CALENDAR

GAT labs