Drive Audit Checklist for Professional Firms (Google Workspace)

The “State of Order” Context (Why this audit exists)

In professional firms, Google Drive disorder is not an aesthetic issue—it’s operational drag with measurable risk. The failure mode is predictable:

- **Data drift:** the environment’s “intended” structure (client/matter taxonomy, retention expectations, permission boundaries) diverges from reality as teams create ad-hoc folders, copy templates, and share links outside policy.
- **Fragmentation:** critical work artifacts sprawl across My Drive, Shared Drives, and external shares. Search becomes probabilistic; staff recreate work because they can’t reliably locate the canonical version.
- **Security exposure:** public links, unmanaged external sharing, and over-broad group permissions create silent breach paths—especially in accounting and legal workflows where client confidentiality is non-negotiable.
- **Workflow breakage:** link rot, duplicate “final” files, and inconsistent naming disrupt handoffs (review → approval → filing), increasing cycle time and error rates.

A Drive audit is the mechanism that re-establishes **operational integrity**: a governed, predictable, auditable workspace where permissions are intentional, content is discoverable, and lifecycle rules are enforceable.

Technical Framework: Multi-tier Drive Audit Rubric (scored)

Use this rubric to score governance maturity across six tiers. Each tier is scored **0–3**:

- **0 = Uncontrolled** (ad-hoc, high risk)
- **1 = Partially controlled** (inconsistent, exceptions dominate)
- **2 = Controlled** (defined standards, moderate exceptions)
- **3 = Governed** (standards + enforcement + monitoring)

Audit scoring model

Compute an overall score and a risk-weighted score.

Overall maturity (%):

$$Maturity = \frac{\sum Tier\ Scores}{(\#Tiers \times 3)} \times 100$$

Optional risk-weighted maturity (assign weights to tiers based on firm risk tolerance):

$$Weighted\ Maturity = \frac{\sum(Tier\ Score \times Tier\ Weight)}{\sum(3 \times Tier\ Weight)} \times 100$$

Tier 1 — Identity & Access Baseline (Groups, roles, admin boundaries)

Objective: Ensure access is mediated through groups and least-privilege roles.

Check	Good (Score 3)	Bad (Score 0–1)	Evidence to capture
Group strategy	Role-based Google Groups (e.g., "Tax-Associates", "Client-Services-Partners")	Individual user permissions dominate	List of groups + mapping to roles
Admin roles	Custom roles scoped to Drive settings; minimal Super Admins	Many Super Admins; unclear delegation	Admin role list
Offboarding	Automated suspension + transfer/retention policy	Departed users retain ownership/ shares	Offboarding SOP + logs

Tier 2 — Shared Drives vs. My Drive Boundary

Objective: Institutional work lives in Shared Drives; My Drive is personal scratch only.

Check	Good (Score 3)	Bad (Score 0–1)	Evidence to capture
Canonical location	Client/matter work is in Shared Drives	Client work in My Drive with ad-hoc shares	Sampling of top client folders
Ownership model	Shared Drive managers are groups	Individuals are managers/owners	Shared Drive membership export
Creation controls	Shared Drive creation restricted	Anyone can create drives	Admin setting screenshot

Tier 3 — External Sharing & Link Governance

Objective: External access is intentional, time-bounded, and reviewable.

Check	Good (Score 3)	Bad (Score 0–1)	Evidence to capture
Default sharing	Restricted; domain-only by default	"Anyone with link" common	Admin sharing settings
External access	Allowed only via approved groups + justification	Individual external shares uncontrolled	External share report
Link types	No public links; link expiration where possible	Persistent public links	Sample of link settings

Tier 4 — Information Architecture (Folder taxonomy + naming)

Objective: Predictable structure that supports search, handoffs, and retention.

Check	Good (Score 3)	Bad (Score 0–1)	Evidence to capture
Folder taxonomy	Standard client/matter template	Every team invents structure	Template doc + examples
Naming schema	Enforced patterns (client, year, doc-type, status)	"Final_final_v7" chaos	50-file sample review
Archive model	Separate archive with read-only permissions	Archives mixed with active work	Archive drive/folder map

Tier 5 — Data Quality (Duplicates, orphaned files, stale content)

Objective: Reduce duplication and eliminate orphaned/abandoned artifacts.

Check	Good (Score 3)	Bad (Score 0–1)	Evidence to capture
Duplicate handling	Duplicates identified + quarantined	Duplicates proliferate	Duplicate scan summary
Orphaned files	Ownership and location are known	Files owned by departed users	Ownership report
Stale content	Lifecycle rules + periodic review	No review cadence	Stale content metrics

Storage efficiency improvement (if you have baseline vs. optimized storage):

$$Storage\ Efficiency\ Improvement = \left(1 - \frac{Optimized\ Storage}{Baseline\ Storage}\right) \times 100$$

Tier 6 — Monitoring, Auditability, and Change Control

Objective: Governance is continuously verifiable, not a one-time cleanup.

Check	Good (Score 3)	Bad (Score 0–1)	Evidence to capture
Audit logs	Drive audit logs reviewed on cadence	Logs unused	Review schedule + owners
Exception handling	Documented exceptions with expiry	Permanent exceptions	Exception register
Change control	Preview-first changes; rollback plan	Untracked bulk edits	Change tickets + approvals

The How-To: Performing the audit in Google Admin Console

This is a practical sequence you can execute as a Workspace admin or delegated Drive governance admin.

Prerequisites

- Confirm you have **Admin Console** access with permissions for:
  - Drive and Docs settings
  - Groups (or visibility into group structure)
  - Reports / audit logs
- Define the audit scope:
  - Organizational units (OUs) included
  - Shared Drives included (all vs. high-risk business units)
  - Time window (e.g., last 90 days for sharing activity)

Step 1 — Capture baseline Drive sharing posture

1. In **Admin Console**, navigate to **Apps → Google Workspace → Drive and Docs**.
2. Review and record:
   - Default sharing settings (internal vs. external)
   - Link sharing defaults
   - Whether users can publish files to the web

3. Document the current state as “Baseline Settings v1” (date-stamped).

Step 2 — Validate Shared Drive creation and management controls

1. In **Drive and Docs**, locate **Shared Drives** settings.
2. Confirm:
    - Who can create Shared Drives (restricted vs. open)
    - Whether managers can modify membership and sharing
3. Export or record:
    - List of Shared Drives
    - Manager assignments (prefer groups)

Step 3 — Audit external sharing behavior (activity + hotspots)

1. Go to **Reports → Audit and investigation → Drive log events**.
2. Filter for:
    - “Visibility changed” events
    - “External user added” events
    - “Link sharing enabled” events
3. Segment findings:
    - By OU / department
    - By Shared Drive vs. My Drive
    - By top actors (repeat sharers)
4. Capture:
    - Counts by event type
    - Top 10 drives/folders with external sharing activity

Step 4 — Audit group model and permission hygiene

1. Review Google Groups used for access control (via Admin Console or your group directory).
2. Identify anti-patterns:
    - Groups with nested external members
    - Groups with unclear naming (“Team1”, “Misc”)
    - Direct user permissions used instead of groups
3. Record:
    - Group naming conventions
    - Ownership/manager of each group
    - Whether groups map to firm roles

Step 5 — Sample information architecture quality (taxonomy + naming)

This is a sampling exercise; you do not need to inspect everything.

1. Select a representative sample:
    - 5–10 Shared Drives (high-volume + high-risk)
    - 3–5 client/matter areas per drive
2. Evaluate:
    - Presence of a standard top-level taxonomy
    - Consistency of naming patterns
    - Clear “active vs. archive” separation
3. Score Tier 4 using the rubric.

Step 6 — Identify orphaned ownership and lifecycle gaps

1. Review user lifecycle posture:
    - How Drive ownership is handled on suspension/departure
2. Pull a list of suspended/departed accounts and confirm:
    - Ownership transfer process exists
    - Shared Drive membership is removed
3. If available, capture:
    - Files owned by suspended users
    - High-risk shares created by departed users

Step 7 — Produce the audit scorecard + remediation plan

1. Score each tier 0–3.
2. Compute maturity using the formula above.
3. Output two artifacts:
    - **Scorecard** (current state)
    - **Remediation backlog** (ranked by risk reduction)

Recommended remediation prioritization:

- External sharing controls and public links
- Shared Drive boundary enforcement
- Group-based permission normalization
- Lifecycle/archival separation
- Duplicate/orphaned cleanup

Automation Logic: What an autonomous engine (NeatDrive) should do vs. manual work

Manual audits fail for one reason: they are episodic. Drift resumes immediately after the audit window closes.

Ideal autonomous handling (metadata-only, preview-first)

An autonomous governance engine should:

- **Continuously scan Drive metadata** (owners, paths, permissions, link visibility, timestamps) without reading file contents.
- **Detect and classify risk**:
  - Public links
  - External collaborators
  - Over-broad group permissions
  - “My Drive as system-of-record” patterns
- **Identify duplicates** using deterministic and probabilistic signals (hashing where available, filename/size/time heuristics) and produce a confidence score.
- **Generate a previewed cleanup plan**:
  - Proposed moves/renames
  - Permission normalization
  - Quarantine candidates (not deletion)
- **Maintain audit trails and rollback**:
  - Every change is logged
  - Rollback is one action, not a forensic project

What remains human-controlled (by design)

- Approval of policy boundaries (what external sharing is acceptable)
- Exception approvals (client-specific requirements)
- Final execution approval for bulk changes

Guardrails that prevent operational damage

- No content access (metadata-only analysis)
- Preview-first changes
- Quarantine instead of deletion
- Rollback support and immutable audit logs

Printable / Internal Policy Summary (copy-paste memo)

Purpose

To establish a repeatable audit process that verifies Google Drive governance, reduces confidentiality risk, and restores operational predictability across Shared Drives and My Drive.

Scope

Applies to all firm personnel, contractors, and service accounts using Google Workspace Drive, including Shared Drives, My Drive, and externally shared content.

Definitions

- **Shared Drive:** Team-owned storage for institutional work products.
- **My Drive:** Individual workspace for personal drafts; not a system of record.
- **External share:** Any file/folder shared outside the firm's Google Workspace domain.
- **Public link:** "Anyone with the link" or "Published to web" access.

Policy Statements

1. **System of record:** Client/matter work products must reside in Shared Drives. My Drive is not an approved system of record.
2. **Access control:** Permissions must be assigned through role-based Google Groups wherever feasible. Direct user permissions are exceptions requiring justification.
3. **External sharing:** External sharing is restricted to approved scenarios and must be reviewable. Public links are prohibited unless explicitly approved and time-bounded.
4. **Information architecture:** Shared Drives must follow the firm's approved taxonomy and naming conventions to ensure discoverability and lifecycle enforcement.
5. **Lifecycle:** Active work and archived work must be separated. Archived areas are read-only by default.
6. **Auditability:** Drive governance must be auditable via Admin Console reports and logs. Exceptions must be documented with an owner and expiry.

Audit Cadence and Ownership

- **Cadence:** Quarterly governance audit; monthly external-sharing review.
- **Owner:** Operations / IT Governance Lead.
- **Evidence:** Scorecard (tiers 1–6), remediation backlog, and log snapshots.

Exception Handling

Exceptions require:

- Business justification
- Named owner
- Expiry date and review date
- Documented compensating controls

Enforcement

Non-compliant configurations may be remediated via permission normalization, relocation to Shared Drives, and removal of public links, subject to change control and rollback procedures.