

Migration Complete. Now What?

A Public Sector Guide for Controlling
Sprawl, Cost, and Risk



Most public sector organizations can get to "migration complete." The harder part is making sure day-to-day collaboration stays governable, auditable, and affordable once people are working in the new environment.

While AvePoint supports the full migration lifecycle, this guide focuses on what happens after the cutover. When governance becomes operational, not just planned.

This isn't a Microsoft-only or Google-only challenge. Whether you are moving to a Microsoft 365 tenant, consolidating Google Workspace, or operating in a mixed environment during transition, the same three problems tend to show up fast:

- Collaboration sprawl grows faster than the team that manages it.
- Compliance obligations don't implement themselves. Retention, records, legal holds, and eDiscovery require operating discipline.
- Storage growth becomes budget risk, especially as content volumes and pricing models change.

This guide focuses on what tends to go wrong when migration is treated as a one-time move, and what to put in place immediately after the cutover so collaboration stays governable, audit-ready, and financially sustainable over time.



Who this is for

Public sector IT and security leaders, digital workplace owners, and records and compliance stakeholders who are migrating (or have recently migrated) between modern cloud collaboration environments and need to regain control of content, risk, and cost.



Reality Check

Most cloud collaboration suites include baseline admin and compliance features, but many public sector teams still struggle with (1) consistent lifecycle enforcement, (2) cross-workspace visibility, (3) repeatable controls that don't depend on scripts or heroics, and (4) recovery speed when something goes wrong.

The following steps address these problems in a sequence that works for constrained public sector teams: baseline first, then define constraints and decision rights, then implement controls that can be measured and improved over time.

What To Prioritize After The Move

Treat this as an operating model, not a post-project checklist. You don't need perfection on day one, but you do need a clear set of priorities that can be measured and improved over time.

Operational Outcomes

- Users can collaborate quickly without creating unmanaged spaces.
- IT can see what is being created, where sensitive data lives, and which workspaces are risky.
- Workspaces have owners, lifecycles, and predictable end-of-life paths.

Compliance Outcomes

- Retention and records policies are implementable in the way people actually work.
- Legal holds and exceptions are traceable and defensible.
- Discovery and public records responses are timely and repeatable.

Financial Outcomes

- Storage growth is measured, forecasted, and governed.
- Archiving and lifecycle policies reduce cost without undermining compliance.
- Cleanup and disposition happen continuously, not as a once-a-year emergency.

Step 1: Baseline Your Reality (Inventory Before Decisions)

The problem: Most organizations start trying to "fix governance" without knowing what they're governing. You can't manage sprawl, enforce retention, or control costs if you don't know how many workspaces exist, who owns them, where sensitive data lives, or how fast storage is growing.

Before you implement controls, establish a baseline you can defend.

Baseline Checklist

Surface area: How many collaboration spaces exist today (sites, shared drives, groups, teams, channels)?

Ownership: What percentage of spaces have a named owner and backup owner?

External exposure: How much external sharing exists, and where?

Sensitivity: Where does regulated or high-risk data likely live?

Lifecycle: Do spaces have a purpose, expected lifespan, and closure path?

Records posture: Are retention categories and policies in place, consistent, and understood?

Discovery readiness: Could you respond to a hold or public records request predictably?

Storage economics: What is your growth rate, and what is it projected to cost over 12–24 months?

Evidence To Gather (So The Baseline Isn't Guesswork)

- ☐ A current export or report of spaces with owners, last activity, and external access

- ☐ Storage consumption and top growth areas

- ☐ A list of retention policies and categories in use, including exceptions

- ☐ A summary of recent incidents: oversharing, mis-permissioning, orphaned spaces, and "mystery" content



Note

Governance platforms like AvePoint can automate much of this baseline discovery and reporting, providing visibility you can't easily get from native admin tools alone.

Examples: In Microsoft environments, this may include Teams, SharePoint sites, and OneDrive. In Google environments, this may include Shared Drives and Drive ownership patterns.

Step 2: Define constraints and decision rights

The problem: Most post-migration pain isn't about missing features; it's about unclear decision rights. When no one knows who decides what, governance defaults to either "central IT does everything" which doesn't scale or "everyone does their own thing" (which creates risk and sprawl).

Defining constraints and decision rights early prevents governance paralysis later.

Define Constraints

- Data classification and handling requirements (restricted data types, sharing rules)
- Records retention obligations (program schedules, holds, exceptions)
- Audit and reporting expectations (who needs what proof, and when)
- Availability and continuity expectations (what must never break)

Once constraints and decision rights are clear, a collaboration governance platform like AvePoint can enforce them consistently across your collaboration environment.

Define Decision Rights (Who Decides What)

Decision	Typical owner	Also involved
Workspace creation standards and guardrails	Central IT / digital workplace owner	Security, records, key business units
Retention and records policies and exceptions	Records / legal	IT, security, program owners
External sharing rules	Security	IT, procurement, program owners
Disposition and cleanup cadence (the process of archiving or deleting content according to retention rules)	IT + records	Program owners
Storage tiering and archiving approach	IT / infrastructure	Records, security, finance

Step 3: Govern The Collaboration Surface Area (So Sprawl Doesn't Win)

The problem: Users create new workspaces faster than IT can track them. Orphaned workspaces accumulate when owners change roles. External sharing happens without oversight. Within months, you have hundreds of unmanaged spaces, unclear ownership, and no clear path to clean up the mess.

The goal is to keep collaboration fast while reducing unmanaged growth.

What Strong Governance Platforms Automate:

- Provisioning with guardrails (intake, approvals, templating)
- Ownership and access reviews to enforce least privilege
- Lifecycle enforcement (active → inactive → archive → disposition)
- Central reporting for risk hotspots, oversharing, and orphaned workspaces
- Delegated administration with oversight and audit trails

These capabilities are available now with the right platform. The question is how to deploy them in a way your organization can absorb.

Minimum Guardrails To Put In Place

- Standardized workspace requests with required fields (purpose, owner, sensitivity, external access, expected lifespan)
- Lifecycle states (active, inactive, archived, ready for disposition)
- Ownership requirements (no owner, no workspace)
- Naming conventions that support search, audit, and reporting
- Permission standards that reduce accidental exposure

Delegated Administration (Scale Without Expanding Central IT Forever)

If central IT is responsible for 100% of administration, governance will always lag. Define a delegated model:

- Which tasks can be delegated to trained business admins
- How approvals work for higher-risk requests
- What reporting and audit trails are required
- How you remove admin rights cleanly when roles change

Quick Self-Check

- Can you explain, in one sentence, how a new workspace gets created and who approves it?
- Can you identify your top 20 riskiest workspaces (and why) in under one hour?

Step 4: Retention, Records, and Defensible Disposition

The problem: Retention policies sit in binders while teams collaborate in ways those schedules never anticipated. Chat, shared files, and workspace artifacts don't map neatly to traditional retention categories. When legal holds or public records requests arrive, you can't respond predictably—and disposing of eligible content feels too risky, so nothing ever gets deleted.

Retention isn't a document. It's an operating system that must work across how people actually collaborate.

Q What To Look For (Records & Retention)

Defensible disposition, audit trails, and retention that applies consistently across how people actually work (shared spaces, files, and collaboration artifacts), not just email.

Make Retention Implementable

- Translate schedules into clear categories that map to how teams work (not how org charts look)
- Design for exceptions: legal holds, investigations, public records requests
- Ensure policies apply consistently across the collaboration surface area (chat, files, shared spaces)

AvePoint's policy engine can apply retention rules across Microsoft 365, Google Workspace, and other collaboration tools, making it possible to enforce retention where people actually work, not just where your records schedule says they should.

Defensible Disposition

Disposing of content is where organizations tend to freeze. "Do nothing" creates its own risk. Start by defining:

- What content is eligible for disposition
- Who approves disposition, and what evidence is required
- How you document decisions and action

Evidence To Request (Internal or Vendor Evaluation)

- How retention policies apply end-to-end, including exceptions and holds
- What audit logs exist for policy changes and for lifecycle actions
- How you demonstrate defensibility to auditors, legal, and oversight bodies

Step 5: Storage Lifecycle and Cost Control (Optimize Without Breaking Compliance)

The problem: Storage costs tend to rise quietly until they become a budget crisis. Unmanaged workspace creation, large file sprawl, and the absence of lifecycle controls mean your storage footprint (and your bill) grow faster than expected. By the time finance flags it, you're scrambling for quick fixes that often conflict with compliance obligations.

The solution is treating storage optimization as a lifecycle problem, not a "buy cheaper storage" problem.



Practical Note:

Storage cost control is usually a lifecycle problem more than a "buy cheaper storage" problem. The biggest wins come from preventing unmanaged growth, archiving inactive content appropriately, and creating a disposition routine that teams can execute with confidence.

What To Measure

- Growth rate by workload and by business unit
- Top growth drivers (large file types, duplicates, unmanaged personal storage)
- Age distribution (how much content is truly "active")

What To Change (In Order)

- 1.Reduce unnecessary creation through workspace standards and lifecycle controls.
- 2.Move inactive content to appropriate tiers or archives.
- 3.Dispose of eligible content through a defensible workflow.

Specialized platforms can automate much of this lifecycle work, such as identifying inactive content, enforcing tiering policies, and executing disposition workflows at scale.

Avoid Common Mistakes

- Optimizing storage by breaking retention or discovery readiness
- Treating archiving as "out of sight, out of mind" instead of a governed lifecycle stage

Step 6: Operationalize With Roles, Workflows, and a Cadence

Governance fails when it's a project. It works when it's a routine.



Don't Skip Resilience

Mature programs pair governance with recovery—because the best retention policy doesn't help if you can't restore a workspace

- How quickly can you restore a deleted file, a shared drive, or an entire workspace?
- Can you recover from misconfiguration or ransomware-related disruption without weeks of rebuild?

Platforms that unify governance, lifecycle control, and recovery (like AvePoint) address these problems together, which is why this guide treats them as part of the same operating model rather than separate projects.

Core Roles (Minimum Viable)

- Digital workplace service owner: accountable for standards, reporting, and operational health
- Security lead: accountable for access posture and risk boundaries
- Records and legal stakeholders: accountable for retention policy and defensibility
- Business workspace owners: accountable for content, membership, and lifecycle decisions

Monthly Governance Cadence (30–60 minutes)

Review: new workspaces created, high-risk changes, and external sharing trends
Review: orphaned workspaces, inactivity, and pending lifecycle actions
Review: disposition pipeline, holds, and exceptions
Review: storage growth and forecast vs. plan
Decide: the top 3 actions for the next 30 days and owners for each

Procurement and Evaluation Prompts (When You Need Tools, Services, or Both)

If you are assessing improvements, keep the evaluation grounded in outcomes and evidence.

Demo and Validation Prompts

- “Show how you identify workspaces with risk factors (no owner, external sharing, sensitive content) and how you remediate at scale.”
- “Show how retention policies apply end-to-end, including exceptions and holds.”
- “Show the audit trail for policy changes and for content lifecycle actions.”
- “Show reporting that a non-technical stakeholder can use to govern their area.”
- “Show how you forecast storage growth and tie recommendations to measurable cost impact.”

Reference Questions (Ask Organizations Like Yours)

- “What surprised you most after the migration, and what did you wish you had implemented earlier?”
- “What governance routines actually stuck, and which ones failed?”
- “How did you operationalize disposition without getting stuck in approvals?”
- “How did you scale administration without ballooning central IT headcount?”

A Realistic First 90 Days Plan

This is a pragmatic rollout sequence. With a platform like AvePoint, you can deploy comprehensive capabilities quickly. The pacing is about adoption and change management, not building functionality from scratch.

Weeks 1-2: Baseline and align

- Run automated discovery to baseline your collaboration environment (surface area, ownership, external access, storage growth)
- Confirm decision rights and constraints with stakeholders
- Use platform reporting to identify the top 10 risk hotspots and top 3 cost drivers

At this point, you'll have data-driven visibility into where sprawl and risk are concentrated, and who needs to be involved in fixing it.

Weeks 3-6: Deploy guardrails and reporting

- Activate workspace provisioning controls (request workflows, naming standards, ownership requirements)
- Turn on automated lifecycle management for orphaned and inactive workspaces
- Configure executive and operational dashboards to support the monthly governance cadence

This phase brings sprawl under control and makes governance visible to stakeholders who need to act on it.

**Weeks 7–12:
Operationalize
retention and
optimization**

- Deploy retention policies across collaboration workloads (starting with highest-risk or highest-volume areas)
- Activate storage lifecycle automation (archiving, tiering, and defensible disposition)
- Refine and document operating rhythms (what happens monthly, quarterly, and when incidents occur)

This phase makes compliance implementable and storage costs predictable, with evidence you can show auditors and finance.

Success Metrics (Choose a Small Set)

- % of workspaces with valid owners
- of high-risk workspaces reduced month over month
- Time to respond to discovery and public records requests (baseline vs. improved)
- Storage growth rate reduction or cost avoidance
- Disposition throughput (eligible content processed per month)



Connect with AvePoint

Migration isn't the finish line. The goal is a collaboration environment that stays governable, audit-ready, and financially sustainable.

Want to see how AvePoint can help your organization implement this roadmap? [Connect with AvePoint](#) to discuss your post-migration governance needs.

Explore how
AvePoint is
supporting the
public sector.



2026