Microsoft Purview Information Protection

Sensitivity Labeling & Watermark Deployment

Hands-on lab demonstration in a production tenant

Torrey Naylor

Microsoft Cybersecurity Practitioner

t-naylor.com

Cert track: AZ-900 → SC-900 → AZ-500 → SSCP

B.S. Cybersecurity, CSU Global (in progress, exp. March 2027)

Executive Summary

This portfolio piece documents a hands-on deployment of Microsoft Purview Information Protection in a live Microsoft 365 tenant. The objective was to configure sensitivity labels with visual content marking (watermarks), publish them through a label policy, validate label application across Office 365 surfaces, and verify the audit trail via the unified audit log.

The work demonstrates practical competency in data classification, label policy design, M365 licensing constraints, and the operational realities of Purview at the Business Premium tier — including where the license boundary draws the line between manual and service-side automated labeling.

Outcomes Delivered

- Sensitivity label configured with watermark content marking and email/file scope
- Label publishing policy deployed and synced to licensed user accounts
- End-to-end validation: label applied in Word for the web and Excel desktop; watermark renders as expected
- DLP policy ("U.S. Financial Data") deployed in Test with notifications mode, sync completed
- Audit log query authored against the unified audit log to surface SensitivityLabelApplied events
- Licensing constraint identified and documented (auto-labeling at rest requires E5 / IP&G add-on)

Lab Environment

Single-tenant Microsoft 365 environment, owned and administered by the author. One licensed test user; one dedicated SharePoint Online site for label testing.

License Stack

Tenant license	Microsoft 365 Business Premium
Identity	Entra ID P2
Email security	Defender for Office 365 Plan 2
Automation	Power Automate (Free)
Test SharePoint site	DLP — Purview Lab Site (private group, 2 members)
Test user	Single licensed account in tenant

Licensing Observation

Business Premium fully supports manual sensitivity labeling and content marking. Service-side auto-labeling of files at rest in SharePoint/OneDrive, however, requires Microsoft 365 E5, the E5 Compliance add-on, or the Information Protection & Governance add-on. This deployment therefore validates the manual labeling and policy publishing path — the operationally relevant path for any organization not on E5 — while documenting the next license step required to scale via automation.

Technical Walkthrough

1. Sensitivity Label Configuration

Two sensitivity labels were created in Microsoft Purview Information Protection:

- Internal Use only – No Public Access (Priority 0; scope: Files & other data assets, Email)
- Executive View Access (Priority 1; scope: Files & other data assets)

The lower-priority Internal label was configured with content marking — specifically, a diagonal watermark with the text "Elevated Information Technology Internal Use Only". This label was the focus of the watermark validation testing.

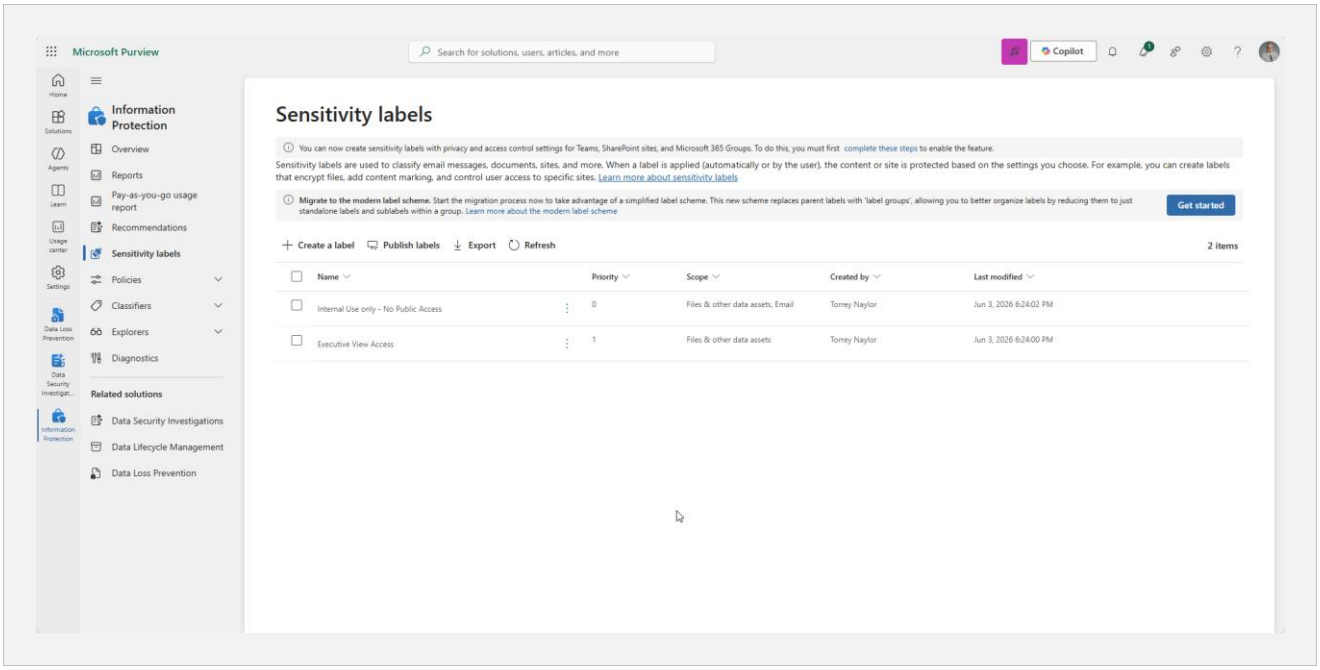

Figure 1. Sensitivity labels configured in the Purview portal.

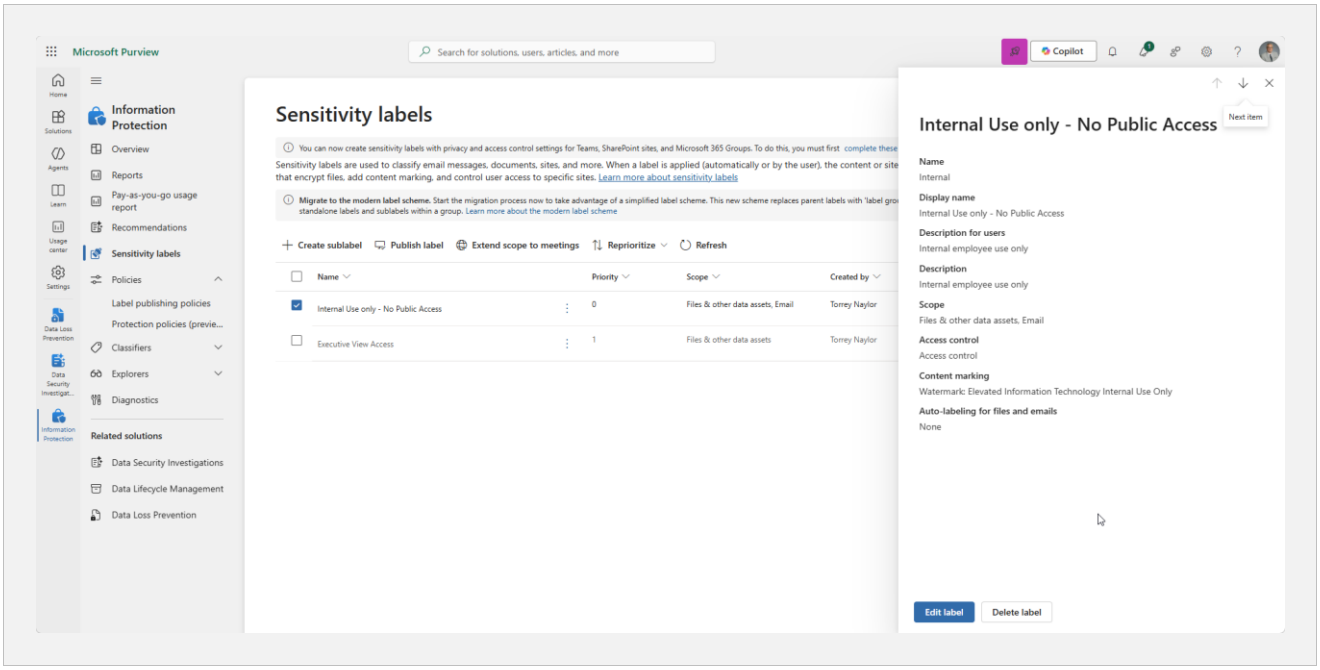

Figure 2. Label configuration: watermark content marking applied, scope set to files and email.

2. Label Publishing Policy

Two label publishing policies were deployed ("EIT Initial Policy" and "Initial Policy"), both showing Sync completed status. The publishing policy is what makes labels available to end users in Office applications — it does not, by itself, apply labels to existing content.

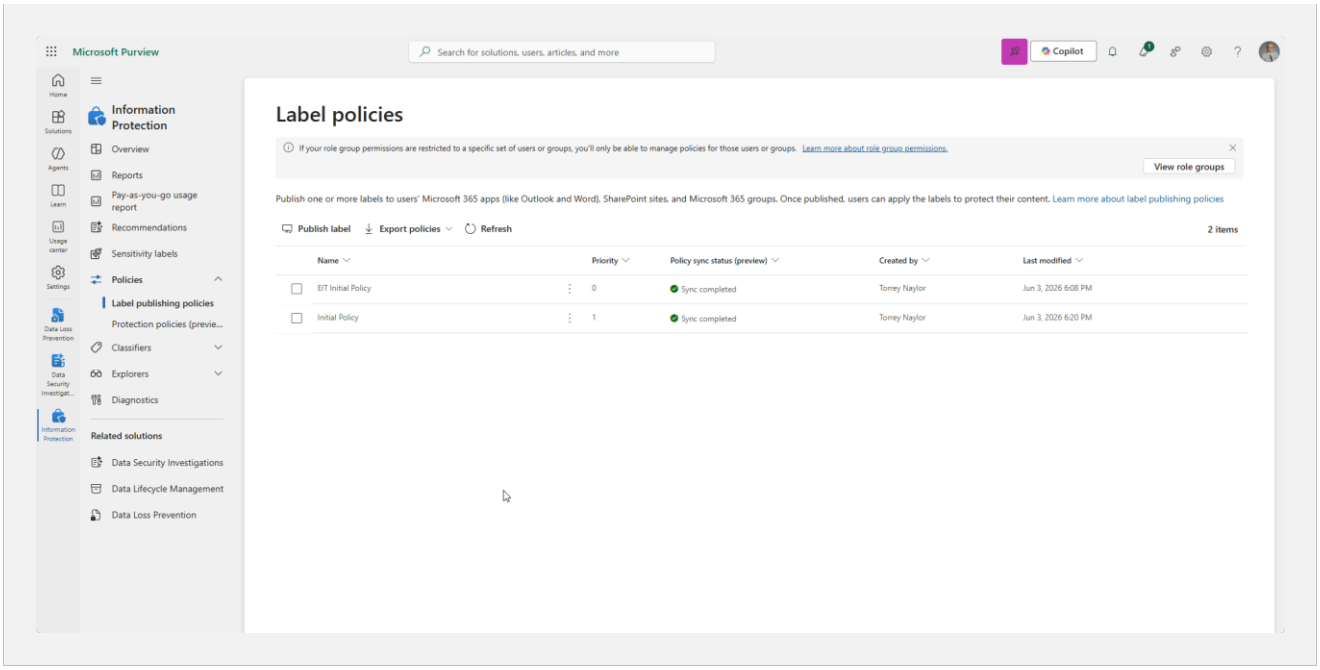

Figure 3. Label publishing policies, synced and active.

3. DLP Policy Deployment

A Data Loss Prevention policy named "U.S. Financial Data" was deployed and set to Test with notifications mode. This audit-only mode allows verification of detection accuracy before moving the policy into enforcement — the recommended approach to avoid disrupting legitimate business activity during initial rollout.

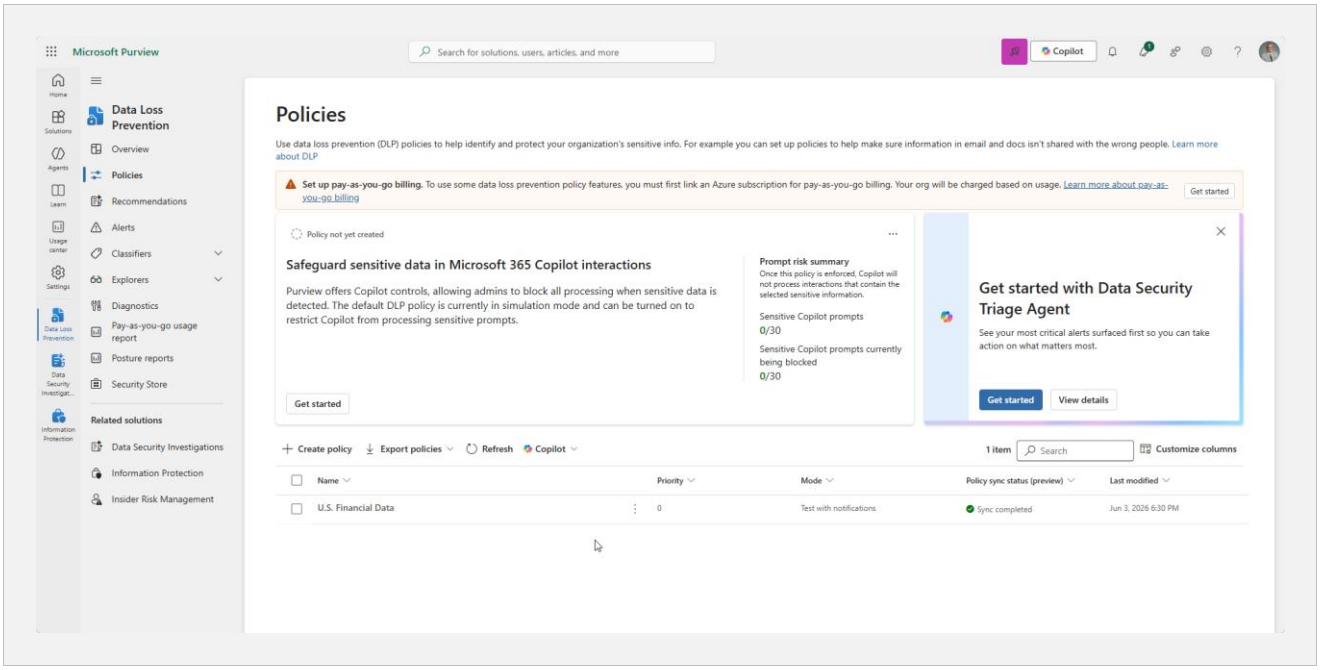

Figure 4. DLP policy deployed in audit (Test with notifications) mode.

4. Label Application — Excel

A test Excel workbook containing Microsoft's published test credit card numbers (Visa 4111-…, Mastercard 5500-…, Amex 3714-…, Discover 6011-…) was opened in Excel desktop. The Sensitivity control on the Home ribbon presented both labels from the publishing policy; the Internal label was applied manually.

Note: Excel does not render watermarks in the default Normal view. Watermarks render in Page Layout view and in Print preview/output. This is a common point of confusion when validating Excel labeling.

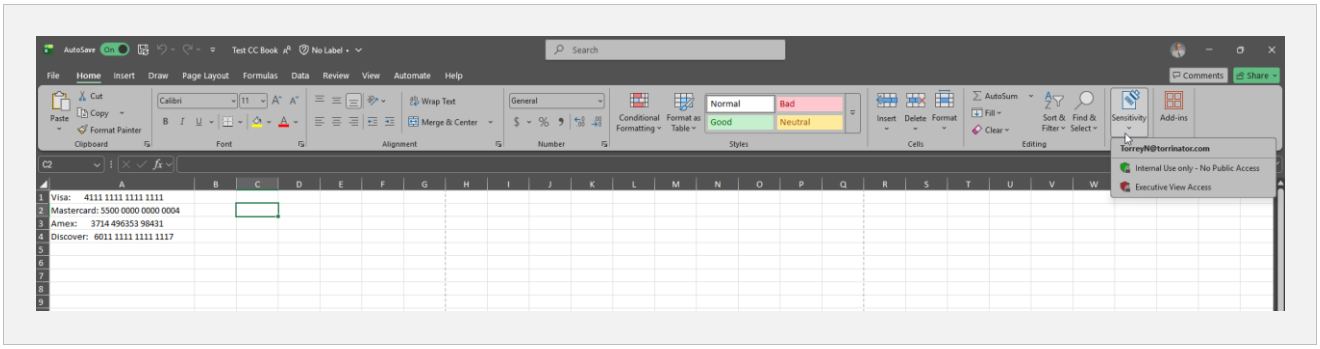

Figure 5. Sensitivity labels available on the Excel Home ribbon, served via the publishing policy.

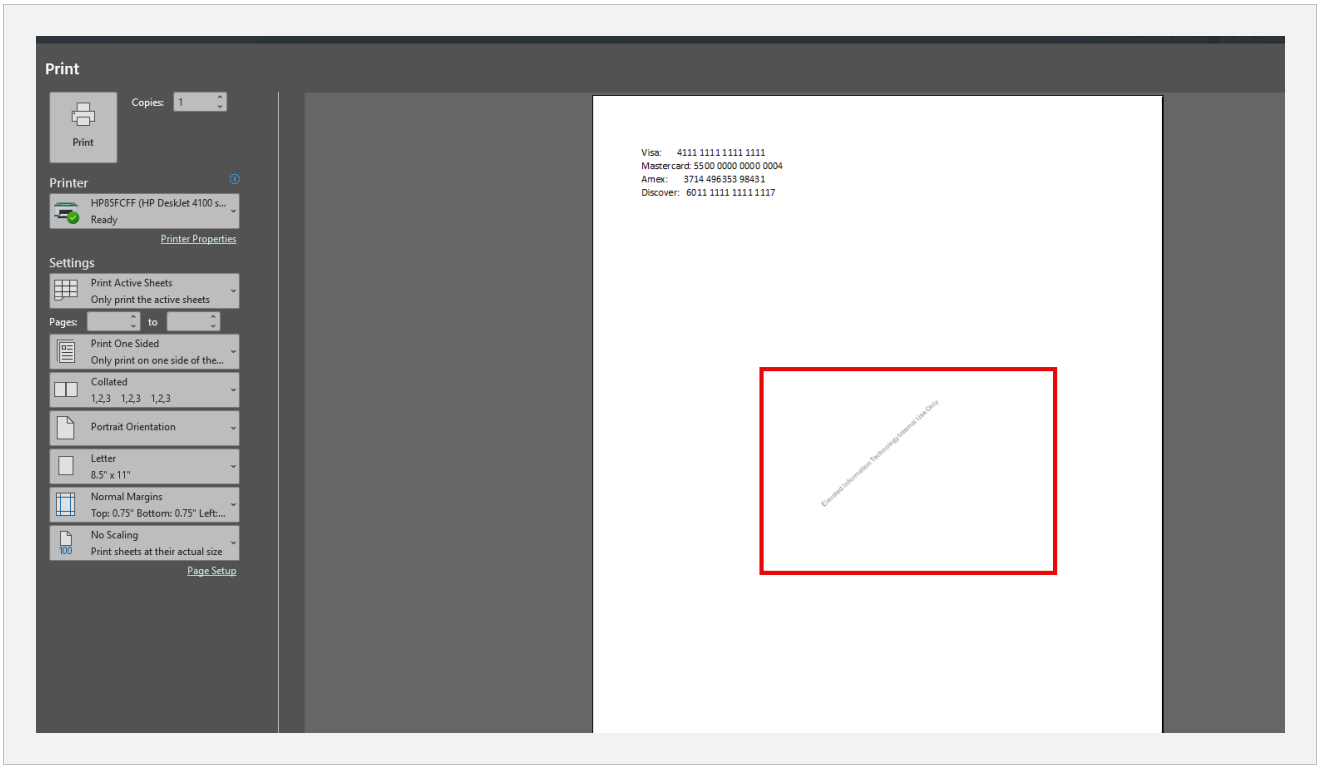

Figure 6. Watermark rendering on the labeled Excel workbook in Print preview.

5. Label Application — Word

A test Word document ("INTERNAL – Q3 Architecture Review Notes") was created in the same SharePoint site and opened in Word for the web. The Internal label was applied via the Sensitivity control. Unlike Excel, Word renders watermarks directly in the editing canvas — no view change required — making it the cleaner surface for demonstrating content marking.

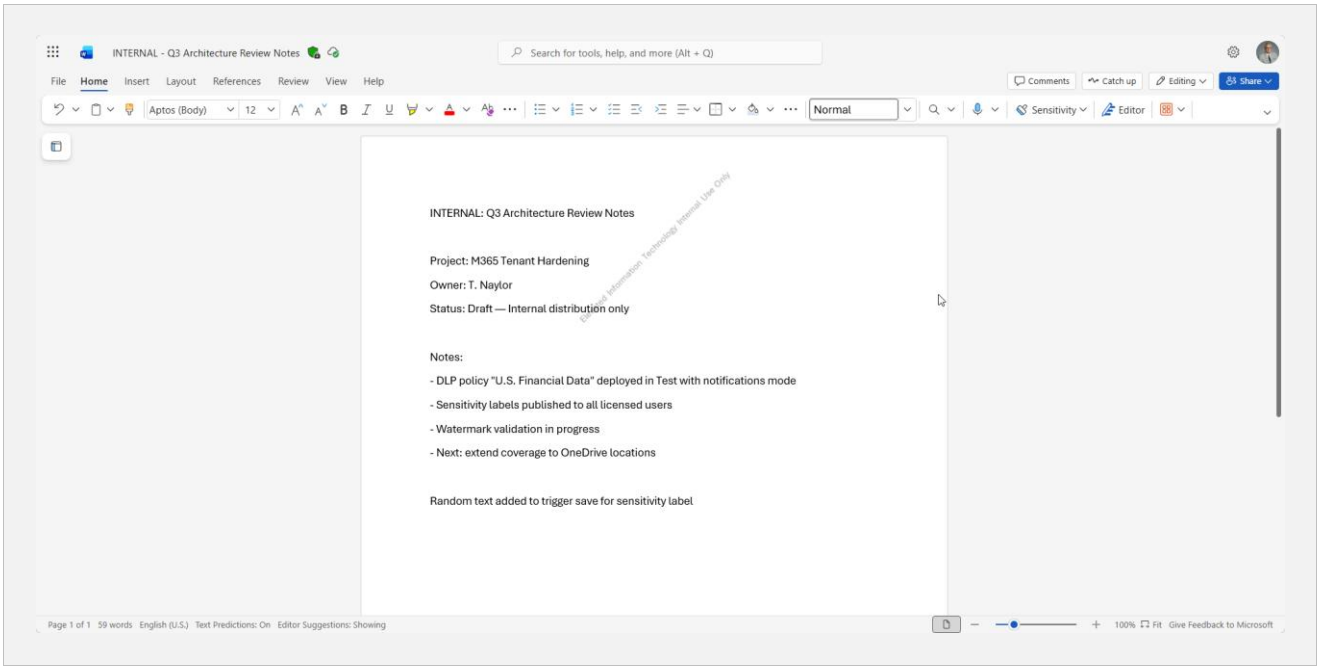

Figure 7. Watermark rendered in Word for the web editing view immediately after label application.

6. Audit Log Verification

Activity Explorer (Information Protection → Explorers → Activity explorer) is the curated dashboard for labeling and DLP events, but it operates with significant ingestion latency — particularly on Business Premium tenants, where events may take several hours to surface.

As a faster and more authoritative verification, the underlying unified audit log was queried directly via the Purview Audit search interface. A targeted query was authored against the operation names SensitivityLabelApplied and SiteSensitivityLabelApplied for the test date range.

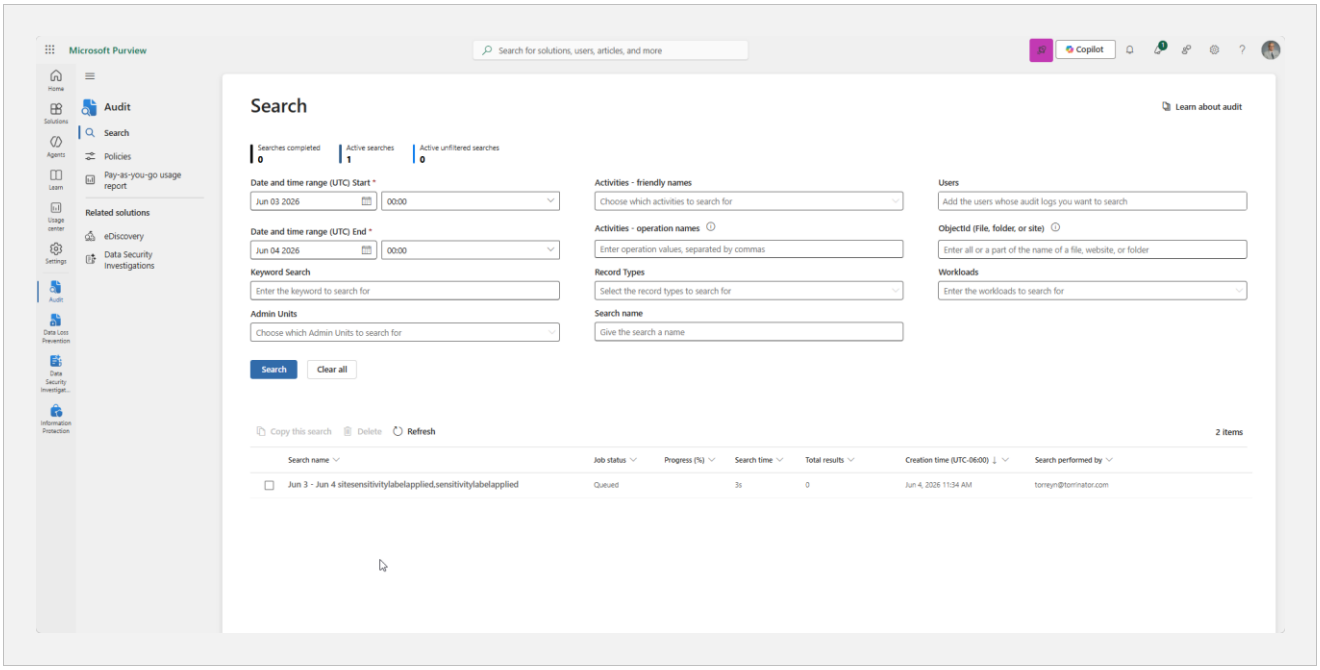

Figure 8. Direct audit log query authored against the unified audit log for label apply events.

Capabilities Demonstrated

This deployment exercises practical skills across the Microsoft 365 security and compliance stack:

Data Classification & Protection

- Sensitivity label design (taxonomy, scope selection, content marking, encryption posture)
- Label publishing policies and target user/group scoping
- DLP policy design with sensitive information types and audit-mode rollout

Microsoft 365 Administration

- Tenant-level configuration in Purview, SharePoint Online, and Microsoft 365 admin center
- Licensing analysis — mapping feature requirements to license entitlements
- End-user surface validation across Office desktop, Office for the web, and SharePoint

Audit & Compliance Operations

- Unified audit log search using operation-name queries (SensitivityLabelApplied, etc.)
- Understanding the relationship between Activity Explorer (curated view) and the underlying unified audit log (authoritative source)
- Distinguishing label apply events vs. Copilot interaction events in audit telemetry

Operational Judgment

- Audit-mode-first rollout discipline (DLP set to Test with notifications, not block)
- Recognition of latency in cloud telemetry pipelines and appropriate troubleshooting cadence
- Articulation of license-to-capability boundaries when scoping projects for non-E5 customers

Lessons Learned & Scale Considerations

Hands-on lab work surfaces details that documentation alone does not. The following notes capture observations from this deployment and how they would inform a real enterprise rollout.

Lessons Learned from the Lab

Purview RBAC is not Global Admin

Global Administrator in Microsoft 365 does not, by itself, grant the operational permissions needed to work in Purview. Purview uses its own role group model, and full administrative work — creating labels, publishing policies, querying the unified audit log, viewing Activity Explorer — depends on membership in the relevant Purview role groups (Information Protection Admin, Compliance Administrator, Compliance Data Administrator, Audit Reader, and others, depending on the workload).

Practical implication: even a tenant owner needs to explicitly assign themselves to the appropriate Purview role groups to perform compliance work. This is a deliberate separation-of-duties design — security and compliance administration are decoupled from tenant administration — and it must be planned into any rollout.

Publishing a label is not the same as applying it

A label publishing policy makes labels available to end users; it does not apply labels to existing content. Application happens through manual selection in Office apps, through default-label settings in the publishing policy (applies at save/create time in Office), or through auto-labeling policies (license-gated). This distinction is easy to miss when reading product documentation and is a frequent source of "why isn't this working?" troubleshooting.

Excel watermarks render where you don't expect them

Excel does not display watermarks in the default Normal view, only in Page Layout view and in Print preview/output. This is consistent behavior but unintuitive — many first-time deployments conclude that Excel watermarks are broken when in fact they simply weren't being viewed in a mode that renders them. Word, by contrast, renders watermarks immediately in the editing canvas, making it the better surface for stakeholder demos.

Audit telemetry has real latency

Activity Explorer in Purview is a curated dashboard built on top of the unified audit log. On Business Premium tenants in particular, ingestion latency can stretch from minutes to several hours. The unified audit log search interface is the authoritative source and often surfaces events faster than the curated Activity Explorer view. For time-sensitive verification, query the audit log directly using operation names (e.g., SensitivityLabelApplied).

The license boundary is operationally meaningful

Business Premium supports the full manual labeling workflow but does not include service-side auto-labeling for files at rest. This is not a gap that can be worked around — it is a license boundary. Any architecture conversation about scaling Purview Information Protection must include an honest license assessment and either a justification for the E5/IP&G add-on or a strategy that operates within manual-labeling constraints (e.g., default labels, user training, DLP-driven label application).

Considerations for Enterprise Scale

The lab work demonstrates the mechanics. Operationalizing this across a real organization requires deliberate planning across multiple disciplines.

Stakeholder engagement before configuration

Sensitivity labels are not just a technical control — they encode organizational decisions about what information matters, who can see it, and how it is handled. A rollout that begins in the admin portal without prior stakeholder engagement will produce a taxonomy that does not reflect how the business actually works.

- Engage department leads (Finance, HR, Legal, R&D, Sales) to identify their classification needs and existing handling practices
- Map labels to real business workflows rather than abstract sensitivity tiers
- Identify edge cases (M&A documents, board materials, customer PII, regulated data) early — they often need their own labels or sublabels

Legal coordination

Sensitivity labels have legal and regulatory implications beyond information security. Label decisions intersect with:

- Records retention obligations (labels can drive retention policies — get retention requirements from Legal/Records Management before publishing)
- Attorney-client privilege markings and litigation hold considerations
- Regulatory requirements (HIPAA, GDPR, SOX, FERPA, ITAR, CJIS, etc., depending on the industry) — labels are part of the compliance evidence chain
- Employee notice obligations — in some jurisdictions, applying classification or monitoring controls requires advance employee notification
- Cross-border data handling — some labels may need to drive geofencing or encryption requirements for international operations

Communications plan

Users see sensitivity labels in their daily Office experience. A rollout without a communications plan generates support tickets, workarounds, and erosion of the program's credibility.

- Pre-rollout announcement explaining what labels are, why they matter, and what users will see
- Training material — short, role-appropriate, with concrete examples relevant to each department
- Visible help resources (intranet page, Teams channel, ticket category) for user questions
- Manager/team-lead briefings before user-wide rollout so frontline questions can be answered locally
- Post-rollout follow-up after 30/60/90 days to gather feedback and adjust

Phased deployment

Avoid big-bang rollouts. A phased approach reduces blast radius and creates evidence to inform later waves.

- Pilot group: representative users across departments, with explicit feedback loop

- Audit mode first: DLP policies start in Test with notifications, auto-labeling in simulation mode, then graduate to enforcement
- Wave deployment by department or geography, with checkpoints between waves
- Pre-defined rollback criteria — if metrics (mis-classification rate, support volume, false-positive DLP hits) exceed threshold, pause and reassess

Operational monitoring

A deployment is not complete at go-live; it needs ongoing measurement.

- Coverage metrics: % of in-scope documents that carry a label
- Quality metrics: rate of label changes, downgrades, and user-reported mis-classifications
- DLP signal-to-noise: ratio of true positives to false positives over time
- Audit log review cadence — who looks at the unified audit log, how often, and against what criteria
- Quarterly label taxonomy review — labels accrue meaning over time; periodic review keeps the schema honest

Exception handling

Every classification program needs a defined process for exceptions — situations where a user legitimately needs to override, downgrade, or remove a label. Without a documented process, exceptions become shadow workarounds. A good exception process includes a request channel, an approver, a logged decision, and a periodic review of granted exceptions to identify systemic issues.

Certification Track Alignment

This work directly reinforces the Microsoft cybersecurity certification path the author is currently pursuing:

Certification	Domain coverage exercised in this lab
AZ-900	Azure fundamentals, including identity and shared responsibility model. Tenant administration and licensing covered here directly.
SC-900	Security, compliance, and identity fundamentals. Sensitivity labels, DLP, Purview, and Defender are core SC-900 exam objectives — this lab covers them hands-on.
AZ-500	Azure security technologies. The information protection and DLP work here is foundational for the AZ-500 "Manage security operations" domain and overlaps with M365 security tooling.
SSCP	Vendor-neutral security operations. The audit log query work and audit-mode policy rollout discipline map to SSCP "Risk Identification, Monitoring, and Analysis" and "Incident Response" domains.

Concurrent Coursework

The author is also actively enrolled at Colorado State University Global in:

- ITS350 — Information Systems and Security
- ITS415 — Principles of Cybersecurity

Both courses overlap directly with the deployment work shown here — information classification, access control, and audit/compliance operations are core to both curricula.

My credentialing is deliberately structured to build both vendor-specific and vendor-neutral cybersecurity foundations. The Microsoft track (AZ-900, SC-900, AZ-500, then SSCP and eventually CISSP) maps to federal compliance work; concurrent enrollment at CSU Global toward a B.S. in Cybersecurity (expected March 2027) reinforces the vendor-neutral concepts that NIST, HIPAA, and FedRAMP require. The combination positions me to translate between Microsoft's capability language and CMS's compliance language — the bridge role any CCSQ Product Manager must occupy.

Contact

Torrey Naylor

TorreyN@t-naylor.com

This portfolio piece documents lab work performed in the author's personal Microsoft 365 tenant. All sensitive data shown is synthetic test data using Microsoft's published test card numbers (e.g., Visa 4111-1111-1111-1111). No real customer or production data was used.