

MICROSOFT 365 DATA GOVERNANCE TOOLKIT







Practical tools to find your data, secure it, and govern AI — built on what you already own

Companion resource · AI Compliance as a Competitive Advantage Workshop



Most Microsoft 365 tenants are already licensed for powerful data governance and security tools — but fewer than 20% of organizations actively use them. This guide walks you through the key tools, the reports you can run TODAY, and the practical steps to understand where your data lives, who can access it, and where AI might be touching it without your knowledge.

1 | MICROSOFT PURVIEW — Data Governance & Compliance

Your command center for knowing what data you have, where it lives, and who can touch it.

TOOL	WHAT IT DOES	HOW TO ACCESS + QUICK WIN	NOTES / LICENSE
 Content Explorer	Shows every item across Exchange, SharePoint, OneDrive, and Teams that has a sensitivity label or retention label applied.	🔗 Go to: purview.microsoft.com → Data Classification → Content Explorer <i>⚡ Quick Win: See exactly which files/emails contain sensitive data (PII, financials, health records) and where they are stored.</i>	Requires: Information Protection Reader or higher role
 Activity Explorer	Logs every action taken on labelled content — who copied, printed, shared, or downloaded what, and when.	🔗 Go to: purview.microsoft.com → Data Classification → Activity Explorer <i>⚡ Quick Win: Audit trail for sensitive data. Instantly see if someone emailed a 'Confidential' document externally last week.</i>	Requires: Information Protection Analyst role or higher
 Sensitivity Labels	Tag data at source (email, document, meeting) so protection travels with the file — encryption, watermarking, access restrictions.	🔗 Go to: purview.microsoft.com → Information Protection → Labels <i>⚡ Quick Win: Auto-labelling can scan existing content and apply labels without user action — finds your unclassified sensitive data.</i>	Requires: Microsoft 365 E3/E5 or Purview Information Protection license
 Data Loss Prevention (DLP) Policies	Detect and block sensitive data from leaving your environment — stops paste into ChatGPT, external email of credit card numbers, etc.	🔗 Go to: purview.microsoft.com → Data Loss Prevention → Policies <i>⚡ Quick Win: Build a policy to block unclassified data from being sent to any generative AI endpoint (OpenAI, Claude, Gemini, etc.).</i>	Can run in 'audit only' mode first — see what WOULD have been blocked before enforcing.
 Data Map (Purview Governance Portal)	Scans connected data sources (Azure, AWS S3, SQL, SharePoint, Power BI) and builds a visual map of your data estate.	🔗 Go to: purview.microsoft.com → Data Map → Data Sources <i>⚡ Quick Win: Discover data you forgot you had. Shadow databases, old SharePoint sites, abandoned cloud storage.</i>	Requires: Microsoft Purview Data Governance license (separate from M365)
 Retention Policies & Labels	Define how long data is kept and when it is deleted — essential for HIPAA, FCA, and SEC obligations.	🔗 Go to: purview.microsoft.com → Data Lifecycle Management →	






Commented [ZL1]: Not sure on this one since I have never used it. Looks neat

		Retention policies ⚡ <i>Quick Win: Run a Retention Policy report to see gaps — data being kept too long (liability) or deleted too soon (legal hold risk).</i>	
 Compliance Manager	Scores your organization against 300+ regulatory frameworks (HIPAA, ISO 27001, NIST CSF, GDPR, SOC 2, FedRAMP).	 Go to: purview.microsoft.com → Compliance Manager ⚡ <i>Quick Win: Generates a Compliance Score and actionable improvement actions ranked by risk and effort. Free to access.</i>	 TIP: Filter by 'AI' in Compliance Manager to see AI-specific controls being added for regulations.

2 | MICROSOFT DEFENDER FOR CLOUD APPS — Shadow AI Discovery

Find every AI tool your employees are already using — approved or not.

Defender for Cloud Apps (formerly MCAS) catalogues 31,000+ cloud apps and now includes an 'AI Apps' category that specifically flags generative AI tools. It can tell you which AI services your organization is connecting to, how much data is flowing through them, and whether any are high-risk.

STEP	ACTION	WHERE TO GO + HOW TO DO IT	WHAT YOU'LL FIND
STEP 1	Run the Cloud Discovery Report	 Defender portal (security.microsoft.com) → Cloud Apps → Cloud Discovery → Dashboard Select date range (last 30 days) → Filter by Category: 'Generative AI' → Export report	You will see every AI app accessed, number of users, data uploaded/downloaded, and a risk score (1–10).
STEP 2	Review the AI App Risk Score	 Cloud Discovery → Discovered Apps → Filter: Category = AI/ML or Generative AI Sort by 'Risk Score' descending. Anything scoring 1–5 warrants investigation.	Risk score considers: does the app train on your data? Where is data stored? Is there a DPA? SOC 2 certified?
STEP 3	Identify your top AI data consumers	 Cloud Discovery → Users tab See which individuals or departments are uploading the most data to unapproved AI tools.	This is your Shadow AI heat map — you may be surprised which teams are most active.
STEP 4	Sanction or Block apps	 Discovered Apps → Select app → Mark as Sanctioned / Unsanctioned Unsanctioned apps can be automatically blocked via integration with Defender for Endpoint.	Create a 'Sanctioned AI' list — your Green Lane — and block everything else.
STEP 5	Set up ongoing AI app monitoring alerts	 Cloud Apps → Policies → App Discovery Policies → Create Policy Set alert: 'Notify me when a new Generative AI app is discovered with 5+ users'	Ongoing monitoring — you'll catch new Shadow AI tools as they appear, not 6 months later.

Commented [ZL2]: Step one and two could be done manually if you weren't using Intune. Just an app baseline

3 | MICROSOFT ENTRA ID — Who Has Access to What?

The identity and access layer — understand who can reach your sensitive data and prune what they shouldn't.

TOOL	WHAT IT DOES	HOW TO USE + QUICK WIN	NOTES / LICENSE
Access Reviews	Automated campaigns that ask managers: 'Does this person still need access to this group/app/role?'	🔗 Entra admin center (entra.microsoft.com) → Identity Governance → Access Reviews → New Access Review ⚡ Run a review on: (1) All Global Admin roles, (2) SharePoint site owners, (3) Users with access to sensitive data stores	Requires: Microsoft Entra ID P2 or Governance license
Privileged Identity Management (PIM)	Makes admin access time-limited and approval-based — nobody has standing Global Admin access.	🔗 Entra admin center → Identity Governance → Privileged Identity Management ⚡ Immediately see who has permanent privileged roles. Convert to 'eligible' (just-in-time) access.	🔗 Eliminates the #1 insider threat: over-privileged accounts sitting dormant.
Sign-in & Audit Logs	Every login, every app access, every password change — searchable, exportable, 30-day retention natively.	🔗 Entra admin center → Monitoring & Health → Sign-in logs ⚡ Filter: App = 'Microsoft Copilot' or any AI app name → see who is accessing AI tools and from where.	Export to Log Analytics / Sentinel for 90-day+ retention and automated alerting.
Conditional Access Policies	Rules that control HOW users can access apps — require MFA, block personal devices, restrict by location.	🔗 Entra admin center → Protection → Conditional Access → Policies ⚡ Create a policy: If user accesses an AI app → require MFA + compliant device + corporate network.	Requires: Entra ID P1 or higher
My Access Portal — Entitlement Management	Self-service access request portal — users request access to groups/apps, managers approve, access auto-expires.	🔗 myaccess.microsoft.com — set up via Entra admin center → Identity Governance → Entitlement Management ⚡ Build an access package for 'AI Tools — Approved Users' — staff request access, it's governed and auditable.	Eliminates ad-hoc access sharing. Every access grant has an owner, expiry, and justification.
Identity Secure Score	Scores your identity security posture 0–100 with ranked recommendations.	🔗 Entra admin center → Overview → Identity Secure Score ⚡ Run immediately — free, no configuration needed. Shows your top 10 identity risk actions.	

Commented [ZL3]: This requires an E3 or E5 license now I believe

Commented [ZL4]: Haven't done much with this one. Seems like a lot of overhead for all users but good for Admins or IT group

4 | GOVERNING MICROSOFT 365 COPILOT — Before You Enable It

Copilot surfaces data your employees can already access — so overpermissioned data becomes an AI risk.

⚠️ **Critical context: Microsoft 365 Copilot does NOT create new data access — it surfaces what users already have permission to see. If your data permissions are too broad (which they usually are), Copilot will expose that. The steps below must be done BEFORE enabling Copilot at scale.**

ACTION / TOOL	WHY IT MATTERS	HOW TO DO IT	WHAT YOU'LL FIND
Run the SharePoint Oversharing Report	Identifies SharePoint sites, libraries, and files shared with 'Everyone', 'Everyone except external users', or large groups.	🔗 SharePoint Admin Center (admin.microsoft.com → SharePoint) → Reports → Sharing → Export ⚡ <i>You will likely find hundreds of files accessible org-wide that contain sensitive data — remediate these first.</i>	Free. Run this before ANY Copilot rollout — Microsoft themselves recommend it as step 1.
Microsoft 365 Copilot Dashboard (Viva Insights)	Shows Copilot usage patterns, adoption rates, and which features are being used by whom.	🔗 admin.microsoft.com → Reports → Viva Insights → Copilot Dashboard ⚡ <i>Post-rollout: see if employees are using Copilot to access data outside their normal work context.</i>	Requires: Microsoft 365 Copilot license + Viva Insights
Sensitivity Label + Copilot Integration	Copilot respects sensitivity labels — it will not summarise or reference 'Highly Confidential' content unless the user has access.	🔗 Purview → Information Protection → Labels → Enable Copilot integration ⚡ <i>Label your most sensitive content FIRST. Copilot becomes a governance tool, not a risk.</i>	Requires: Microsoft Purview Information Protection
Copilot Usage Reports (Admin Center)	Shows which users have been assigned Copilot licenses, who is actively using it, and which apps they're using it in.	🔗 admin.microsoft.com → Reports → Microsoft 365 Apps Usage → Copilot ⚡ <i>Track adoption vs. license cost AND spot users accessing Copilot in unexpected contexts.</i>	Free with Copilot license
Data Access Governance (DAG) Reports — SharePoint	New Microsoft tool specifically designed to find overshared content before Copilot exposes it.	🔗 SharePoint Admin Center → Reports → Data Access Governance ⚡ <i>Run: 'Sites sharing with everyone' AND 'Sensitivity label activity' reports. Remediate top findings.</i>	Free. One of the most valuable pre-Copilot steps you can take.

⚡ 5 KEY REPORTS TO RUN THIS WEEK — No Configuration Required

These reports are available to any Microsoft 365 Global Admin or Security Reader right now — no extra license or setup needed.

REPORT 1: MICROSOFT SECURE SCORE

🔗 [security.microsoft.com](#) → Secure Score | Your security posture scored 0–100 with prioritised, actionable recommendations. Baseline in 5 minutes.

🎯 **Target:** score your organization today, share with leadership as your 'starting line'

REPORT 2: COMPLIANCE SCORE (COMPLIANCE MANAGER)

🔗 [purview.microsoft.com](#) → Compliance Manager | Scores against NIST, HIPAA, ISO 27001, GDPR and 300+ frameworks. Shows gap analysis and recommended actions.

🎯 **Target:** identify your top 3 compliance gaps and the Microsoft actions that will close them

REPORT 3: CLOUD APP DISCOVERY REPORT (SHADOW AI)

🔗 [security.microsoft.com](#) → Cloud Apps → Cloud Discovery | Every cloud and AI app being accessed by your users. Filter by 'Generative AI' category.

🎯 **Target:** count the number of AI apps. Present this number to leadership — it's always higher than expected

REPORT 4: SHAREPOINT DATA ACCESS GOVERNANCE REPORT

📍 SharePoint Admin Center → Reports → Data Access Governance | Files and sites shared with 'Everyone'. Critical pre-Copilot hygiene step.

🎯 **Target: identify top 10 overshared sites and assign remediation owners**

REPORT 5: IDENTITY SECURE SCORE

📍 entra.microsoft.com → Overview → Identity Secure Score | Scores your identity and access configuration. Flags weak spots like no MFA, standing admin access, etc.

🎯 **Target: complete the top 3 recommended identity actions — MFA alone often adds 20+ points**

6 | FREE MICROSOFT RESOURCES — Go Deeper

RESOURCE	URL / WHERE TO FIND IT	WHAT YOU GET
📖 Microsoft Purview Documentation Hub	learn.microsoft.com/en-us/purview/	Full documentation for all Purview tools — start with 'Get started with data governance'
🏠 Microsoft Learn: Information Protection	learn.microsoft.com/en-us/training/paths/implement-information-protection/	Free self-paced learning path — implement sensitivity labels and DLP from scratch. ~4 hours.
🏠 Microsoft Learn: AI Security Fundamentals	learn.microsoft.com/en-us/training/paths/responsible-ai-business-principles/	Microsoft's own Responsible AI principles and implementation guidance. Free.
📰 Microsoft Digital Defense Report (Annual)	microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2024	Annual threat intelligence report — real stats on AI-related threats, data breaches, and identity attacks.
🛡️ Microsoft Security Adoption Framework	aka.ms/MSRA	Step-by-step guidance for maturing your security posture across Zero Trust, identity, data, and AI.
📄 Microsoft AI and Responsible AI Resources	microsoft.com/en-us/ai/responsible-ai	Microsoft's Responsible AI Standard, impact assessment templates, and AI governance guidance.
📋 Microsoft Compliance Manager — Regulation Templates	purview.microsoft.com → Compliance Manager → Regulations	300+ regulatory templates — HIPAA, NIST CSF, ISO 27001, FCA, SOC 2, FedRAMP, PCI-DSS. All free to assess against.
💡 Microsoft Tech Community — Security & Compliance Blog	techcommunity.microsoft.com/category/security	Stay current — Microsoft posts practical 'how to' guidance for new features as they release.
🔍 Microsoft Purview: Data Governance for AI Workloads	learn.microsoft.com/en-us/azure/purview/concept-best-practices-ai-data-governance	Specifically covers how to govern data that flows through AI models. Highly relevant for this audience.
📺 Microsoft Mechanics — YouTube Channel	youtube.com/@MicrosoftMechanics	Video walkthroughs of every Microsoft security and compliance tool. Search 'Purview', 'Copilot governance', 'Defender for Cloud Apps'.

🚀 **YOUR FIRST ACTION: Log in to purview.microsoft.com and security.microsoft.com this week. You already own these tools. Start using them.**

Companion resource for: AI Compliance as a Competitive Advantage Roundtable