Microsoft Purview best practices

Atle Skjekkeland, CEO at Infotechtion
Microsoft MVP for Purview
Email: Atle.S@infotechtion.com



Infotechtion

Agenda

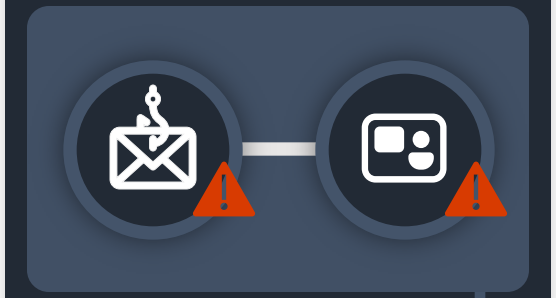
- Your data and AI risks
- Critical success factors for Purview
- Information Protection
- Data Loss Prevention
- Insider Risk Management
- Crawl-walk-run
- Operating model

Your data security risks

Data at risk of misuse if organization has no visibility into their data estate

External risks

User falls prey to phishing attack, compromises user credentials



Data compromise by external threat

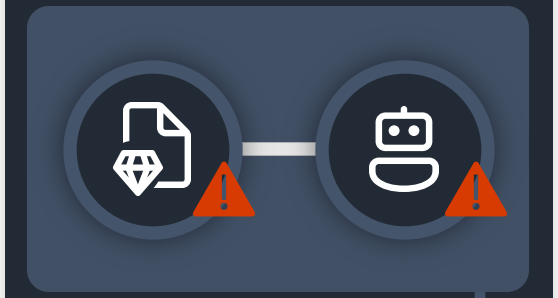
Internal risks

User copies file to a USB, then uploads to a personal Dropbox to take to a competitor



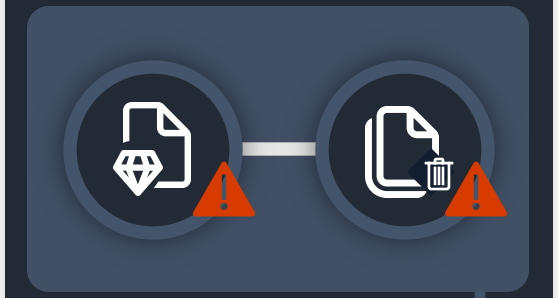
Data theft by malicious insider

User negligently shares sensitive data in generative AI apps



Data leak by negligent insider

User deletes sensitive information before leaving the organization



Data sabotage by disgruntled insider

Your AI risks



Data flowing into generative AI services grew 30x over the past year (source: Netskope 2025 Generative AI Cloud and Threat Report)



Nearly all employees (98%) use unsanctioned apps including shadow AI, creating a near-universal challenge for enterprise security and data governance (source: Varonis 2025 State of Data Security Report)



77% of organizations still lack the essential data and AI security practices needed to protect their business models and cloud infrastructure (source: Accenture State of Cybersecurity Resilience 2025)



Gartner predicts that by 2030, **more than 40% of enterprises will experience security or compliance incidents caused by shadow AI**.

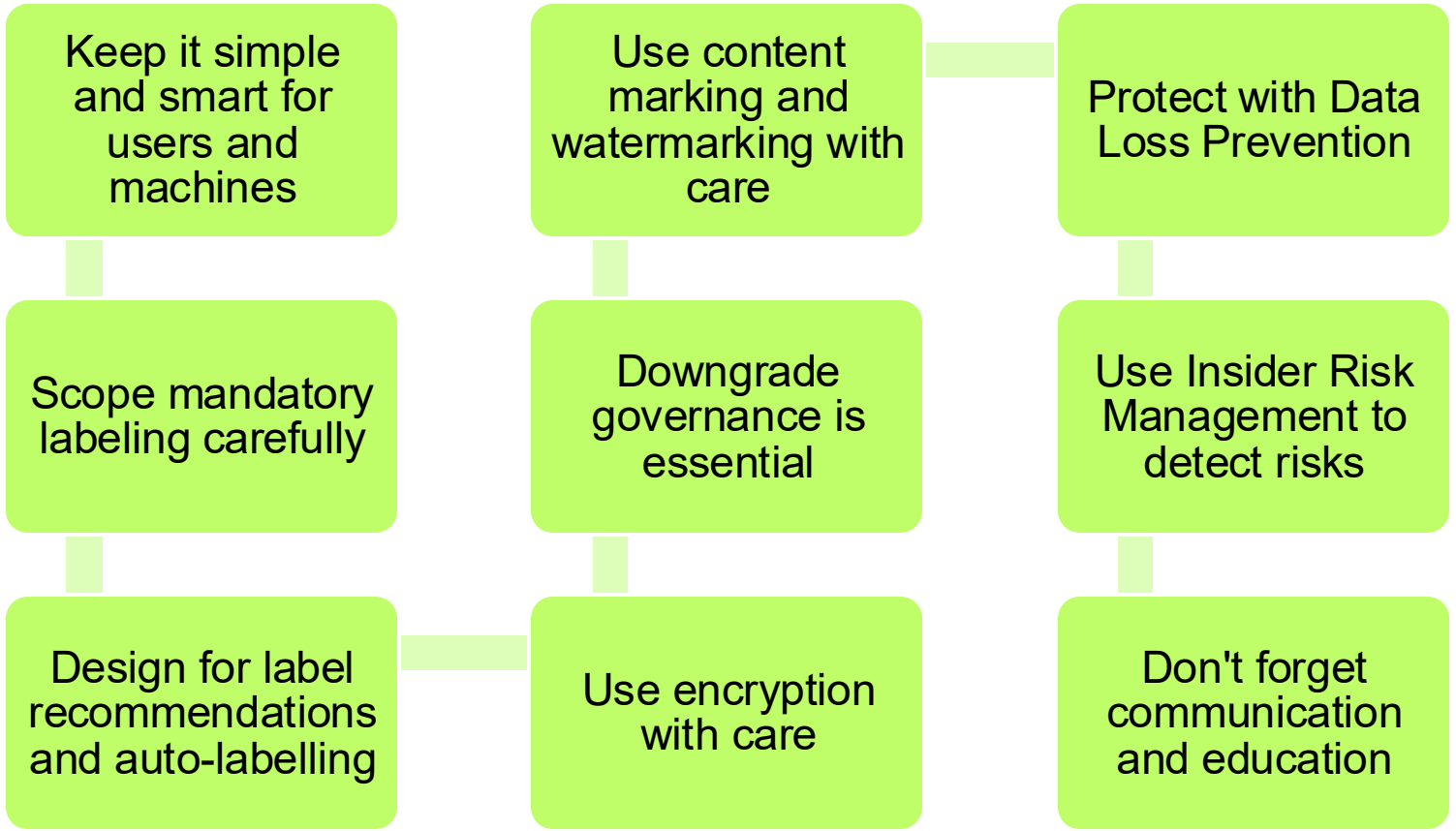


Gartner analysts expect that by 2028, **~25% of enterprise breaches will be traced back to AI agent abuse** — showing the long-term concern about these autonomous systems' role in threat landscapes.

Critical success factors for Microsoft Purview

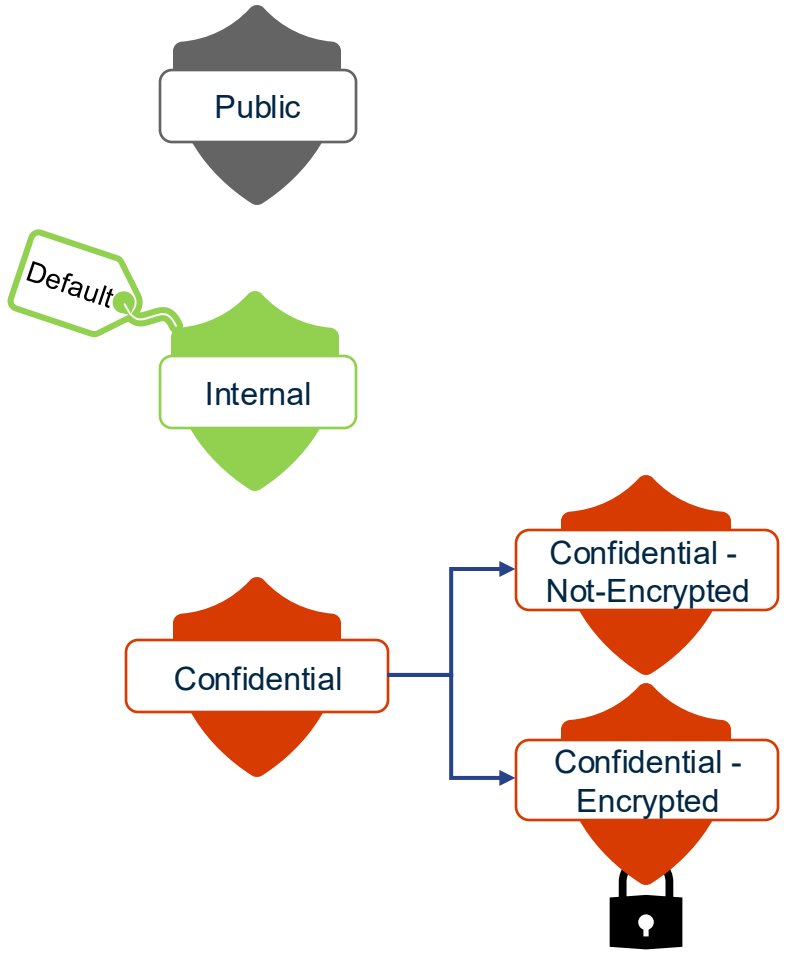
Governance model	Technology blueprint	Change management	Operating model
Establish policy and procedures defining how data must be secured and governed with roles and responsibilities	Establish baseline data security and compliance controls in Microsoft 365 with Microsoft Purview	Establish communication and education for users and workspace owners	Establish roles and responsibilities for monitoring and ongoing improvements (crawl-walk-run)
Examples:	Examples:	Examples:	Examples:
All information must have a security classification to ensure it is protected based on its sensitivity	Automating item sensitivity label classification based on storage location for new workspaces with provisioning engine	Quick tips and FAQs about how to best secure and govern data in Microsoft 365 and beyond, e.g., when to use Chat vs Channel, OneDrive vs SharePoint	Operating models for Microsoft Purview Information Protection, Data Loss Prevention, Insider Risk Management, Data Lifecycle Management, etc.
Information of value must be stored in shared workspaces to ensure it survives changes to people, organization, and technology	Real-time policy tips for users about correct security classification based on the sensitivity of the content	Data security training course for all employees covering: 1) store information in the correct location, 2) label information correctly, 3) Share links in emails instead of attachments	Processes for ongoing improvements, e.g. use of Content Explorer, Activity Explorer.

Best practices for Information Protection with sensitivity labels



Sensitivity label design example

- Three levels with future sub-labels when required
- Internal as default label in Office and Outlook
  - Files and emails labelled as internal can be shared with partners if there is a legitimate business need.
- Defult labelling to ensure old files get a label when opened by users
- Confidential has sub-categories with and without encryption
- Use of Confidential Not-Encrypted is monitored by IRM with low-threshold for alerts to identify wrong usage for the users with access to the label
- Additional sub-labels when required to cover unique requirements for specific user groups

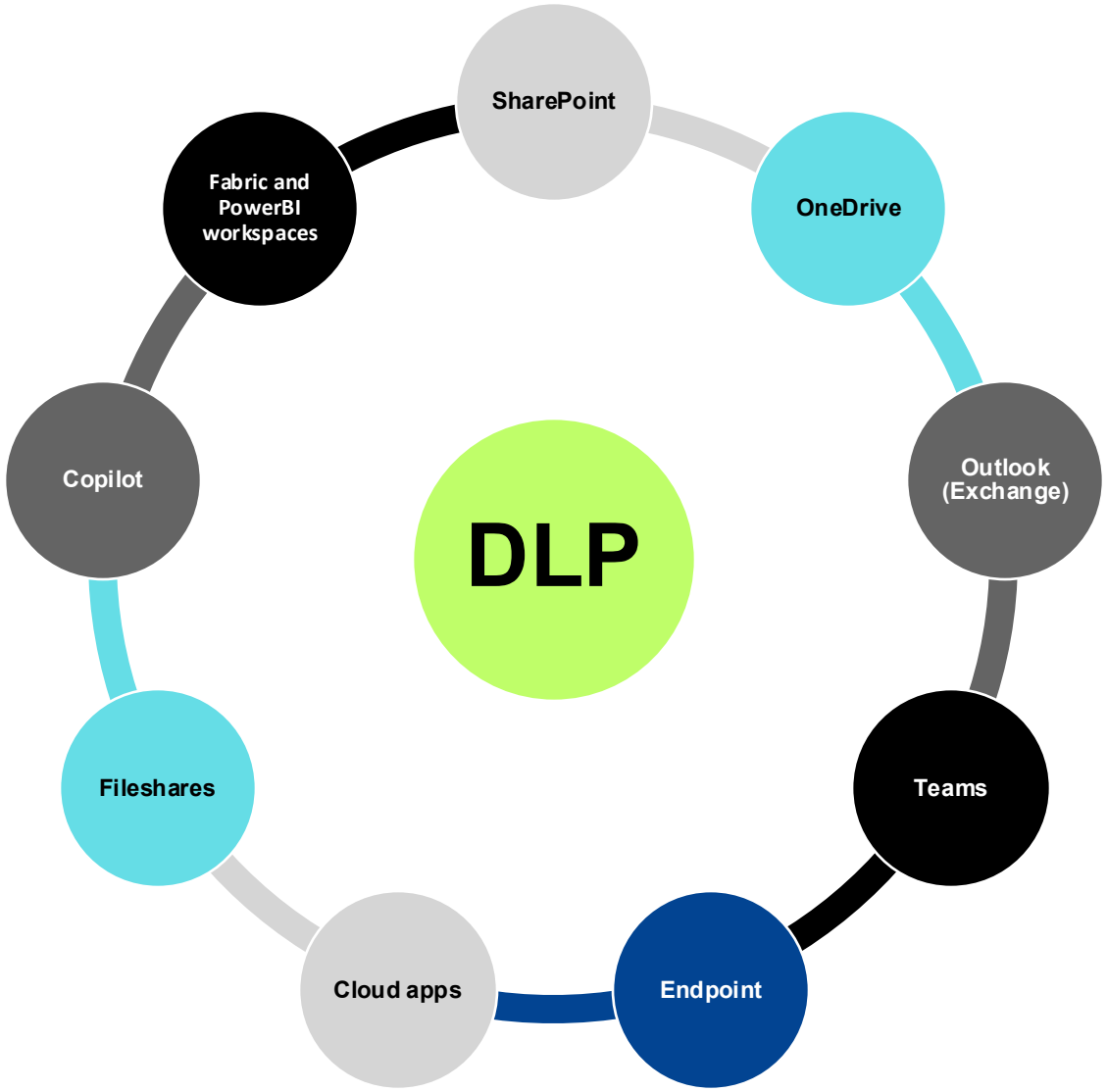


Container label design example with default sensitivity labels

Label name	Privacy	Guest users	Conditional access settings	Content can be shared with	Private team discoverability	Teams shared channels	Description
Internal workspace with Externals	Private	Yes	Unmanaged devices (Web-only access)	Everyone in org + new and existing guests	Yes	N/A	For content intended for internal use and a need for collaboration with external accounts.
Internal workspace without Externals	Private	No	Managed devices only	Everyone in org	Yes	Internal	For content intended for internal use and with no collaboration from external accounts.
Confidential workspace with Externals	Private	Yes	Unmanaged devices (Web-only access)	Everyone in org + new and existing guests	No	Internal	For Confidential content intended for internal use and a need for collaboration with external accounts.
Confidential workspace without Externals	Private	No	Managed devices only	Everyone in org	No	Internal	For confidential content intended for internal use and with no collaboration from external accounts.

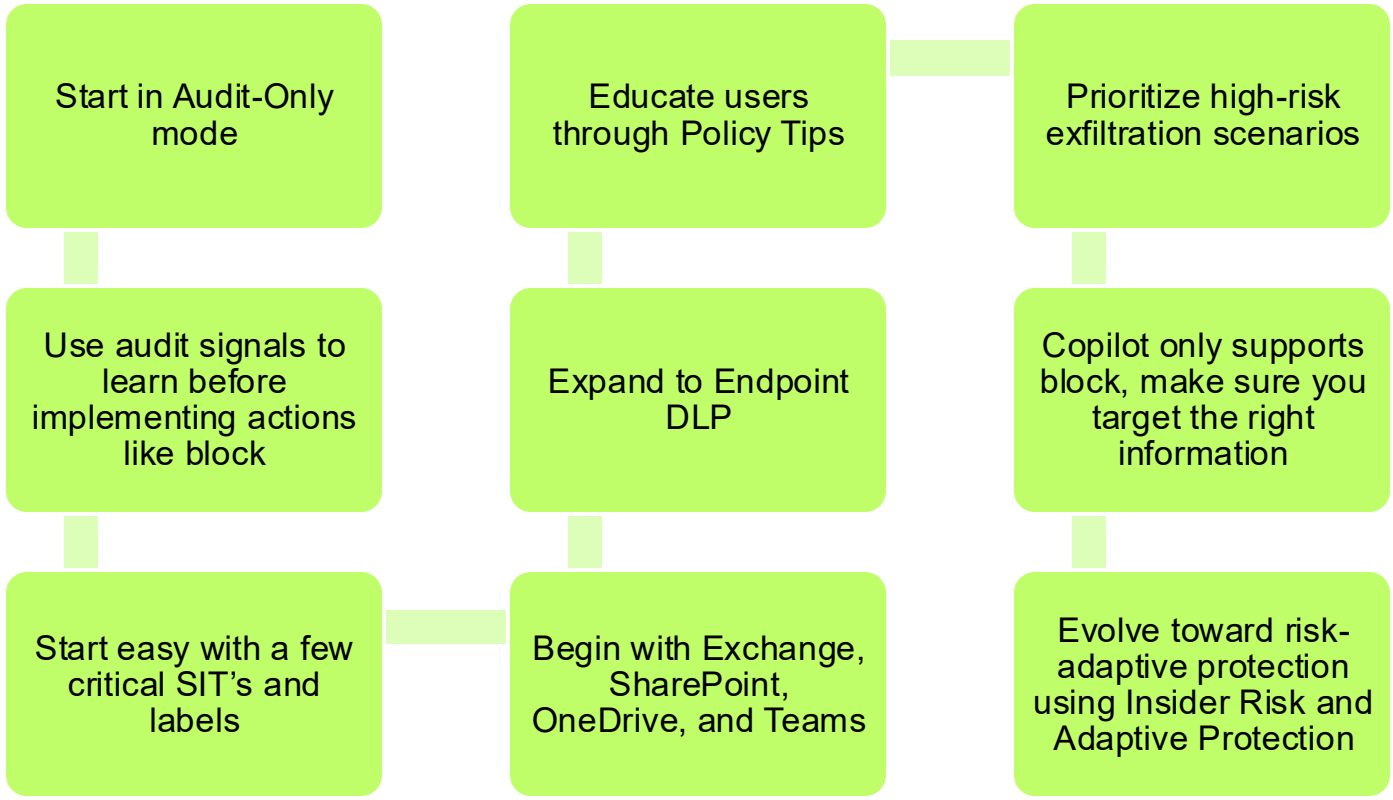
Data loss prevention

- Data Loss prevention has many features an organization can use.
- Examples:
  - Policy tips when privacy data is discovered in content
  - Soft-block the external sharing of information with, but allow users to override with justification
  - Hard-block sharing of internal information of specific value
  - Stop M365 Copilot from using some sensitive data
  - Block users from copying sensitive information to Shadow IT



Best practices with Data loss prevention (DLP) to protect information

- Don’t try to solve every “problem” from the beginning
- Use insights to take informed decisions and actions
- The goal is two-fold
  - Educate and raise awareness of information protection
  - Protect vital information



DLP design example

Name	Description	Why
Sending emails or files labelled as Confidential Encrypted	Sharing confidential information with externals is prohibited in XXX unless signed NDA is in place.	To guide the users in ensuring the correct sharing rules are being followed
Sending emails labelled as Confidential Not-Encrypted	Sharing confidential information without encrypted must only be used when handing over the information to the recipient	To guide the users in ensuring the correct sharing rules are being followed
Sending emails with .dwg and other CAD attachments	You are about to share a potentially sensitive filetype. Please ensure that the mail is marked with the appropriate label.	To see how often .dwg files are sent outside the org by email.
Policy tip on sharing links to information labelled as Confidential	When sharing files with confidential label, please ensure you share this with the correct people.	To guide the users to be wary when sharing confidential information
Copying content from files labelled as Confidential to low-risk apps	Sharing or uploading confidential information to external applications is not allowed in XXX	To prevent data leakage.

Insider Risk Management

IRM detects risky user behavior, and enables organizations to assess impact and respond to risk

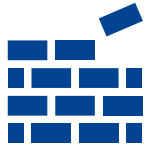
It helps identify both unintentional mistakes and malicious behavior by analyzing user activities across Microsoft 365



Transparency
Balance user privacy and organizational risks with privacy-by-design architecture



Configurable
Configurable policies based on industry, geographical and business groups

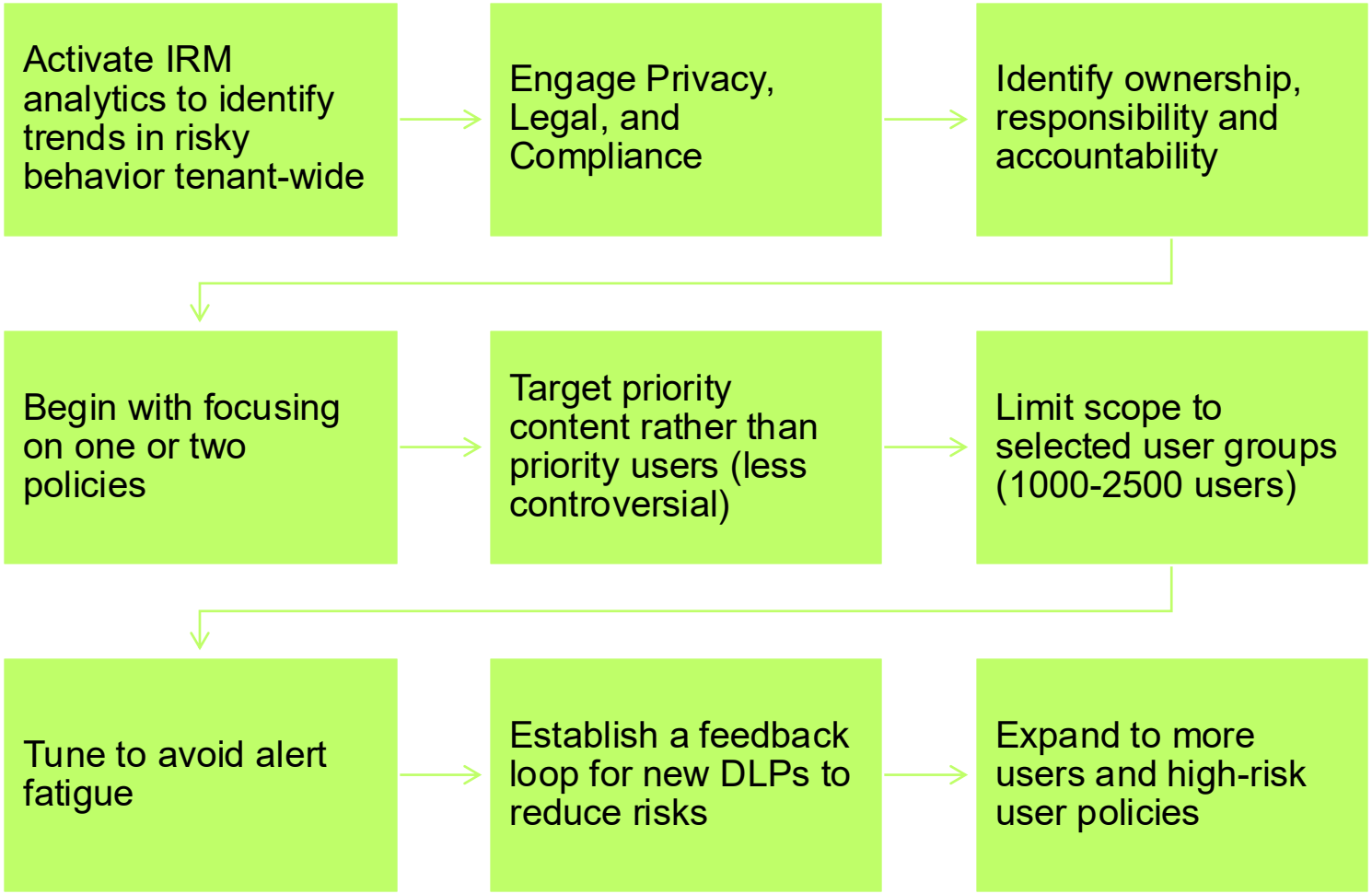


Integration
Integrated workflows across Microsoft Purview solutions



Actionable
Provides insights to enable reviewer notifications, data investigations and user investigations

First steps with IRM



Crawl-walk-run

Crawl
Get visibility



- Discover and understand your data
- Identify sensitive information
- Assess current risks
- Establish governance and key stakeholders

Know your data

Walk
Put controls in place



- Apply sensitivity labels
- Introduce DLP policies (start with guidance)
- Protect key data and workloads
- Build user awareness and processes

Reduce risk

Run
Scale and automate



- Automate classification and policy enforcement
- Extend to all workloads (cloud, endpoints, AI)
- Continuously monitor and improve
- Integrate with broader security and compliance

Protect at scale

Operating model for ongoing improvements



Additional resources

Sensitivity Label Best Practices – Keep the Taxonomy Simple and Let Microsoft Purview Do the Work | Infotechtion

Build DLP Baseline Policies Around Risk, Not Features | Infotechtion

Best practices for Microsoft Purview Insider Risk Management | Infotechtion

Microsoft Records Management Best Practices: Lessons from large scale implementations | Infotechtion

Your Organisation Has More AI Than You Think. The Real Question Is Who Controls It. | Infotechtion

How ROT Data Increases AI Risk, Compliance Exposure, and User Distrust | Infotechtion

Practical Agentic AI Governance – Building Confidence Before Scaling | Infotechtion

Stop Guessing, Start Governing | Infotechtion