Reality Tech
SharePoint Excellence

Microsoft Purview Readiness Assessment

5 Critical Gaps That Delay Governance & Secure AI Adoption

Is your organization truly prepared for secure AI adoption and enterprise-wide data governance with Microsoft Purview?

Many organizations implement governance controls but still face compliance gaps, inconsistent policy enforcement, and limited visibility into sensitive data across Microsoft 365 workloads.

Before expanding governance initiatives or enabling AI capabilities like Microsoft Copilot, assess whether these common risk indicators exist within your environment.

1. Are Sensitivity Labels Being Applied Consistently?

Your organization has labels configured, but employees classify data differently across Teams, SharePoint, Exchange, and OneDrive.

Common Indicators

- Sensitive documents remain unlabeled
- Labels are applied inconsistently across departments
- No auto-labeling or default labeling strategy exists

Potential Risk: Inconsistent classification weakens DLP enforcement, access governance, and encryption controls.

2. Are DLP Policies Preventing Data Exposure — Or Only Generating Alerts?

DLP policies exist, but security teams continue seeing excessive alerts, false positives, or repeated policy overrides.

Common Indicators

- Policies remain in audit-only mode
- High alert volume with limited remediation
- Users frequently bypass policy warnings

Potential Risk: Sensitive information may still be shared externally without effective enforcement controls

3. Do You Have Full Visibility Into Sensitive Data Across Microsoft 365?

Your organization cannot confidently identify where regulated or business-critical information exists.

Common Indicators

- Unknown external sharing activity
- Legacy repositories remain unclassified

- Limited visibility into sensitive data locations

Potential Risk: Governance blind spots increase compliance exposure and operational risk.

4. Are Retention & Compliance Policies Properly Aligned?

Retention policies have evolved over time without centralized governance oversight.

Common Indicators

- Conflicting retention configurations
- Inconsistent records management practices
- Delays responding to audits or eDiscovery requests

Potential Risk: Misaligned compliance controls increase audit preparation effort and regulatory exposure.

5. Is AI Being Enabled Before Governance Foundations Are Mature?

AI tools are being introduced before validating data classification, access governance, and protection controls.

Common Indicators

- Broad permissions across Microsoft 365 workloads
- Sensitive data accessible to large user groups
- Incomplete governance validation before AI rollout

Potential Risk: AI systems inherit existing access permissions and data exposure risks.

Executive Readiness Checklist

✓ Sensitive data discovery enabled across Microsoft 365
✓ DLP policies actively enforced and validated
✓ Sensitivity labels standardized and adopted
✓ Retention policies aligned with compliance requirements
✓ External sharing and access governance reviewed regularly
✓ Governance controls validated before AI enablement initiatives

Organizations that address these governance gaps early improve compliance readiness, strengthen data protection, and accelerate secure AI adoption.