CoreView's M365 Governance Starter Kit

Intro

58% of sensitive cloud data is stored in **SharePoint, Teams, and OneDrive**. This reliance on M365 has turned it into a **goldmine of sensitive data**.

With Microsoft 365 housing so much sensitive data, governance is a **#1 priority for CIOs** and CISOs.

Despite this, the data shows that **M365 customers are overwhelmed** with the task and **struggling with the basics**. The sheer scale of what Microsoft offers—**18 admin portals, 40 data silos**, and hundreds of APIs—makes the task, at best, an operational nightmare.

At worst, **unified control and governance is almost impossible**.

Failure to monitor and enforce these policies across all applications leads to **failed compliance requirements** and a **weakened security posture**.

Don't let establishing a robust governance framework bottleneck your initiative.

Get started building your M365 Governance plan with this starter kit.

What's in this Starter Kit?

This kit includes checklists, templates, and tools to form the basis of your M365 governance plan.

Click the link below to jump to the relevant section:

M365 Governance Assessment Checklist

This checklist acts as an initial diagnostic tool. Use it to identify and document the current state of M365 governance within the organization, focusing on compliance, security posture, and efficient use of M365 services.

Objective: Assess the current governance landscape by identifying strengths and weaknesses

Item	Status (compliant, non-compliant, N/A)	Notes
Identity and Access Management		
Enforce Multi-Factor Authentication (MFA) for all users		
Implement Hierarchical Conditional Access Policies based on departmental roles and needs		
Secure guest collaboration with periodic audits		
Establish and enforce strong password policies for cloud administrators, including regular reviews		
Audit external users and security groups to ensure relevance and security		
Scale identity management with automation. (E.g. automated audit and risk assessment tools)		
Security and Compliance		
Benchmark security posture and track progress through Secure Score and Compliance Score, setting clear benchmarks		
Configure anti-phishing and Microsoft Defender policies tailored to departmental risks across all applications		
Enable Insider Risk Management to proactively detect potential threats		
Customize Data Loss Prevention (DLP) policies for department-specific data types		
Review and schedule audit logs periodically, with alerts for unusual activities		
Sensitivity and retention policies, customized per data category and departmental needs		

Item	Status (compliant, non-compliant, N/A)	Notes
Integrate eDiscovery tools for content searches, holds, and exports as part of compliance activities		
Consider advanced data governance tools that leverage ML/AI technologies for smarter data governance.		
Teams Governance and Collaboration		
Establish Teams naming conventions and creation policies, adaptable for different departments		
Periodically review empty and inactive Teams groups		
Regularly audit guest user access and adjust external sharing settings to comply with security policies.		
Apply sensitivity labels for Teams, customized for varying levels of data sensitivity		
Integrate third-party applications in Teams following stringent security assessments		
Tailor external sharing settings to align with corporate security policies		
Set up Quality of Service (QoS) policies for optimal performance		
Use PowerShell scripts or other M365 automation tools for bulk task management		
M365 Licensing		
Conduct regular audits to align licenses with user roles and needs		
Identify unused or underused licenses for reallocation or cancellation.		
Maintain an up-to-date inventory of licenses to ensure compliance with Microsoft agreements.		
Implement license optimization tools or practices to match the right licenses with the right users, based on their usage patterns and needs.		
A license optimization or management tool can help scale this process.		
SharePoint and OneDrive Management		
Tailor classification, retention, and deletion policies to data governance policies.		
Regular review and adjustment of sharing and access permissions.		

Item	Status (compliant, non-compliant, N/A)	Notes
Establish guidelines for site creation, naming conventions, and template use		
Monitor storage quotas		
Implement SharePoint Syntex for better integration with external data systems and content management.		
Exchange Management		
Configure advanced security features including anti-phishing, anti-spam, and anti-malware policies.		
Establish policies for mailbox sizes, archival procedures, and distribution group memberships to maintain order and efficiency.		
Regularly audit mailboxes and distribution groups		
Device Management		
Implement customized Mobile Device Management (MDM) policies		
Review and adjust endpoint security strategies to align with corporate security policies		
Establish detailed BYOD policies to manage application access and data security		
Configure application protection policies in Microsoft Endpoint Manager		
Training and Awareness		
Create end-user training programs, tailored for different user groups within M365 tools		
IT staff trained on advanced M365 governance features, tools, and practices		
Regular governance reviews and updates communicated across all levels		
Governance Lifecycle and Policy Management		
Data centralized across all M365 admin portals		
Integrate governance policies with business workflows and third-party applications		
Automate detection of policy violations.		
Implement change management strategies for smooth transition to new governance frameworks		

Item	Status (compliant, non-compliant, N/A)	Notes
Build feedback mechanisms for continuous governance improvement		
Leverage automation and AI for policy management and enforcement		
Operational Integration and Change Management		
Establish guidelines for integrating governance policies with business processes		
Detail steps for communicating changes, handling resistance, and training in a change management playbook		
Establish a continuous feedback loop with IT, HR, legal, and business units to refine governance strategies		
Establish feedback channels for governance framework assessment from all stakeholders		
Adopt an agile governance adaptation process based on real-time feedback and organizational needs		
Create a Change Management Playbook		

PRINT CHECKLIST HERE

M365 Governance Assessment Strategy Template

Use this action-oriented template to identify gaps, compliance issues, and opportunities for optimization.

Objective: Gather detailed insights and create a structured plan of action

M365 governance plan for _____

(your company name)

Created on _____

(MM/DD/YYYY)

Version _____

Action Item	Instructions	Due date	Notes
Define Purpose	Briefly describe the goal of this M365 governance assessment, focusing on secure, compliant, and efficient use of Microsoft 365 within the organization.		
Define Scope	List the M365 services (e.g., Teams, SharePoint Online, Exchange Online) and features to be assessed.		☐ Exchange Online ☐ SharePoint Online ☐ Teams ☐ OneDrive for Business ☐ Yammer ☐ Additional tools: ☐ Custom tools:
Define Objectives	Define SMART objectives for the assessment, such as identifying gaps in compliance, improving data governance, or enhancing security postures.		
Stakeholder List	List out key stakeholders across IT, security, compliance, and business units.		
Stakeholder Roles and Responsibilities	Clearly delineate the involvement of each stakeholder in the governance process.		

Action Item	Instructions	Due date	Notes
Current State Analysis			
Configuration and Usage	Document the current setup and utilization patterns for each M365 service, including configurations and policies.		
Data Collection Tools	Specify tools (e.g., Microsoft 365 admin center, Compliance Manager) and methods for gathering necessary information.		
Service-Specific Usage Analysis	Analyze how each M365 service is being used within the organization.		
Third-Party Integrations	Assess the governance around third-party apps and services integrated with M365. This includes reviewing the permissions granted to these apps and evaluating their security and compliance posture.		
Security and Compliance Posture	Assess current security settings, compliance policies, and any existing governance measures.		
Benchmark Against Best Practices	Use Microsoft's best practices and industry standards as a benchmark. Consider including specific regulatory requirements that are relevant to your industry or sector, which might affect how you benchmark your practices.		
Detailed Risk Analysis	Break down the risk analysis to include specific threats to different M365 services.		
Risk Mitigation Strategies	For each identified risk, outline specific mitigation strategies, including technical controls, policy updates, and user training.		
Identify Gaps	Highlight areas of non-compliance, security vulnerabilities, and inefficient use of M365 services.		

Prioritize Issues	Rank the identified gaps based on risk, impact, and feasibility of mitigation. Incorporate a cost-benefit analysis for addressing each identified gap. This will help in prioritizing issues based on the value they bring versus the effort/cost required to mitigate them.		
Prepare Assessment Report:	Compile findings, gap analysis, and recommendations. Include: • An executive summary that highlights key findings, risks, and recommendations in a concise manner for quick consumption by senior management. • A detailed action plan with specific steps, responsible parties, and timelines for addressing each recommendation.		
Stakeholder Presentation	Present the assessment results to key stakeholders and discuss potential next steps. Define a mechanism for periodic follow-up on the implementation of governance improvements. This could include setting up quarterly review meetings.		

PRINT TEMPLATE HERE

M365 Governance Plan Template

Use this template to build a comprehensive Microsoft 365 governance framework that prioritizes security and collaboration.

Objective: Transform assessment insights into a concrete governance framework.

M365 governance plan for _____

(your company name)

Created on _____

(MM/DD/YYYY)

Version _____

Action Item	Instructions	Due date	Notes
Define the plan			
Define the purpose	Explain the necessity of the governance plan across Microsoft 365.		
Define the scope	Specify areas covered, including departments or the entire organization.		
Assign roles and responsibilities	Identify roles and their responsibilities within Microsoft 365.		
Establish policies and procedures			
Develop Microsoft 365 Lifecycle guidelines	Define policies for the management of resources across Microsoft 365.		
Establish Data Governance policies	Ensure secure and appropriate data management across Microsoft 365.		
Develop Application Management policies	Manage the use and integration of apps within Microsoft 365.		
Establish External Collaboration policies	Detail management of external sharing and guest access.		
Create Data Retention and Archival Policies	Determine retention schedules and archival practices.		

Action Item	Instructions	Due date	Notes
User and Activity Monitoring	Outline monitoring processes for Microsoft 365 activities.		
Security, privacy, and compliance			
Establish Security Measures	Implement security protocols across Microsoft 365.		
Control Privacy Settings	Manage privacy settings within Microsoft 365 services.		
Ensure Regulatory Compliance	Ensure compliance with regulations across Microsoft 365.		
Establish an Incident Response Plan	Prepare a strategy for potential security incidents.		
Control External Data Sharing	Set policies for secure data sharing externally.		
Define Backup and Recovery Processes	Detail backup and recovery plans for Microsoft 365 data.		
Establish Change Management Policies	Outline the process for changes within the Microsoft 365 environment.		
Ongoing training, adoption, and review			
Establish Accessibility Guidelines	Ensure Microsoft 365 content complies with accessibility standards.		
User Support	Define support mechanisms for Microsoft 365 users.		
Establish Performance Monitoring	Monitor performance and usage of Microsoft 365 services.		
Train Employees	Implement training on effective and secure use of Microsoft 365.		
Create Dispute Resolution Policies	Outline procedures for resolving Microsoft 365 related disputes.		
Establish Review Process	Set a schedule for regular reviews of the governance plan.		
Set up an Ongoing Audit Process	Implement audits of Microsoft 365 use for compliance.		
Define Reporting Requirements	Specify reporting needs for Microsoft 365 usage and compliance.		

PRINT TEMPLATE HERE

Additional resources

ARTICLE

Navigating Audit Logs

Learn to manage Office 365 audit logs, set retention policies, audit security events, and discover alternatives.

Read now

ARTICLE

Understanding Admin Roles

Learn about key admin roles, such as Global and Billing Admins, with our concise recommendations.

Read now

TEMPLATE

Microsoft Teams Governance Plan

Discover how to streamline Microsoft Teams collaboration and security with our template.

Download now

CHECKLIST

Teams Governance Checklist

Optimize Microsoft Teams governance: Plan strategically, manage access, and enforce clear policies.

Download now

VIDEO

5 Pillars of M365 Governance Model

Learn to establish governance policies, monitor compliance, evaluate strategies, and more.

Watch now

GUIDE

M365 Governance Best Practices

Learn M365 governance best practices for security, identities, Teams, SharePoint, and more.

Access now

End-to-end M365 security and governance

M365 workloads and Entra ID Tenants are a **#1 focus for cloud security**.

Despite this, the data shows organizations using M365 often **misconfigure critical tenant permissions, store sensitive cloud data in exposed files** and collaboration apps, and assign **global admin rights** just to stay productive.

Why? Because the scale and complexity of **M365 & Entra ID** environments are **overwhelming for admins and security** teams.

Organizations looking to **turn the tide on M365 governance** must:

- **Close the door on deadly misconfigurations**
- **Identify and remediate key collaboration and identity risks**
- **Prevent dangerous privilege exposure**

Make best practice M365 governance, security, and administration effortless with license oversight, no code automation, unified reporting and control, and automated tenant configuration from CoreView.

See end-to-end M365 security, governance, and automation made easy.
Take a [3-minute virtual tour] of the platform.