

Compliance Manager First-Week Priority Map

A 5-Day Operational Blueprint for CISOs & IT Administrators.

Opening Microsoft Purview Compliance Manager for the first time often triggers setup paralysis due to hundreds of unassigned improvement actions. This guide outlines the exact sequence of high-yield actions to execute during Week 1 to maximize your score gain with minimal operational effort.

DAY 1

Automated Assessment Sync & Baseline Scoping

Focus Area	Action Item	Score Impact
Secure Score Sync	Ensure automated testing is active so Microsoft Defender & Entra ID technical settings automatically credit points to Compliance Manager.	Immediate Boost
Framework Selection	Activate relevant assessment templates (e.g., Data Protection Baseline, GDPR, ISO 27001). Avoid enabling unused standards to prevent dashboard noise.	Baseline Setup

DAY 2

High-Impact Identity & Access Quick-Wins

Improvement Action	Technical Implementation	Score Impact
Enforce MFA for Admins	Configure Entra Conditional Access policy requiring MFA for all administrative roles. Automated detection grants instant compliance credit.	+27 Points
Restrict User Consent	Block end-user consent to unverified third-party OAuth apps in Entra ID settings. Automatically satisfies multiple regulatory controls.	+27 Points
Enable Password Protection	Turn on Entra Password Protection for cloud/hybrid accounts to block common weak passwords.	+27 Points

DAY 3 Baseline Data Security Controls

Improvement Action	Technical Implementation	Score Impact
Default Sensitivity Labels	Publish a baseline Sensitivity Label policy applying "Internal" classification to all new M365 files and emails.	+27 Points
Basic DLP Enforcement	Enable a standard DLP policy targeting credit card numbers and national ID data across Exchange, SharePoint, and OneDrive.	+27 Points

DAY 4 Cross-Assessment Documentation Unlocks

Documentation Type	Execution Strategy	Score Impact
Information Security Policy	Upload existing InfoSec policy documentation to a single core Improvement Action. Select "Apply to all related controls" to score across multiple regulations at once.	Multi-Control Multiplier
Incident Response Plan	Upload your current IR response framework to satisfy breach notification requirements across GDPR, NIS2, and ISO templates simultaneously.	Multi-Control Multiplier

DAY 5 Stakeholder Assignment & Audit Readiness

Operational Action	Execution Strategy	Score Impact
Assign Non-Technical Actions	Assign HR, Legal, and Facility improvement actions (e.g., physical security, onboarding policies) directly to responsible owners with clear due dates.	Governance Alignment
Export Executive Report	Generate the Compliance Manager Executive Summary report to present week-one score improvements to leadership.	CISO Reporting

Golden Rule for Compliance Manager Success

- **Automate First, Document Second:** Technical actions tested by automated checks give instant point verification without requiring manual evidence uploads.
- **Use the "Parent Control" Effect:** Uploading core policy evidence once can clear compliance requirements across dozens of frameworks (GDPR, ISO, NIST) simultaneously if mapped correctly.