

FREE COMMUNITY ASSET

Compliance Manager & Zero Trust Starter Kit

Pre-audit assessment blueprint mapping native free controls to HIPAA, NIST 800-53, and CMMC frameworks without third-party overhead.

1.0 ZERO TRUST ARCHITECTURE: THE THREE GOLDEN RULES

Zero Trust is an operational security model that eliminates implicit trust from all system interactions. Whether a request originates inside the corporate local network or from a remote coffee shop, Zero Trust mandates:

- * **1. Verify Explicitly:** Always authenticate and authorize based on all available data points (identity, location, device health, resource classification).
- * **2. Use Least Privileged Access:** Limit user access with Just-In-Time (JIT) and Just-Enough-Access (JEA) models, adaptive risk policies, and data protection.
- * **3. Assume Breach:** Minimize blast radius by segmenting access by network, user, devices, and application awareness. Encrypt all end-to-end telemetry.

2.0 MICROSOFT PURVIEW COMPLIANCE MANAGER: FREE BASELINE

Microsoft Purview Compliance Manager is built directly into Microsoft 365 to measure compliance progress against global standards. Every tenant receives the 'Data Protection Baseline' assessment free of charge.

- * **Regulatory Alignment:** Maps native cloud configurations directly against controls from NIST CSF, ISO 27001, and HIPAA.
- * **Continuous Evidence Gathering:** Automatically audits whether encryption at rest, audit logging, and role separations are active without manual spreadsheets.

3.0 PRE-AUDIT SELF-ASSESSMENT QUESTIONNAIRE

- * **[] Identity Hygiene:** Are administrative accounts strictly separated from everyday email/browsing accounts? (Yes / No)
- * **[] Disk Encryption:** Is BitLocker (Windows) or FileVault (macOS) enforced with TPM hardware attestation on all laptops? (Yes / No)
- * **[] Audit Logging:** Is Unified Audit Logging enabled in Purview, retaining 180+ days of mailbox and file access logs? (Yes / No)
- * **[] Network Isolation:** Are office printers, IoT smart TVs, and guest Wi-Fi segregated into isolated VLANs away from production workstations? (Yes / No)
- * **[] Offboarding Killswitch:** Does your offboarding checklist terminate Active Directory/Entra tokens within 15 minutes of employee departure? (Yes / No)

REGULATORY PENALTIES WARNING

HIPAA and CMMC compliance investigations focus heavily on 'lack of basic technical controls' (e.g., missing MFA, unencrypted laptops). Documenting your native configurations using this starter kit provides critical safe-harbor evidence in dispute resolutions.

4.0 IMPLEMENTATION PATH

- * **Access Portal:** Sign in to Microsoft Purview at <https://purview.microsoft.com/> or <https://compliance.microsoft.com>.

- * **Select Assessments:** Open 'Compliance Manager' -> 'Assessments'. Review your baseline score percentage.
- * **Assign Improvement Actions:** Delegate control tasks (e.g., 'Turn on BitLocker') directly to system administrators with step-by-step verification notes.

5.0 DIRECT LINKS & REFERENCE FRAMEWORKS

Microsoft Purview Compliance Portal: <https://compliance.microsoft.com>

Microsoft Zero Trust Guidance Center: <https://learn.microsoft.com/en-us/security/zero-trust/>

NIST Computer Security Resource Center: <https://csrc.nist.gov>