Microsoft 365 & Entra Security Posture Assessment Checklist

Multifactor Authentication (MFA)

What to Evaluate: Ensure MFA is enforced for all users, especially admins, service accounts, and external users.

Tool: Microsoft Entra > Conditional Access

Where to Find It: Microsoft Entra Admin Center → Protection → Conditional Access

Conditional Access Policies

What to Evaluate: Evaluate risk-based policies, proper scoping (admins, contractors, high-privilege roles).

Tool: Microsoft Entra > Conditional Access

Where to Find It: Microsoft Entra Admin Center → Protection → Conditional Access

Identity Protection

What to Evaluate: Review sign-in risk detections, user risk detections, and risk remediation policies.

Tool: Microsoft Entra > Identity Protection

Where to Find It: Microsoft Entra Admin Center → Protection → Identity Protection

User and Group Review

What to Evaluate: Check for orphaned accounts, accounts without MFA, role assignments, external/guest users.

Tool: Microsoft Entra > Users, Groups, and Roles

Where to Find It: Microsoft Entra Admin Center → Identity → Users / Groups / Roles and Administrators

Audit Logs

What to Evaluate: Monitor admin activities, logins, privilege escalations, group changes.

Tool: Microsoft 365 Compliance Center > Audit

Where to Find It: compliance.microsoft.com → Audit → Search

Microsoft Defender for Office 365

What to Evaluate: Evaluate Safe Links, Safe Attachments, anti-phishing, and impersonation protection settings.

Tool: Microsoft 365 Security Center > Policies & Rules

Where to Find It: security.microsoft.com → Email & collaboration → Policies & rules → Threat policies

Microsoft Secure Score

What to Evaluate: Review overall score and actionable improvement recommendations.

Tool: Microsoft Secure Score

Where to Find It: security.microsoft.com → Secure Score

Mail Flow Rules (Transport Rules)

What to Evaluate: Check for DLP rules, external email banners, spoofing protections.

Tool: Exchange Admin Center > Mail Flow

Where to Find It: admin.exchange.microsoft.com → Mail flow → Rules

Privileged Role Access Reviews

What to Evaluate: Audit Global Admin, Security Admin access and usage. Review PIM use if available.

Tool: Microsoft Entra > Roles and Administrators + PIM

Where to Find It: Microsoft Entra Admin Center → Identity → Roles and administrators

Compliance Manager

What to Evaluate: Check regulatory gaps (e.g., HIPAA, ISO) and review improvement actions.

Tool: Microsoft Compliance Center > Compliance Manager

Where to Find It: compliance.microsoft.com → Compliance Manager

Microsoft Defender Recommendations

What to Evaluate: Review endpoint onboarding, AV/firewall/EDR settings, and alert configurations.

Tool: Microsoft 365 Defender / Defender for Endpoint

Where to Find It: security.microsoft.com → Device inventory / Recommendations

Sign-in Logs & Risky Sign-ins

What to Evaluate: Identify unusual login patterns, legacy protocols, and frequent failures.

Tool: Microsoft Entra > Sign-in logs

Where to Find It: Microsoft Entra Admin Center → Monitoring → Sign-in logs

App Registrations & Permissions

What to Evaluate: Audit enterprise apps with high-level permissions and third-party consent grants.

Tool: Microsoft Entra > Enterprise Applications

Where to Find It: Microsoft Entra Admin Center → Identity → Applications → Enterprise Applications

Data Loss Prevention (DLP)

What to Evaluate: Review policies for PII, PHI, financial data across Teams, Email, OneDrive, SharePoint.

Tool: Microsoft Purview > Data Loss Prevention

Where to Find It: compliance.microsoft.com → Data loss prevention

Baseline Configuration Benchmark

What to Evaluate: Compare settings with Microsoft Baseline or CIS Benchmarks.

Tool: MS Baseline Security Analyzer or CIS Benchmark Guide

Where to Find It: https://learn.microsoft.com/en-us/security/benchmark or https://www.cisecurity.org/cis-benchmarks