Security Baseline Validation – Strategy & Approach

Version: 2025-09-28 14:25 UTC | Branding: Generic

# 1. Executive Summary

This document defines the strategy and approach to validate the Microsoft 365, Entra ID, and Azure baseline controls. Role validation is limited to user assignment and least-privilege checks for Entra ID and Azure RBAC built-in roles (no functional action testing).

# 2. Scope

Controls in scope (from baseline):

* CA1: Require & enforce MFA for organization admins
* CA2: Require & enforce MFA for enablement admins/users
* CA3: Activate MFA for M365 cloud users
* CA4: Identity Protection policy active for risky users and risky sign-ins
* CA5: Block legacy authentication for activated cloud users
* CA6: Restrict access by location to Zscaler IP (exception group for MSFT staff)
* CA7: Require App Protection Policy (MAM) on mobile devices
* AC1: Project users are cloud-only accounts
* AC2: Guest access disabled (no guests or sharing)
* PW1: Minimum password policy – complexity >= 12 characters
* DV1: Corporate devices provisioned with Mworks/Intune and compliant
* TL1: Defender for Cloud Apps enabled (default state)
* TL2: Explore policy to block files (optional)
* TL3: Safe Links and Safe Attachments for Teams/SPO/OneDrive
* TL4: Customer Key Management for M365 configured
* TL5: M365 Unified Auditing is enabled
* IP1: Publish labels: Highly Confidential, Confidential, Restricted, Public (org users)
* IP2: Default label 'Restricted' for org users
* IP3: Microsoft users default label 'Confidential'
* IP4: Labels allow project team members in Teams to consume documents
* IP5: No sensitivity reduction allowed
* DLP1: Block MY/SG IDs, passport, credit cards & encrypted attachments
* DLP2: Block USB and Bluetooth for all users
* DLM1: Retention policy 15 years for EXO/SPO/Teams/M365 Groups/Copilot

Entra ID roles in scope (assignment-only):

* Global Administrator
* Identity Governance Administrator
* Privileged Role Administrator
* Lifecycle Workflows Administrator
* Privileged Authentication Administrator
* Microsoft Graph Data Connect Administrator
* Conditional Access Administrator
* Permissions Management Administrator
* Intune Administrator
* Power Platform Administrator
* Security Administrator
* Search Administrator
* Billing Administrator
* Security Operator
* Exchange Administrator
* Security Reader
* Teams Administrator
* Teams Communications Administrator
* AI Administrator
* Application Administrator
* Windows 365 Administrator
* Windows Update Deployment Administrator
* Attribute Assignment Administrator
* Attribute Assignment Reader
* Attribute Definition Reader
* Attribute Log Administrator
* Attribute Log Reader
* Attribute Provisioning Administrator
* Attribute Provisioning Reader
* Authentication Administrator
* Authentication Policy Administrator
* Azure DevOps Administrator
* Azure Information Protection Administrator
* B2C IEF Keyset Administrator
* B2C IEF Policy Administrator
* Cloud App Security Administrator
* Cloud Application Administrator
* Cloud Device Administrator
* Compliance Administrator
* Customer Lock Box Access Approver
* Directory Writers
* Domain Name Administrator
* Dynamics 365 Administrator
* Dynamics 365 Business Central Administrator
* External Identity Provider Administrator
* Fabric Administrator
* Global Reader
* Global Secure Access Administrator
* Global Secure Access Log Reader
* Hybrid Identity Administrator

Azure RBAC roles in scope (assignment-only):

* Owner
* Contributor
* Reader
* User Access Administrator
* Key Vault Administrator
* Key Vault Certificates Officer
* Key Vault Secrets Officer
* Key Vault Reader

# 3. Resources Required

## 3.1 Accounts

|  |  |  |
| --- | --- | --- |
| Type | Example ID | Purpose |
| Admin - Global | admin-global@testtenant.com | Tenant-wide configuration/evidence collection |
| Admin - Security | admin-security@testtenant.com | Security portal, DLP, Safe Links/Attachments, Audit |
| Admin - Identity | admin-identity@testtenant.com | Entra ID Conditional Access, Identity Protection, MFA |
| Standard User | user-standard@testtenant.com | User-side validation of CA, labels, DLP |
| Guest (negative) | guest-ext@external.com | Guest/External access negative tests if applicable |

## 3.2 Devices

|  |  |
| --- | --- |
| Device | Use |
| Windows 11 Corporate Laptop (Intune-managed) | Positive path; compliant device; Zscaler egress IP |
| Unmanaged Personal Laptop | Negative path; non-compliant; non-Zscaler IP |
| Managed iOS/Android with Authenticator | MFA verification and App Protection Policy checks |

## 3.3 Tools/Portals

|  |  |  |
| --- | --- | --- |
| Tool | URL | Use |
| Entra Admin Center | https://entra.microsoft.com | Conditional Access, Identity Protection, Sign-in logs, Role assignments |
| Microsoft 365 Admin Center | https://admin.microsoft.com | User provisioning, Org settings |
| Microsoft Purview (Compliance) | https://compliance.microsoft.com | DLP, Information Protection labels, Audit, Retention |
| Microsoft Defender Portal | https://security.microsoft.com | Safe Links, Safe Attachments, Threat policies |
| Azure Portal | https://portal.azure.com | Azure RBAC (IAM), Defender for Cloud, Key Vault RBAC |
| Office Apps | N/A | Word/Excel/Outlook/Teams clients for user-side tests |
| PowerShell / Azure CLI | N/A | Export role assignments and evidence where required |

# 4. Validation Methodology

1. Identify the control and target scope.
2. Execute steps in the designated portal/URL using the specified account and device.
3. Capture evidence (screenshots, exports, logs).
4. Record result and exceptions in the Excel Execution Workbook.

# 5. Control Procedures (High Level)

## CA1 – Require & enforce MFA for organization admins

Domain: Conditional Access

Portal/Tool: Entra (https://entra.microsoft.com)

Accounts: admin-identity, admin-global | Devices: Corporate laptop + Authenticator

Procedure:

1. 1. Open Entra Admin Center (https://entra.microsoft.com) and sign in as admin-identity.
2. 2. Go to Protection > Conditional Access > Policies.
3. 3. Locate policy 'MFA for Admins' (if absent, record as gap).
4. 4. Open the policy and verify Assignments: Users = admin roles, Cloud apps = All, Grant = Require multifactor authentication, Enable = On.
5. 5. Sign out and sign in with admin-global to confirm MFA challenge occurs.

Expected Result: Policy exists and is enabled; all targeted admin sign-ins require MFA.

Evidence: Screenshot of policy settings; Entra Sign-in log showing MFA requirement and success for admin-global.

## CA2 – Require & enforce MFA for enablement admins/users

Domain: Conditional Access

Portal/Tool: Entra (https://entra.microsoft.com)

Accounts: admin-identity, admin-security | Devices: Corporate laptop + Authenticator

Procedure:

1. 1. In Entra Conditional Access > Policies, find 'MFA for Enablement Admins/Users'.
2. 2. Verify Assignments include Security Administrator, User Administrator (or relevant groups).
3. 3. Verify Grant controls include 'Require multifactor authentication' and policy is Enabled.
4. 4. Sign in as admin-security to confirm MFA prompt.

Expected Result: Enablement admin accounts are forced to use MFA.

Evidence: Policy screenshot; sign-in log for admin-security showing MFA enforced.

## CA3 – Activate MFA for M365 cloud users

Domain: Conditional Access

Portal/Tool: Entra (https://entra.microsoft.com)

Accounts: user-standard | Devices: Corporate laptop + Authenticator

Procedure:

1. 1. In Entra > Conditional Access > Policies, locate 'MFA for All Users' (or per-group).
2. 2. Confirm Users/Groups include cloud-only users (project group).
3. 3. Confirm Grant includes 'Require multifactor authentication' and is Enabled.
4. 4. Sign in as user-standard at https://portal.office.com and confirm MFA prompt.

Expected Result: All cloud users in scope are challenged for MFA.

Evidence: Policy screenshot and sign-in log for user-standard with MFA satisfied.

## CA4 – Identity Protection policy active for risky users and risky sign-ins

Domain: Conditional Access

Portal/Tool: Entra (https://entra.microsoft.com)

Accounts: user-standard | Devices: Corporate laptop + VPN (unusual IP)

Procedure:

1. 1. Navigate to Entra > Protection > Identity Protection > User risk policy & Sign-in risk policy.
2. 2. Verify policies are Enabled with 'Require password change' or 'Require MFA' as per design, and include in-scope users.
3. 3. Initiate a sign-in from an unusual IP (VPN) using user-standard.
4. 4. Review Identity Protection > Risky sign-ins to confirm detection and enforcement.

Expected Result: Risk policies are enabled and enforce extra controls for risky events.

Evidence: Screenshots of policy settings and Risky sign-ins entry for user-standard.

## CA5 – Block legacy authentication for activated cloud users

Domain: Conditional Access

Portal/Tool: Entra (https://entra.microsoft.com)

Accounts: user-standard | Devices: Unmanaged laptop

Procedure:

1. 1. In Entra > Conditional Access > Policies, locate 'Block Legacy Authentication'.
2. 2. Verify Conditions include Client apps: 'Other clients' & 'Legacy authentication clients'; Grant = Block.
3. 3. Attempt IMAP/POP/Basic auth (e.g., legacy PowerShell) sign-in using user-standard (if feasible).
4. 4. Check Entra > Monitoring > Sign-in logs > Legacy auth tab for a blocked attempt.

Expected Result: Legacy protocols are blocked for scoped users.

Evidence: Policy screenshot; Sign-in log showing legacy auth blocked.

## CA6 – Restrict access by location to Zscaler IP (exception group for MSFT staff)

Domain: Conditional Access

Portal/Tool: Entra (https://entra.microsoft.com)

Accounts: user-standard | Devices: Unmanaged laptop vs Corporate (Zscaler)

Procedure:

1. 1. In Entra > Conditional Access > Named locations, confirm Zscaler/Mworks IP range exists.
2. 2. Open policy 'Location Restriction - Zscaler Only'. Verify Users = All users minus 'MSFT Staff' group (exclude), Conditions: Locations = Not in 'Zscaler', Grant = Block, State = On.
3. 3. Attempt sign-in from unmanaged device on non-Zscaler network as user-standard (should block).
4. 4. Attempt sign-in from corporate device egressing Zscaler (should succeed).

Expected Result: Non-Zscaler logins are blocked except members of the exception group.

Evidence: Policy screenshot; two sign-in log entries (blocked and successful).

## CA7 – Require App Protection Policy (MAM) on mobile devices

Domain: Conditional Access

Portal/Tool: Intune/Entra (https://entra.microsoft.com)

Accounts: user-standard | Devices: Managed mobile with Authenticator & Office

Procedure:

1. 1. In Intune (Entra Admin Center > Intune), navigate to Apps > App protection policies.
2. 2. Locate MAM policy targeting in-scope users/devices and confirm it is assigned and active.
3. 3. From the managed mobile, launch Outlook/Teams signed in as user-standard; confirm policy prompts/enforcement (PIN, data transfer restrictions).

Expected Result: MAM protections are enforced on mobile apps for in-scope users.

Evidence: Policy screenshot; mobile prompt/evidence capture (photo) where allowed.

## AC1 – Project users are cloud-only accounts

Domain: Identity/Accounts

Portal/Tool: M365 Admin (https://admin.microsoft.com)

Accounts: admin-global | Devices: Corporate laptop

Procedure:

1. 1. Open Microsoft 365 Admin Center > Users > Active users.
2. 2. Add 'Source' column to the view and verify project users show 'Azure AD' (not 'Synced from on-prem').
3. 3. Export CSV for evidence.

Expected Result: All project users are cloud-based (no hybrid sync).

Evidence: CSV export and screenshot of 'Source' column.

## AC2 – Guest access disabled (no guests or sharing)

Domain: Identity/Accounts

Portal/Tool: Entra/M365 (https://entra.microsoft.com)

Accounts: admin-identity, user-standard, guest-ext | Devices: Browser

Procedure:

1. 1. In Entra > External Identities > External collaboration settings, verify guest invitations are disabled as per policy.
2. 2. Attempt to add guest-ext to a Teams/SharePoint resource using user-standard (should fail).

Expected Result: Guest invites/sharing are blocked.

Evidence: Screenshot of settings and the failed guest add attempt.

## PW1 – Minimum password policy – complexity >= 12 characters

Domain: Password Policy

Portal/Tool: Entra (https://entra.microsoft.com)

Accounts: user-standard | Devices: Corporate laptop

Procedure:

1. 1. In Entra > Users > Password reset > Password protection (or Security > Authentication methods > Password protection), verify custom banned password and length policy is set to min 12 characters.
2. 2. Have user-standard attempt password change to <12 characters at https://mysignins.microsoft.com; confirm rejection.

Expected Result: Passwords <12 characters are rejected; policy reflects 12-char minimum.

Evidence: Screenshot of policy blade and rejection message.

## DV1 – Corporate devices provisioned with Mworks/Intune and compliant

Domain: Devices

Portal/Tool: Intune (https://entra.microsoft.com)

Accounts: admin-identity | Devices: Corporate laptop

Procedure:

1. 1. In Intune admin center, navigate to Devices > All devices.
2. 2. Verify corporate devices for project users show 'Compliant' and have required configuration profiles installed.
3. 3. Open one device record and capture compliance and configuration profile tabs.

Expected Result: Devices show 'Compliant' and are enrolled.

Evidence: Screenshots of device list and one device details.

## TL1 – Defender for Cloud Apps enabled (default state)

Domain: Tooling

Portal/Tool: Defender (https://security.microsoft.com)

Accounts: admin-security | Devices: Corporate laptop

Procedure:

1. 1. Open Microsoft Defender portal > Settings > Cloud Apps.
2. 2. Verify Microsoft Defender for Cloud Apps (MDCA) is enabled and connected to M365.
3. 3. Capture overview status.

Expected Result: MDCA enabled and connected.

Evidence: Screenshot of MDCA settings/overview.

## TL2 – Explore policy to block files (optional)

Domain: Tooling

Portal/Tool: Defender/Purview (https://security.microsoft.com)

Accounts: admin-security | Devices: Corporate laptop

Procedure:

1. 1. If applicable, in Defender or Purview create a test file-block rule (e.g., malware/EICAR).
2. 2. Validate detection/blocked result in message trace or activity explorer.

Expected Result: (If executed) file-block rule triggers as designed.

Evidence: Screenshots of policy and block event.

## TL3 – Safe Links and Safe Attachments for Teams/SPO/OneDrive

Domain: Tooling

Portal/Tool: Defender (https://security.microsoft.com)

Accounts: admin-security, user-standard | Devices: Corporate laptop

Procedure:

1. 1. In Defender > Policies & rules > Threat policies, verify Safe Links and Safe Attachments policies exist and target Teams, SharePoint, and OneDrive.
2. 2. Send a known test URL to user-standard in Teams; confirm URL rewrite and block page.
3. 3. Send EICAR file to user-standard via email/OneDrive; confirm attachment blocked/quarantined.

Expected Result: Unsafe links/attachments are blocked or detonated; logs present.

Evidence: Policy screenshots; message trace/quarantine screenshots.

## TL4 – Customer Key Management for M365 configured

Domain: Tooling

Portal/Tool: Admin/Security (https://admin.microsoft.com)

Accounts: admin-global | Devices: Corporate laptop

Procedure:

1. 1. In Microsoft 365 Admin Center > Settings > Org settings > Security & privacy (or Security portal > Information protection), verify Customer Key is configured and assigned to workloads per design.
2. 2. Capture key info (no secrets) and workload association.

Expected Result: Customer Key configured.

Evidence: Screenshot of Customer Key configuration pages.

## TL5 – M365 Unified Auditing is enabled

Domain: Tooling

Portal/Tool: Purview (https://compliance.microsoft.com)

Accounts: admin-security | Devices: Corporate laptop

Procedure:

1. 1. Open Purview > Audit.
2. 2. Run a search for recent sign-in or SharePoint events to confirm logs are present.

Expected Result: Unified Audit Log is enabled with events populated.

Evidence: Screenshot of audit results.

## IP1 – Publish labels: Highly Confidential, Confidential, Restricted, Public (org users)

Domain: Information Protection

Portal/Tool: Purview (https://compliance.microsoft.com)

Accounts: admin-security, user-standard | Devices: Corporate laptop

Procedure:

1. 1. In Purview > Information protection > Labels, verify labels exist with correct names and descriptions.
2. 2. In Label policies, verify a policy publishes these labels to org users.
3. 3. On user-standard Word desktop/web, check the Sensitivity menu to confirm labels appear.

Expected Result: All required labels published and visible to users.

Evidence: Screenshots of label list, policy, and Word sensitivity UI.

## IP2 – Default label 'Restricted' for org users

Domain: Information Protection

Portal/Tool: Purview (https://compliance.microsoft.com)

Accounts: admin-security, user-standard | Devices: Corporate laptop

Procedure:

1. 1. Open Purview > Information protection > Label policies.
2. 2. Open the org users policy and confirm 'Require users to apply a label' with default = 'Restricted'.
3. 3. Create a new Word document as user-standard and save to OneDrive; confirm default label applied.

Expected Result: 'Restricted' label applied by default for org users.

Evidence: Policy screenshot; document Info panel showing default label.

## IP3 – Microsoft users default label 'Confidential'

Domain: Information Protection

Portal/Tool: Purview (https://compliance.microsoft.com)

Accounts: admin-security | Devices: Corporate laptop

Procedure:

1. 1. In Purview > Label policies, locate the policy scoped to Microsoft users group.
2. 2. Verify default label is set to 'Confidential'.
3. 3. Capture policy settings including scope (MSFT users group).

Expected Result: 'Confidential' is default for Microsoft users per scope.

Evidence: Policy screenshot with scoped group + default label.

## IP4 – Labels allow project team members in Teams to consume documents

Domain: Information Protection

Portal/Tool: Purview/Teams (https://compliance.microsoft.com)

Accounts: user-standard | Devices: Corporate laptop

Procedure:

1. 1. Open label configuration for 'Restricted/Confidential' and review protection settings (permissions).
2. 2. Ensure the Teams project group is included as viewer/editor.
3. 3. Share a labeled file in the project Team; open as another member to confirm access.

Expected Result: Project team members can open labeled docs within Teams.

Evidence: Screenshots of label permissions & successful open.

## IP5 – No sensitivity reduction allowed

Domain: Information Protection

Portal/Tool: Purview/Word (https://compliance.microsoft.com)

Accounts: user-standard | Devices: Corporate laptop

Procedure:

1. 1. Create a document labeled 'Highly Confidential'.
2. 2. Attempt to downgrade the label to 'Confidential' or 'Public' in Word/Excel.
3. 3. Confirm action is blocked with justification not allowed (or requires admin).

Expected Result: Users cannot reduce sensitivity labels.

Evidence: Screenshot of blocked downgrade message.

## DLP1 – Block MY/SG IDs, passport, credit cards & encrypted attachments

Domain: DLP

Portal/Tool: Purview (https://compliance.microsoft.com)

Accounts: admin-security, user-standard | Devices: Corporate laptop

Procedure:

1. 1. In Purview > Data loss prevention > Policies, verify policy exists targeting Exchange, Teams, SharePoint, OneDrive.
2. 2. Confirm rules include detection for MY/SG national IDs, passport, credit card numbers, and encrypted attachment condition with Block/Quarantine action.
3. 3. Test by attempting to share sample data via email/Teams/SharePoint; confirm block or policy tip triggers.

Expected Result: Sensitive data sharing is blocked/quarantined across channels.

Evidence: Policy screenshots and incident/activity explorer.

## DLP2 – Block USB and Bluetooth for all users

Domain: DLP

Portal/Tool: Intune/Endpoint (https://entra.microsoft.com)

Accounts: admin-identity | Devices: Corporate laptop

Procedure:

1. 1. In Intune > Endpoint security > Attack surface reduction > Device control, verify policy that blocks removable storage and Bluetooth.
2. 2. On a corporate laptop, insert USB drive and attempt file copy; attempt Bluetooth transfer; confirm blocked.

Expected Result: USB/Bluetooth blocked on corporate devices.

Evidence: Intune policy screenshot; OS notification of block.

## DLM1 – Retention policy 15 years for EXO/SPO/Teams/M365 Groups/Copilot

Domain: Data Lifecycle

Portal/Tool: Purview (https://compliance.microsoft.com)

Accounts: admin-security | Devices: Corporate laptop

Procedure:

1. 1. In Purview > Data lifecycle management > Microsoft 365 > Retention policies, verify a policy named 'Baseline 15Y' applied to Exchange, SharePoint, OneDrive, Teams, M365 Groups, and Copilot data (if available).
2. 2. Open each workload scope to confirm inclusion and retention settings (15 years; retain & delete as designed).

Expected Result: Retention policies enforce 15-year retention across workloads.

Evidence: Screenshots of policy overview and included locations.

# 6. Role Validation Approach (Assignment Only)

## 6.1 Entra ID Built-in Roles

* Sign in to Entra Admin Center (https://entra.microsoft.com) with admin-identity.
* Navigate to Roles & administrators; open the target role.
* Review Assignments: users/groups, assignment type (eligible/active), and scope.
* Export assignments via portal or Microsoft Graph/PowerShell.
* Verify least privilege; flag or remove excessive assignments.
* Record findings in the Excel workbook (Entra Roles tab).

## 6.2 Azure RBAC Roles

* Sign in to Azure Portal (https://portal.azure.com) with admin-global.
* Subscriptions > select subscription > Access control (IAM) > Role assignments.
* Filter by role (Owner/Contributor/Reader/User Access Administrator/Key Vault roles). Export assignments.
* Repeat at Resource Group level for project RGs and at Key Vault resource level for RBAC.
* Confirm scopes are minimal and justified; no broad Owner at high scopes unless approved.
* Record findings in the Excel workbook (Azure RBAC tab).

# 7. Evidence Retention

Store screenshots (PNG), exports (CSV/JSON), and the signed Excel workbook in the project evidence repository under /Security/Baseline-Validation/<date>. Maintain per retention policy.

# 8. Conclusion & Next Steps

Execute the Excel workbook to complete testing. Remediate deviations, re-test, and present the summary to management.