Microsoft 365 & Azure Security Baseline Validation and Testing Approach

# 1. Purpose

This document provides the validation and testing strategy for security baseline controls across identity, access, information protection, and application layers. The objective is to confirm that configurations are correct, controls function as expected, misuse is prevented, and evidence is retained for compliance and audit needs.

# 2. Scope

This framework applies to the following domains:  
- Entra ID Standard Roles  
- Azure RBAC Standard Roles  
- Conditional Access  
- Information Protection (Document Labelling for Office, SharePoint, Exchange)  
- Azure Key Vault (AKV)  
- Break Glass Accounts  
- Application Protection Policies (Intune / MAM)

# 3. Validation Approach

Each domain is tested at four levels:  
1. Configuration Validation – Automated exports compared against baselines.  
2. Functional Testing – Simulation of expected user actions under assigned roles/policies.  
3. Security Testing – Controlled attempts to misuse or bypass the controls.  
4. Audit & Evidence – Collection of logs, screenshots, and SIEM alerts as proof of enforcement.

## 4.1 Entra ID Standard Roles

Objective: Ensure only approved accounts hold privileged roles, and each role functions with least privilege.

Testing:  
Automated daily export of role assignments; compare to approved matrix.  
Functional simulation: User Administrator resets a user password (allowed); attempt to assign Global Admin (denied).  
Misuse simulation: Privileged Role Administrator assigns Global Admin; should succeed but trigger alert.

Evidence:  
Role membership reports, screenshots, Entra audit logs.

## 4.2 Azure RBAC Standard Roles

Objective: Confirm access at subscription/resource group level is least privilege.

Testing:  
Automated export of role assignments; validate against baseline.  
Functional simulation: Reader attempts to delete VM (denied), Contributor attempts role assignment (denied).

Evidence:  
Exported assignment JSON, denied action logs, Azure Activity Logs.

## 4.3 Conditional Access

Objective: Validate authentication and device compliance enforcement.

Testing:  
Automated export of policies (MFA, device compliance, legacy auth).  
Manual test logins: unmanaged device (blocked), compliant device (allowed), external IP (MFA enforced).

Evidence:  
Sign-in log exports, blocked login screenshots.

## 4.4 Information Protection (Document Labelling)

Objective: Ensure sensitivity labels protect documents across Office, SharePoint, and Exchange.

Testing:  
Automated export of label/policy definitions.  
Functional simulation: Apply 'Confidential' to a Word document → attempt external email (blocked).  
Auto-labelling trigger: document containing financial data → label automatically applied.

Evidence:  
Label policy exports, blocked action screenshots, audit log entries.

## 4.5 Azure Key Vault (AKV)

Objective: Validate secure access to secrets and keys.

Testing:  
Automated export of RBAC and access policies.  
Functional simulation: Reader role attempts secret read (denied), Contributor role attempts secret read (allowed).

Evidence:  
Diagnostic logs, access denial screenshots.

## 4.6 Break Glass Accounts

Objective: Confirm emergency access accounts are operational and monitored.

Testing:  
Automated check of CA exclusions for break glass accounts.  
Manual login simulation during restricted access scenario; must succeed, and activity must be logged.

Evidence:  
Audit log entries of usage, screenshots of access results.

## 4.7 Application Protection Policies

Objective: Enforce mobile application data protection.

Testing:  
Automated export of Intune App Protection Policies.  
Functional simulation: Copy/paste from Outlook app → personal app (denied).  
Conditional launch tested: app requires PIN/biometric.

Evidence:  
Policy exports, blocked copy/paste screenshots.

# 5. Reporting

- Control Matrix: Each control tested with Pass/Fail/Observation.  
- Monthly Dashboard: Config drift alerts, compliance percentages per domain.  
- Quarterly Review: Summary of manual functional and misuse testing.

# 6. Continuous Monitoring

- Daily automated jobs for drift detection (roles, CA, labels, RBAC).  
- Alerts sent to SIEM for abnormal role changes or policy modifications.  
- Quarterly functional abuse simulations.  
- Annual full-scope validation including red-team style tests.