microsoft-cloud-security-checklist-2025

1. **Identity & Access Management (IAM)**

- [ ] Enforce **Multi-Factor Authentication (MFA)** for all accounts (especially admins).
- [ ] Disable **legacy authentication protocols** (POP3, IMAP, SMTP AUTH).
- [ ] Use **Conditional Access Policies** (require compliant device, restrict risky logins).
- [ ] Apply **least privilege** for Global Admins (minimize number of permanent global admins).
- [ ] Enable **Privileged Identity Management (PIM)** for just-in-time access.

2. **Endpoint & Device Security**

- [ ] Enforce **Intune device compliance policies** (patching, AV, disk encryption).
- [ ] Require **BitLocker** on Windows devices.
- [ ] Require **Defender for Endpoint** on all devices.
- [ ] Block **unmanaged devices** from accessing corporate resources.

3. **Data Protection**

- [ ] Enable **Microsoft Information Protection (MIP)** for classification & labeling.
- [ ] Apply **DLP (Data Loss Prevention)** policies for sensitive data (PII, PCI, HIPAA).
- [ ] Use **sensitivity labels** for Teams, SharePoint, OneDrive.
- [ ] Encrypt emails with **Microsoft Purview Message Encryption**.

4. **Threat Protection**

- [ ] Enable **Microsoft Defender for Office 365** (safe links, safe attachments).
- [ ] Configure **Defender for Cloud Apps (MCAS)** for shadow IT discovery.
- [ ] Enable **Microsoft Sentinel (SIEM)** or connect logs to an external SIEM.
- [ ] Turn on **audit logging** in Microsoft 365 Security & Compliance Center.

5. **Network & Cloud Security**

- [ ] Restrict **Azure Network Security Groups (NSGs)** to least privilege.
- [ ] Use **Azure Firewall or WAF** to protect applications.
- [ ] Enable **DDoS Protection Standard** for internet-facing resources.
- [ ] Apply **Just-In-Time VM Access** in Defender for Cloud.

6. **Backup & Recovery**

- [ ] Enable **Azure Backup** for critical VMs and SQL databases.
- [ ] Use **Microsoft 365 Backup** (new 2025 feature) for Exchange/SharePoint/OneDrive.
- [ ] Test **disaster recovery** with Azure Site Recovery.

7. **Monitoring & Governance**

- [ ] Enable **Microsoft Secure Score** and review regularly.
- [ ] Use **Azure Policy** for compliance enforcement.

- [ ] Enable **Activity Alerts** for high-risk actions (mailbox access, data exfiltration).
- [ ] Automate security posture reporting with **PowerShell** or **Graph API**.

PowerShell script that connects to Microsoft 365/Azure AD (Entra ID), pulls key security insights, and exports them for review.

⚠️ **Note**: To run this script, admins need:

- PowerShell 5.1 or 7+
- The following modules installed:
- Install-Module -Name Microsoft.Graph -Scope CurrentUser
- Install-Module -Name Microsoft.Graph.Identity.SignIns -Scope CurrentUser
- Install-Module -Name Microsoft.Graph.Security -Scope CurrentUser
- Install-Module -Name Microsoft.Graph.Authentication -Scope CurrentUser

```
<#

.SYNOPSIS

  Microsoft Cloud Security Audit Starter Script (2025)

.DESCRIPTION

  Checks MFA enforcement, Secure Score, risky users, and exports logs.

  Requires Microsoft Graph PowerShell SDK.

#>


Write-Host "=== Microsoft Cloud Security 2025 Audit ===" -ForegroundColor Cyan


# 1. Connect to Microsoft Graph

Write-Host "`n[+] Connecting to Microsoft Graph..." -ForegroundColor Yellow

Connect-MgGraph -Scopes
"SecurityEvents.Read.All","Reports.Read.All","AuditLog.Read.All","Directory.Read.All"


# Show signed-in user

$me = Get-MgUser -UserId (Get-MgContext).Account
```

```
Write-Host "Connected as: $($me.DisplayName) <$($me.UserPrincipalName)>"

# 2. Check MFA Status
Write-Host "`n[+] Checking MFA Enforcement..." -ForegroundColor Yellow
$mfaStatus = Get-MgUserAuthenticationMethod -UserId $me.Id
if ($mfaStatus) {
   Write-Host "MFA is enabled for this account."
} else {
   Write-Host "[!] MFA is NOT enabled for this account!" -ForegroundColor Red
}

# Organization-wide MFA check
$users = Get-MgUser -All -Property "userPrincipalName,strongAuthenticationMethods"
$mfaReport = foreach ($u in $users) {
   [PSCustomObject]@{
      UserPrincipalName = $u.UserPrincipalName
      MFAEnabled       = ($u.StrongAuthenticationMethods -ne $null)
   }
}
$mfaReport | Export-Csv -Path ".\MFA-Report.csv" -NoTypeInformation
Write-Host "MFA report saved to MFA-Report.csv"

# 3. Retrieve Secure Score
Write-Host "`n[+] Retrieving Microsoft Secure Score..." -ForegroundColor Yellow
$secureScore = Get-MgSecuritySecureScore -Top 1
if ($secureScore) {
```

```
    Write-Host "Current Secure Score: $($secureScore.CurrentScore) /
$($secureScore.MaxScore)"

    Write-Host "Weighted Score Percentage: $([math]::Round(($secureScore.CurrentScore /
$secureScore.MaxScore) * 100,2)) %"

} else {

    Write-Host "[!] Could not retrieve Secure Score. Ensure you have Security Reader role." -
ForegroundColor Red

}



# 4. Risky Users (Identity Protection)

Write-Host "`n[+] Checking for risky users..." -ForegroundColor Yellow

$riskyUsers = Get-MgRiskyUser -All

if ($riskyUsers) {

    Write-Host "[!] Risky users found:" -ForegroundColor Red

    $riskyUsers | Select-Object UserPrincipalName, RiskDetail, RiskState, RiskLevel | Format-
Table

    $riskyUsers | Export-Csv -Path ".\RiskyUsers.csv" -NoTypeInformation

    Write-Host "Risky users exported to RiskyUsers.csv"

} else {

    Write-Host "No risky users detected."

}



# 5. Export Audit Logs

Write-Host "`n[+] Exporting recent sign-in logs..." -ForegroundColor Yellow

$signIns = Get-MgAuditLogSignIn -Top 50

$signIns | Select-Object UserDisplayName, UserPrincipalName, AppDisplayName, IpAddress,
Status, CreatedDateTime |

    Export-Csv -Path ".\SignInLogs.csv" -NoTypeInformation
```

Write-Host "Latest sign-in logs saved to SignInLogs.csv"

Write-Host "`n=== Cloud Security Audit Completed ===" -ForegroundColor Cyan

What this script does

✔ Connects to Microsoft Graph with **Security + Audit scopes**
✔ Checks **MFA enforcement** (per-user & export)
✔ Pulls **Microsoft Secure Score**
✔ Lists and exports **risky users** (from Entra ID Identity Protection)
✔ Exports **latest sign-in logs** to CSV