



A FREE GUIDE FROM VERI-TECH, INC.

# The Engineer's *M365 Compliance* Cheat Sheet.

---

12 controls that move the needle, ordered by impact. Each one ships with a 60-second fix and a generated runbook.

Engineers shouldn't also be the audit team.

## Why this exists

---

Every Microsoft 365 tenant ships with the same defaults. Most of those defaults assume you've read 600 pages of admin documentation and made deliberate decisions about identity, sharing, and audit. You haven't. Nobody has.

This cheat sheet is the shortcut. Twelve controls, ranked by how much risk they take off the table per minute of effort. Every one of them maps to multiple compliance frameworks (CISA SCuBA, CIS, NIST 800-53, ISO 27001, HIPAA), so fixing them moves your audit posture across the board, not just one checkbox.

We built this from the same registry that powers Veri-Guard, our M365 compliance scanner. If you want the rest of the 548 controls automated against your tenant, see the back page.

---

## Why M365 is your highest-risk surface

---

If you run a Microsoft 365 tenant, you are running:

- **The world's most-targeted identity provider.** Entra ID is the front door for ~400 million enterprise users. If an attacker gets a session cookie, your VPN, your SaaS, and your code repos are all downstream.
- **The world's most-targeted email system.** 90%+ of breaches start with email. Exchange Online's defaults assume you'll layer on EOP presets. Most tenants never do.
- **A document-sharing platform with anonymous-link defaults.** SharePoint and OneDrive will, by default, let your users share files via "anyone with the link" URLs that bypass authentication entirely.
- **A meeting platform that lets dial-in attendees start meetings.** Teams' anonymous-meeting defaults exist because Microsoft's customers asked for them. They are not safe defaults.
- **A real-time chat federation system.** Teams will, by default, federate with every other M365 tenant on Earth. Your users can be social-engineered by an attacker who registered a tenant yesterday.

The good news: every one of these defaults is changeable in under 60 seconds, and the change is reversible. Below are the twelve we'd fix first.

---

## The 12 Controls

---

### 1. Require MFA for all users via Conditional Access

**What it does:** Enforces multi-factor authentication for every user sign-in, applied through a Conditional Access policy rather than per-user MFA legacy toggles.

**Why it matters:** This is the single highest-impact control in M365. 99% of identity-based attacks target accounts without MFA. Per-user MFA is deprecated; CA-based MFA is the only path that scales, audits, and integrates with risk-based signals.

**60-second fix:** Entra admin center → **Protection** → **Conditional Access** → **New policy**. Assignments: All users (exclude break-glass account). Cloud apps: All. Grant: Require MFA. Enable. *(For tenants without Entra ID P1, enable Security Defaults at Entra → Properties → Manage Security defaults: Enabled.)*

*Maps to: CISA-MS.AAD.3.2, CIS 1.1.1, NIST IA-2, ISO27001 A.5.16, HIPAA 164.312(d)*

---

## 2. Block legacy authentication for Exchange Online

**What it does:** Disables basic-auth protocols (IMAP, POP3, SMTP AUTH, ActiveSync legacy) and forces all Exchange Online clients to use Modern Authentication / OAuth 2.0.

**Why it matters:** Legacy auth bypasses MFA and Conditional Access entirely. An attacker with a valid password and no second factor can read mail through IMAP even if you've enforced MFA on web sign-in. This is how most "MFA-protected" tenants actually get compromised.

**60-second fix:** Exchange admin center → **Settings** → **Modern authentication** → confirm enabled. Then in Entra: Conditional Access → New policy → Conditions: Client apps → Legacy authentication clients → Grant: Block access.

*Maps to: CIS 6.1.1, CISA-MS.AAD.1.1, NIST IA-2(1), ISO27001 A.5.17*

---

## 3. Block legacy authentication for SharePoint and OneDrive

**What it does:** Prevents older Office clients (Office 2013 and earlier without patches) and third-party sync tools from authenticating to SharePoint and OneDrive without modern auth.

**Why it matters:** Same threat model as #2, different surface. Compromised credentials on a legacy SharePoint client can pull entire site libraries before any session-based control fires.

**60-second fix:** SharePoint admin center → **Policies** → **Access control** → **Apps that don't use modern authentication** → Block access.

*Maps to: CISA-MS.SHAREPOINT.1.2, CIS 7.2.1, NIST AC-17, ISO27001 A.8.5*

---

## 4. Enable the Unified Audit Log

**What it does:** Turns on tenant-wide audit logging across Exchange, SharePoint, Teams, and Entra ID, surfacing every administrative and user action through Microsoft Purview.

**Why it matters:** If you don't have audit logs, you cannot investigate an incident. You cannot answer auditor questions about who did what. You cannot prove compliance with retention requirements. Microsoft turns this on by default for new tenants since 2023, but older tenants and many sovereign clouds still ship with it disabled.

**60-second fix:** PowerShell:

```
Connect-ExchangeOnline  
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

*Maps to: CISA-MS.EXO.8.1, CIS 6.5.3, NIST AU-2, ISO27001 A.5.28, HIPAA 164.312(b)*

---

## 5. Privileged Identity Management (PIM) for Global Administrators

**What it does:** Removes standing Global Admin rights and replaces them with eligible-only assignments. Admins activate the role just-in-time, with approval and time-bound expiration.

**Why it matters:** Permanent Global Admin accounts are the highest-value target in any tenant. PIM cuts the attack window from "always" to "the 4 hours an admin needed it." Every privilege activation is logged, auditable, and revocable.

**60-second fix:** Entra → **Identity Governance** → **Privileged Identity Management** → **Microsoft Entra roles** → **Global Administrator** → for each member, change Assignment type from Active to Eligible. Configure activation settings: max 4 hours, require justification, require approval.

*Requires Entra ID P2. Maps to: CIS 1.1.5, NIST AC-2(7), ISO27001 A.5.18, HIPAA 164.308(a)(4)*

---

## 6. Enable Defender for Office 365 preset security policies

**What it does:** Activates Microsoft's Standard or Strict preset policy bundle for anti-phishing, anti-spam, anti-malware, Safe Links, and Safe Attachments.

**Why it matters:** Default Exchange Online Protection is intentionally permissive. Preset policies are Microsoft's curated, continuously-updated baseline. Turning them on is a one-click way to get protection that 90% of tenants are missing.

**60-second fix:** Microsoft Defender portal → **Email & collaboration** → **Policies & rules** → **Threat policies** → **Preset security policies** → Standard protection: Manage → Apply to all recipients → Enable.

*Maps to: CISA-MS.DEFENDER.1.1, CIS 2.1.4, NIST SI-3, ISO27001 A.8.7*

---

## 7. Block external auto-forwarding from Exchange Online

**What it does:** Stops users (and mail rules created by attackers in compromised mailboxes) from automatically forwarding email to external recipients.

**Why it matters:** This is the textbook business-email-compromise exfiltration pattern: attacker compromises a mailbox, sets a forwarding rule to a Gmail address, walks away with months of correspondence. Blocking outbound auto-forward at the tenant level closes this off whether or not the user knows their account is compromised.

**60-second fix:** Exchange admin center → **Mail flow** → **Remote domains** → **Default** → Automatic forwarding: Off. Or via PowerShell:

```
Set-RemoteDomain -Identity Default -AutoForwardEnabled $false
```

*Maps to: CISA-MS.EXO.1.1, CIS 6.2.1, NIST SC-7, HIPAA 164.312(e)*

---

## 8. Restrict SharePoint and OneDrive external sharing to authenticated guests

**What it does:** Prevents users from creating "Anyone with the link" anonymous URLs. External recipients must authenticate (as a guest, with Entra B2B) to access shared content.

**Why it matters:** Anonymous links leak. They get pasted into Slack, forwarded to personal email, indexed by leaky web crawlers. Authenticated guest access is logged, attributable, and revocable. Anonymous links are none of those.

**60-second fix:** SharePoint admin center → **Policies** → **Sharing** → External sharing slider: set to "New and existing guests" (or "Existing guests only" for stricter posture).

*Maps to: CISA-MS.SHAREPOINT.1.1, CIS 7.2.4, NIST AC-3, ISO27001 A.5.14*

---

## 9. Prevent anonymous Teams attendees from starting meetings

**What it does:** Blocks dial-in and anonymous external attendees from initiating a Teams meeting; an authenticated organizer must start it first.

**Why it matters:** A meeting that anonymous users can start is a meeting an attacker can join, record, and impersonate the organizer in. It's also how "ghost meeting" social engineering attacks work: attendees join a meeting that no organizer ever scheduled.

**60-second fix:**

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowAnonymousUsersToStartMeeting $false
```

*Maps to: CISA-MS.TEAMS.1.2, NIST AC-14*

---

## 10. Hold anonymous Teams attendees in the lobby

**What it does:** Anonymous and dial-in users land in the meeting lobby and must be admitted by an organizer; authenticated internal users auto-join.

**Why it matters:** Without a lobby, an anonymous attendee can join while sensitive material is on screen: pre-meeting prep, slides not yet shared, side conversations. The lobby gives the organizer a chance to verify identity before granting access.

**60-second fix:**

```
Set-CsTeamsMeetingPolicy -Identity Global -AutoAdmittedUsers EveryoneInCompanyExcludingGuests
```

*Maps to: CISA-MS.TEAMS.1.3, NIST AC-3*

---

## 11. Restrict Teams external federation

**What it does:** Replaces "federate with everyone" with either a deny-by-default model (no external federation) or an allowlist of approved partner domains.

**Why it matters:** Default Teams federation lets your users be messaged by anyone in any other M365 tenant on the planet. Attackers register tenants on free trial subscriptions and use them to social-engineer Teams users, bypassing email security entirely.

**60-second fix:** Teams admin center → **Users** → **External access** → set to "Block all external domains" (strictest) or configure an allow list of partner domains. PowerShell equivalent:

```
Set-CsTenantFederationConfiguration -AllowedDomainsAsAList $true
```

*Maps to: CISA-MS.TEAMS.2.1, NIST AC-4, ISO27001 A.5.14*

---

## 12. Block third-party Teams apps by default

**What it does:** Inverts the Teams app store from allow-by-default to block-by-default. Third-party and custom-built apps cannot be installed unless explicitly allowed by tenant admins.

**Why it matters:** Teams apps run with delegated user permissions. A malicious or compromised app can read chat history, exfiltrate files, and impersonate users. Most tenants have hundreds of apps available and zero governance over which ones get installed.

**60-second fix:** Teams admin center → **Teams apps** → **Manage apps** → Org-wide app settings → Third-party apps: Off. Then build an approved-app list incrementally.

*Maps to: CIS-M365.8.4.1, CISA-MS.TEAMS.4.1, NIST CM-7, ISO27001 A.8.19*

---

## The 60-second self-audit script

---

Paste this into PowerShell with the Exchange Online and Microsoft Graph modules installed. It checks the tenant-wide settings for the 12 controls above and prints a green/red report.

```

# Engineer's M365 Cheat Sheet: Self-Audit Script
# Requires: ExchangeOnlineManagement, Microsoft.Graph, MicrosoftTeams

Connect-ExchangeOnline -ShowBanner:$false
Connect-MgGraph -Scopes "Policy.Read.All","Directory.Read.All","RoleManagement.Read.Directory" -
Connect-MicrosoftTeams | Out-Null

$results = @()

# 1. CA policies requiring MFA for all users
$caPolicies = Get-MgIdentityConditionalAccessPolicy -All
$mfaForAll = $caPolicies | Where-Object {
    $_.State -eq 'enabled' -and
    $_.Conditions.Users.IncludeUsers -contains 'All' -and
    $_.GrantControls.BuiltInControls -contains 'mfa'
}
$results += [PSCustomObject]@{ Control = 'MFA for all users (CA)'; Pass = [bool]$mfaForAll }

# 2. Legacy auth blocked
$legacyBlock = $caPolicies | Where-Object {
    $_.State -eq 'enabled' -and
    $_.Conditions.ClientAppTypes -contains 'exchangeActiveSync' -and
    $_.GrantControls.BuiltInControls -contains 'block'
}
$results += [PSCustomObject]@{ Control = 'Legacy auth blocked'; Pass = [bool]$legacyBlock }

# 3. SharePoint legacy auth disabled
$spo = Get-SPOTenant -ErrorAction SilentlyContinue
$results += [PSCustomObject]@{ Control = 'SharePoint legacy auth blocked'; Pass = ($spo.LegacyAu

# 4. Unified audit log enabled
$audit = Get-AdminAuditLogConfig
$results += [PSCustomObject]@{ Control = 'Unified audit log enabled'; Pass = $audit.UnifiedAudit

# 5. PIM eligible-only Global Admins (any standing GA = fail)
$ga = Get-MgDirectoryRole -Filter "displayName eq 'Global Administrator'"
$gaMembers = if ($ga) { Get-MgDirectoryRoleMember -DirectoryRoleId $ga.Id -All } else { @() }
$results += [PSCustomObject]@{ Control = 'No standing Global Admins'; Pass = ($gaMembers.Count -

# 6. Defender preset policies enabled
$preset = Get-EOPProtectionPolicyRule -Identity 'Standard Preset Security Policy' -ErrorAction S
$results += [PSCustomObject]@{ Control = 'Defender Standard preset on'; Pass = ($preset.State -e

# 7. External auto-forward blocked
$remote = Get-RemoteDomain Default
$results += [PSCustomObject]@{ Control = 'External auto-forward blocked'; Pass = ($remote.AutoFo

# 8. SharePoint external sharing restricted
$results += [PSCustomObject]@{ Control = 'SharePoint sharing not Anyone'; Pass = ($spo.SharingCa

```

```
# 9 & 10. Teams meeting policies
$teamsPolicy = Get-CsTeamsMeetingPolicy -Identity Global
$results += [PSCustomObject]@{ Control = 'Anonymous cannot start meetings'; Pass = ($teamsPolicy
$results += [PSCustomObject]@{ Control = 'Anonymous wait in lobby'; Pass = ($teamsPolicy.AutoAdm

# 11. Teams federation restricted
$fed = Get-CsTenantFederationConfiguration
$results += [PSCustomObject]@{ Control = 'Teams federation restricted'; Pass = ($fed.AllowFedera

# 12. Teams third-party apps blocked
$teamsApp = Get-CsTeamsAppPermissionPolicy -Identity Global
$results += [PSCustomObject]@{ Control = 'Teams 3rd-party apps blocked'; Pass = ($teamsApp.Globa

$results | Format-Table -AutoSize
"`nPassed: $($results | Where-Object Pass).Count) / $($results.Count)"
```

---

## What to do next

You just read the 12 controls that move the needle. Here's the honest tradeoff with cheat sheets: they tell you what to fix once. They don't tell you when something drifts back, when a new control gets added to a framework, or when Microsoft changes a default underneath you.

That's the gap Veri-Tech closes.

**Veri-Guard** continuously scans your M365 tenant against 548 controls across 12 frameworks (CISA SCuBA, CIS Microsoft 365, NIST 800-53, NIST CSF 2.0, ISO 27001, HIPAA, HHS 405(d), GDPR, SOC 2, FFIEC, PCI DSS, MITRE ATT&CK). When something drifts, you find out the same day. When a control fails, you get a runbook or a one-click auto-remediation.

Three ways to take the next step:

- **Compare us against alternatives:** [veri-tech.net/compare](https://veri-tech.net/compare). See how Veri-Guard stacks up against the broader compliance-platform market.
- **Try the interactive demo:** [veri-tech.net/demo](https://veri-tech.net/demo). Walk through Veri-Guard, Veri-Tune, Veri-Vault, and Veri-Docs without giving us a credit card.
- **Talk to William directly:** [veri-tech.net/book](https://veri-tech.net/book). 30-minute intro call with the founder, no sales team in the loop.

---

*Engineers shouldn't also be the audit team.*

**Veri-Tech, Inc.** Veteran-owned. Indiana-based. Founded 2026. [veri-tech.net](https://veri-tech.net) · [security@veri-tech.net](mailto:security@veri-tech.net)

*Framework references are nominative. CIS Microsoft 365 Foundations Benchmarks are © Center for Internet Security, Inc. ISO/IEC 27001:2022 is © ISO. Veri-Tech is not affiliated with or endorsed by these organizations. See*



*publishers for authoritative control text.*