EntraGUARD
Client: Velzar

AUDITED TENANT

Production

SECURITY AUDIT REPORT

Microsoft 365 Security

Executive summary for management and CISO

REPORT DATE
09/12/2026

SCOPE
Entra ID, SharePoint, OneDrive, Teams, Defender, Exchange

APPLIED BASELINE
Baseline « CMMC 2.0 Level 1 (FAR 52.204-21) » — 159 controls run

WEIGHTED COMPLIANCE SCORE

61 %

- 72 compliant
- 37 warnings
- 41 non-compliant
- 9 not assessed

Executive summary

COMPLIANCE	COMPLIANT	WARNINGS	NON-COMP.	NOT ASSESSED	CONTROLS
61 %	72	37	41	9	159

Weighted score: foundational (L1) controls weigh 3× more than hardening (L2). A warning counts for half its points. Non-assessed controls (connector unavailable or unlicensed feature) are excluded from the score. Read-only audit.

Compliance by referential

Breakdown of compliant, warning and non-compliant controls

Entra 45%

— 33 compliant — 12 warnings — 28 non-compliant— 1 not assessed

SharePoint 0%

— 0 compliant — 3 warnings — 1 non-compliant

OneDrive 20%

— 1 compliant — 4 warnings — 0 non-compliant

Teams 69%

— 9 compliant — 4 warnings — 0 non-compliant

Defender 10%

— 1 compliant — 6 warnings — 3 non-compliant

Exchange 62%

— 28 compliant — 8 warnings — 9 non-compliant— 8 not assessed

Action priorities

The 8 most critical non-compliances to address first

1

Enable Microsoft Authenticator context protections

Entra · L1

In the Microsoft Authenticator configuration, enable application context and geographic location display for all users.

2

Block the device code flow

Entra · L1

Create a Conditional Access policy targeting the Device code authentication flow (Conditions > Authentication flows) with Block, excluding only legitimate scenarios.

3

Limit application credential lifetimes

Entra · L1

Reissue the affected credentials with a maximum validity of 12–24 months and enforce rotation with an app management policy.

4

Enable security defaults or equivalent Conditional Access policies

Entra · L1

Enable Security Defaults (Properties > Manage security defaults), or deploy Conditional Access policies covering MFA and blocking legacy authentication.

5

Require MFA for all administrator roles

Entra · L1

Conditional Access: create a policy targeting directory roles (Global Admin, etc.) with the "Require multi-factor authentication" grant.

6

Require MFA for all users

Entra · L1

Conditional Access: a policy targeting all users (with break-glass exclusions) requiring MFA, ideally via a phishing-resistant authentication strength.

7

Disable weak authentication methods

Entra · L1

Protection > Authentication methods: disable SMS and Voice call, and favor Microsoft Authenticator, FIDO2 and Windows Hello.

8

Configure Entra protection against weak passwords

Entra · L1

Protection > Authentication methods > Password protection: enable protection and a custom banned-password list.

Controls detail

REFERENTIAL	CONTROL	LVL	STATUS
Defender	DEF-015 **Enable user and domain impersonation protection** No active anti-phishing policy. › Defender portal > Policies > Anti-phishing: add the users and domains to protect. CIS Microsoft 365 2.1.7 · NIST SI-8 · CMMC SI.L1-3.14.2 · CSF DE.CM · FedRAMP Mod/High · CJIS 6.0 · Cyber Essentials: Malware protection · ITSG-33 SI-8 · ISO 27001 A.5.14 · CISA SCuBA MS.DEFENDER.2.1/MS.DEFENDER.2.2/MS.DEFENDER.2.3 · DORA Art. 10 · NIS2 21.2(b) · MCSB LT	L1	Non-compliant
Defender	DEF-017 **Quarantine spoof authentication failures** No active anti-phishing policy. › Defender portal > Policies > Anti-phishing: set the spoof action to Quarantine. CIS Microsoft 365 2.1.7 · NIST SI-8 · CMMC SI.L1-3.14.2 · CSF DE.CM · FedRAMP Mod/High · CJIS 6.0 · Cyber Essentials: Malware protection · ITSG-33 SI-8 · ISO 27001 A.5.14 · DORA Art. 10 · NIS2 21.2(b) · MCSB LT	L2	Non-compliant
Defender	DEF-016 **Enable mailbox intelligence** No active anti-phishing policy. › Defender portal > Policies > Anti-phishing: enable mailbox intelligence and its protection. CIS Microsoft 365 2.1.7 · NIST SI-8 · CMMC SI.L1-3.14.2 · CSF DE.CM · FedRAMP Mod/High · CJIS 6.0 · Cyber Essentials: Malware protection · ITSG-33 SI-8 · ISO 27001 A.5.14 · DORA Art. 10 · NIS2 21.2(b) · MCSB LT	L1	Non-compliant

Defender	DEF-002 **Strengthen Identity secure score controls** 7 Identity control(s) out of 13 at 0 points — improvement actions available. › Defender portal > Secure score > filter the Identity category: implement 0-point actions (MFA, roles, Conditional Access). Microsoft Secure Score · NIST IA-2 · CMMC IA.L1-3.5.1, IA.L1-3.5.2, IA.L2-3.5.3 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-6 · ITSG-33 IA-2 · UK GDPR Art.32 · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(i) · MCSB LT	L2	**Warning**
Defender	DEF-010 **Set the Safe Attachments action to Block** Get-SafeAttachmentPolicy not accessible. This protection is part of Microsoft Defender for Office 365: check the license (Plan 1/2) and permissions. EXO 403 on Get-SafeAttachmentPolicy: □ › Defender portal > Policies > Safe Attachments: set the action to Block. CIS Microsoft 365 2.1.4 · NIST SI-3 · CMMC SI.L1-3.14.2, SI.L1-3.14.4, SI.L1-3.14.5 · CSF DE.CM · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Malware protection · NCSC CAF B4 · ACSC E8-4 · ITSG-33 SI-3 · ISO 27001 A.8.7 · DORA Art. 10 · NIS2 21.2(b) · MCSB LT	L1	**Warning**
Defender	DEF-012 **Enable Safe Links for Office apps and Teams** Get-SafeLinksPolicy not accessible. This protection is part of Microsoft Defender for Office 365: check the license (Plan 1/2) and permissions. EXO 403 on Get-AtpPolicyForO365: □ › Defender portal > Policies > Safe Links: enable protection for Office apps and for Teams. CIS Microsoft 365 2.1.1 · NIST SI-3 · CMMC SI.L1-3.14.2, SI.L1-3.14.4, SI.L1-3.14.5 · CSF DE.CM · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Malware protection · NCSC CAF B4 · ACSC E8-4 · ITSG-33 SI-3 · ISO 27001 A.8.7 · DORA Art. 10 · NIS2 21.2(b) · MCSB LT	L1	**Warning**
Defender	DEF-011 **Enable Safe Attachments for SharePoint, OneDrive and Teams** Get-AtpPolicyForO365 not accessible. This protection is part of Microsoft Defender for Office 365: check the license (Plan 1/2) and permissions. EXO 403 on Get-AtpPolicyForO365: □ › Defender portal > Policies > Safe Attachments > Global settings: turn on protection for SharePoint, OneDrive and Teams. CIS Microsoft 365 2.1.5 · NIST SI-3 · CMMC SI.L1-3.14.2, SI.L1-3.14.4, SI.L1-3.14.5 · CSF DE.CM · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Malware protection · NCSC CAF B4 · ACSC E8-4 · ITSG-33 SI-3 · ISO 27001 A.8.7 · CISA SCuBA MS.DEFENDER.3.1 · DORA Art. 10 · NIS2 21.2(b) · MCSB LT	L1	**Warning**
Defender	DEF-019 **Lower the bulk mail threshold** Bulk mail threshold too permissive on: Default (BCL 7). A threshold of 6 is recommended. › Defender portal > Policies > Anti-spam: set the bulk mail threshold to 6 or lower. CIS Microsoft 365 2.1.6 · NIST SI-8 · CMMC SI.L1-3.14.2 · CSF DE.CM · FedRAMP Mod/High · CJIS 6.0 · Cyber Essentials: Malware protection · ITSG-33 SI-8 · ISO 27001 A.8.7 · DORA Art. 10 · NIS2 21.2(b) · MCSB LT	L2	**Warning**
Defender	DEF-013 **Block click-through on Safe Links warnings** Get-SafeLinksPolicy not accessible. This protection is part of Microsoft Defender for Office 365: check the license (Plan 1/2) and permissions. EXO 403 on Get-SafeLinksPolicy: □ › Defender portal > Policies > Safe Links: uncheck 'Let users click through to the original URL'. CIS Microsoft 365 2.1.1 · NIST SI-3 · CMMC SI.L1-3.14.2, SI.L1-3.14.4, SI.L1-3.14.5 · CSF DE.CM · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Malware protection · NCSC CAF B4 · ACSC E8-4 · ITSG-33 SI-3 · ISO 27001 A.8.7 · DORA Art. 10 · NIS2 21.2(b) · MCSB LT	L1	**Warning**
Defender	DEF-018 **Enable zero-hour auto purge (ZAP)** ZAP automatically removes malicious messages already delivered. CIS Microsoft 365 2.1.6 · NIST SI-3 · CMMC SI.L1-3.14.2, SI.L1-3.14.4, SI.L1-3.14.5 · CSF DE.CM · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Malware protection · NCSC CAF B4 · ACSC E8-4 · ITSG-33 SI-3 · ISO 27001 A.8.7 · DORA Art. 10 · NIS2 21.2(b) · MCSB IM	L1	**Compliant**
Entra	ENTRA-ADV-004 **Enable Microsoft Authenticator context protections** No Authenticator context protection enabled. › In the Microsoft Authenticator configuration, enable application context and geographic location display for all users. NIST IA-2 · CMMC IA.L1-3.5.1, IA.L1-3.5.2, IA.L2-3.5.3 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-6 · ITSG-33 IA-2 · UK GDPR Art.32 · ISO 27001 A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	**Non-compliant**
Entra	ENTRA-ADV-005 **Require authentication strengths in Conditional Access** No policy uses an authentication strength. › Replace 'require MFA' with an authentication strength (at minimum on administrator roles) in your Conditional Access policies. CIS Entra ID · NIST IA-2(1) · CMMC IA.L1-3.5.1, IA.L1-3.5.2, IA.L2-3.5.3 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-6 · ITSG-33 IA-2 · UK GDPR Art.32 · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L2	**Non-compliant**

Entra	ENTRA-ADV-010 **Block the device code flow** The device code flow is not blocked. › Create a Conditional Access policy targeting the Device code authentication flow (Conditions > Authentication flows) with Block, excluding only legitimate scenarios. CIS Entra ID · NIST AC-3 · CMMC AC.L1-3.1.1, AC.L1-3.1.2 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-5 · ITSG-33 AC-3 · UK GDPR Art.32 · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(j) · MCSB IM	L1	Non-compliant
Entra	ENTRA-WKL-002 **Limit application credential lifetimes** 20 application(s) carry credentials valid for more than two years. › Reissue the affected credentials with a maximum validity of 12–24 months and enforce rotation with an app management policy. CIS Entra ID · NIST IA-5 · CMMC IA.L1-3.5.2, IA.L2-3.5.7, IA.L2-3.5.10 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-6 · ITSG-33 IA-5 · UK GDPR Art.32 · ISO 27001 A.5.17 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM-3	L1	Non-compliant
Entra	ENTRA-WKL-004 **Identify ownerless applications** 20 ownerless application(s). › Assign at least one owner to every application, or delete orphaned applications that are no longer needed. NIST AC-2 · CMMC AC.L1-3.1.1, AC.L1-3.1.2 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-5 · ITSG-33 AC-2 · UK GDPR Art.32 · ISO 27001 A.5.16 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM-1	L2	Non-compliant
Entra	ENTRA-001 **Enable security defaults or equivalent Conditional Access policies** Neither Security Defaults nor an active Conditional Access policy. › Enable Security Defaults (Properties > Manage security defaults), or deploy Conditional Access policies covering MFA and blocking legacy authentication. CIS Entra ID · NIST IA-2 · CMMC IA.L1-3.5.1, IA.L1-3.5.2, IA.L2-3.5.3 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-6 · ITSG-33 IA-2 · UK GDPR Art.32 · ISO 27001 A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Non-compliant
Entra	ENTRA-002 **Require MFA for all administrator roles** No MFA policy targeting administrator roles. › Conditional Access: create a policy targeting directory roles (Global Admin, etc.) with the "Require multi-factor authentication" grant. CIS Entra ID · NIST IA-2 · CMMC IA.L1-3.5.1, IA.L1-3.5.2, IA.L2-3.5.3 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-6 · ITSG-33 IA-2 · UK GDPR Art.32 · ISO 27001 A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Non-compliant
Entra	ENTRA-003 **Require MFA for all users** No MFA policy targeting all users. › Conditional Access: a policy targeting all users (with break-glass exclusions) requiring MFA, ideally via a phishing-resistant authentication strength. CIS Entra ID · NIST IA-2 · CMMC IA.L1-3.5.1, IA.L1-3.5.2, IA.L2-3.5.3 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-6 · ITSG-33 IA-2 · UK GDPR Art.32 · ISO 27001 A.8.5 · CISA SCuBA MS.AAD.3.2 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Non-compliant
Entra	ENTRA-006 **Disable weak authentication methods** Weak methods enabled (SMS: enabled, Voice: disabled). › Protection > Authentication methods: disable SMS and Voice call, and favor Microsoft Authenticator, FIDO2 and Windows Hello. CIS Entra ID · NIST IA-5(1) · CMMC IA.L1-3.5.1, IA.L1-3.5.2, IA.L2-3.5.3 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-6 · ITSG-33 IA-5 · UK GDPR Art.32 · ISO 27001 A.8.5 · CISA SCuBA MS.AAD.3.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Non-compliant
Entra	ENTRA-008 **Use authentication strengths for sensitive access** No policy requires an authentication strength (e.g. phishing-resistant). › Conditional Access: apply an authentication strength (e.g. phishing-resistant) to administrators and critical applications. CIS Entra ID · NIST IA-5(1) · CMMC IA.L1-3.5.1, IA.L1-3.5.2, IA.L2-3.5.3 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-6 · ITSG-33 IA-5 · UK GDPR Art.32 · ISO 27001 A.8.5 · CISA SCuBA MS.AAD.3.6 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L2	Non-compliant
Entra	ENTRA-009 **Protect security method registration** No policy protects security information registration. › Conditional Access: a policy on the "Register security information" user action (trusted location, prior MFA or Identity Protection). CIS Entra ID · NIST IA-2 · CMMC IA.L1-3.5.1, IA.L1-3.5.2, IA.L2-3.5.3 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-6 · ITSG-33 IA-2 · UK GDPR Art.32 · ISO 27001 A.8.5 · CISA SCuBA MS.AAD.3.8 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Non-compliant
Entra	ENTRA-023 **Configure Entra protection against weak passwords** Protection against weak passwords disabled. › Protection > Authentication methods > Password protection: enable protection and a custom banned-password list. CIS Entra ID · NIST IA-5 · CMMC IA.L1-3.5.2, IA.L2-3.5.7, IA.L2-3.5.10 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-6 · ITSG-33 IA-5 · UK GDPR Art.32 · ISO 27001 A.5.17 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Non-compliant

Entra	ENTRA-024 **Extend password protection to on-premises AD** On-premises protection in Audit mode (recommended: Enforced). › Deploy the Entra password protection agents on the domain controllers and set the on-premises mode to "Enforced". CIS Entra ID · NIST IA-5 · CMMC IA.L1-3.5.2, IA.L2-3.5.7, IA.L2-3.5.10 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-6 · ITSG-33 IA-5 · UK GDPR Art.32 · ISO 27001 A.5.17 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Non-compliant
Entra	ENTRA-026 **Block legacy authentication** Legacy authentication is not blocked. › Conditional Access: create a policy targeting legacy authentication clients (Exchange ActiveSync and others) with the "Block" grant. CIS Entra ID · NIST IA-2(1) · CMMC AC.L1-3.1.1, AC.L1-3.1.2, AC.L2-3.1.11 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-6 · ITSG-33 IA-2 · UK GDPR Art.32 · ISO 27001 A.8.2, A.8.5 · CISA SCuBA MS.AAD.1.1 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Non-compliant
Entra	ENTRA-027 **Require MFA for access to Microsoft Azure Management** No MFA policy on Azure Management. › Conditional Access: a policy targeting the "Microsoft Azure Management" app requiring MFA. CIS Entra ID · NIST AC-2, AC-12 · CMMC AC.L1-3.1.1, AC.L1-3.1.2, AC.L2-3.1.11 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-5 · ITSG-33 AC-2 · UK GDPR Art.32 · ISO 27001 A.8.2, A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Non-compliant
Entra	ENTRA-028 **Configure sign-in frequency and non-persistent sessions for administrators** No session control configured. › Conditional Access: for administrator roles, enable the "Sign-in frequency" and "Persistent browser session = never" session controls. CIS Entra ID · NIST AC-12(1) · CMMC AC.L1-3.1.1, AC.L1-3.1.2, AC.L2-3.1.11 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-5 · ITSG-33 AC-12 · ISO 27001 A.8.2, A.8.5 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1	L2	Non-compliant
Entra	ENTRA-029 **Require compliant or hybrid-joined devices** No compliant device requirement. › Conditional Access: require the "Compliant device" or "Hybrid Entra joined" grant for access to sensitive resources. CIS Entra ID · NIST AC-19(5) · CMMC AC.L1-3.1.1, AC.L1-3.1.2, AC.L2-3.1.11 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · NCSC CAF B2 · ITSG-33 AC-19 · ISO 27001 A.8.2, A.8.5 · CISA SCuBA MS.AAD.3.7 · DORA Art. 9 · NIS2 21.2(h) · MCSB ES	L2	Non-compliant
Entra	ENTRA-037 **Require MFA for device join and registration** No MFA policy on device registration. › Conditional Access: create a policy on the "Register or join devices" user action requiring MFA. CIS Entra ID · NIST IA-2(1) · CMMC IA.L1-3.5.1, IA.L1-3.5.2, IA.L2-3.5.3 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-6 · ITSG-33 IA-2 · UK GDPR Art.32 · ISO 27001 A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Non-compliant
Entra	ENTRA-035 **Automate the identity lifecycle** No lifecycle workflow (joiner/mover/leaver). › Identity Governance > Lifecycle Workflows: create joiner / mover / leaver workflows to automate onboarding and offboarding. CIS Entra ID · NIST AC-2 · CMMC AC.L1-3.1.1, AC.L1-3.1.2 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-5 · ITSG-33 AC-2 · UK GDPR Art.32 · ISO 27001 A.5.16 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Non-compliant
Entra	ENTRA-040 **Restrict device platforms via Conditional Access** No device platform restriction. › Conditional Access: set the "Device platforms" condition to allow only supported platforms. CIS Entra ID · NIST AC-2, AC-12 · CMMC AC.L1-3.1.1, AC.L1-3.1.2, AC.L2-3.1.11 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-5 · ITSG-33 AC-2 · UK GDPR Art.32 · ISO 27001 A.8.2, A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L2	Non-compliant
Entra	ENTRA-036 **Package access via entitlement management** No access package defined. › Identity Governance > Entitlement management: create access packages (catalogs, approvals, expiration) for controlled access grants. CIS Entra ID · NIST AC-2 · CMMC AC.L1-3.1.1, AC.L1-3.1.2 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-5 · ITSG-33 AC-2 · UK GDPR Art.32 · ISO 27001 A.5.16 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Non-compliant
Entra	ENTRA-034 **Set up periodic access reviews** No access review defined. › Identity Governance > Access reviews: create recurring reviews on sensitive groups, roles and applications. CIS Entra ID · NIST AC-2 · CMMC AC.L1-3.1.1, AC.L1-3.1.2 · CSF PR.AA · FedRAMP Low/Mod/High · CJIS 6.0 · Cyber Essentials: Access control · NCSC CAF B2 · ACSC E8-5 · ITSG-33 AC-2 · UK GDPR Art.32 · ISO 27001 A.5.16 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Non-compliant