SAMPLE REPORT — tenant information blurred, real EntraGUARD output

EntraGUARD
entraguard.eu

AUDITED TENANT

[redacted]

[redacted]

SECURITY AUDIT REPORT

Microsoft 365 Security

Executive summary for management and CISO

REPORT DATE
27/07/2026

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

APPLIED BASELINE
Baseline “CIS — level 1” — 64 controls run

WEIGHTED COMPLIANCE SCORE

75%

- 45 compliant
- 7 warnings
- 10 non-compliant
- 2 not assessed

Report generated by EntraGUARD — entraguard.eu — read-only audit.

Executive summary

COMPLIANCE	COMPLIANT	WARNINGS	CONTROLS

75%	45	7	NON-COMP. 10	NOT ASSESSED 2	64

Methodology : weighted score by criticality — foundational (L1) controls weigh 3× more than hardening (L2). A warning counts for half its points. Read-only audit.

Compliance by referential

Breakdown of compliant, warning and non-compliant controls

Entra — 65%

17 compliant · 1 warnings · 6 non-compliant

Exchange — 60%

6 compliant · 3 warnings · 1 non-compliant

Teams — 67%

4 compliant · 2 warnings · 0 non-compliant

Defender — 80%

4 compliant · 1 warnings · 0 non-compliant

Intune — 60%

3 compliant · 0 warnings · 2 non-compliant

SharePoint — 80%

4 compliant · 0 warnings · 1 non-compliant

Purview — 100%

4 compliant · 0 warnings · 0 non-compliant

OneDrive — 100%

3 compliant | 0 warnings | 0 non-compliant

Action priorities

The 8 most critical non-compliances to address first

1 **Remove disabled accounts from privileged roles** ENTRA · L1

Remediation : Remove role assignments from disabled accounts.

2 **Require MFA for all users** ENTRA · L1

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

3 **Require MFA for device join and registration** ENTRA · L1

Remediation : Conditional Access: create a policy on the "Register or join devices" user action requiring MFA.

4 **Block the device code authentication flow** ENTRA · L1

Remediation : Entra portal > Conditional Access: create a policy targeting device code authentication flows with the Block grant.

5 **Control inbound and outbound mail connectors** EXCHANGE · L1

Remediation : Exchange admin center > Mail flow > Connectors: enforce TLS and restrict source domains or IP addresses.

6 **Enumerate non-compliant devices** INTUNE · L1

Remediation : Configure this in the Microsoft Intune admin center.

7 **Analyze configuration profile assignments** INTUNE · L2

Remediation : Configure this in the Microsoft Intune admin center.

8 **Control federation relationships and ADFS configuration** ENTRA · L2

> Remediation : Audit federated domains (authenticationType) and migrate to cloud authentication (PHS/PTA + seamless SSO) where possible.

Controls detail

REFERENTIAL	CONTROL	LVL	STATUS
Defender	**Enable Safe Links for Office apps and Teams** CIS Microsoft 365 2.1.1 · NIST SI-3 · ISO 27001 A.8.7 · DORA Art. 10 · NIS2 21.2(b)	L1	Compliant
Defender	**Block accounts exceeding outbound sending limits** CIS Microsoft 365 2.1.3 · NIST SI-4 · ISO 27001 A.8.16 · DORA Art. 10 · NIS2 21.2(b)	L1	Compliant
Defender	**Tolerate no active high-severity incident** → Defender portal > Incidents: mobilize response on any high-severity incident (containment, eradication, post-mortem). NIST IR-4 · ISO 27001 A.5.26 · DORA Art. 10 · NIS2 21.2(b)	L1	Warning
Defender	**Work down stale active incidents** NIST IR-4 · ISO 27001 A.5.26 · DORA Art. 10 · NIS2 21.2(b)	L2	Compliant
Defender	**Strengthen Apps secure-score controls** Microsoft Secure Score · NIST · ISO 27001 A.8.9 · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
Entra	**Remove disabled accounts from privileged roles** → Remove role assignments from disabled accounts. NIST AC-2 · ISO 27001 A.5.18 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L1	Non-compliant
Entra	**Require MFA for 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 · ISO 27001 A.8.5 · CISA SCuBA MS.AAD.3.2 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j)	L1	Non-compliant
Entra	**Require MFA for device join and registration** → Conditional Access: create a policy on the "Register or join devices" user action requiring MFA. CIS Entra ID · NIST IA-2 · ISO 27001 A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j)	L1	Non-compliant
Entra	**Block the device code authentication flow** → Entra portal > Conditional Access: create a policy targeting device code authentication flows with the Block grant.	L1	Non-compliant

REFERENTIAL	CONTROL	LVL	STATUS
	NIST AC-3 · ISO 27001 A.5.15 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j)		
Entra	**Control federation relationships and ADFS configuration** → Audit federated domains (authenticationType) and migrate to cloud authentication (PHS/PTA + seamless SSO) where possible. CIS Entra ID · NIST CM-6 · ISO 27001 A.8.9 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L2	Non-compliant
Entra	**Limit the maximum PIM role activation duration** → Entra > PIM > Role settings > Activation: lower 'Activation maximum duration' to 8 hours or less. CIS Entra ID · NIST AC-6 · ISO 27001 A.5.15 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L2	Non-compliant
Entra	**Require compliant or hybrid-joined devices** CIS Entra ID · NIST AC-2, AC-12 · ISO 27001 A.8.2, A.8.5 · CISA SCuBA MS.AAD.3.7 · DORA Art. 9 · NIS2 21.2(h)	L2	Compliant
Entra	**Require an approved app or an app protection policy** CIS Entra ID · NIST AC-2, AC-12 · ISO 27001 A.8.2, A.8.5 · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
Entra	**Block legacy authentication** → Conditional Access: create a policy targeting legacy authentication clients (Exchange ActiveSync and others) with the "Block" grant. CIS Entra ID · NIST AC-2, AC-12 · ISO 27001 A.8.2, A.8.5 · CISA SCuBA MS.AAD.1.1 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j)	L1	Not assessed
Entra	**Enable number matching in Microsoft Authenticator** CIS Entra ID · NIST IA-2 · ISO 27001 A.8.5 · CISA SCuBA MS.AAD.3.3 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j)	L1	Compliant
Entra	**Provide break-glass emergency access accounts** CIS Entra ID · NIST AC-6 · ISO 27001 A.8.2 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L1	Compliant
Entra	**Eliminate permanent privileged assignments** CIS Entra ID 1.1.4 · NIST AC-6(1) · ISO 27001 A.8.2 · CISA SCuBA MS.AAD.7.4 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
Entra	**Prohibit insecure redirect URIs (HTTP)** CIS Entra ID · NIST CM-7, AC-6 · ISO 27001 A.8.19 · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
Entra	**Alert on Conditional Access policy changes** CIS Entra ID · NIST AU-6 · ISO 27001 A.8.15 · ANSSI MFA · DORA Art. 10 · NIS2 21.2(b)	L2	Compliant

REFERENTIAL	CONTROL	LVL	STATUS
Entra	**Prohibit guests in privileged roles** → Remove guest accounts from privileged roles and create dedicated internal accounts. CIS Entra ID 1.1.3 · NIST AC-6 · ISO 27001 A.5.15 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L1	Warning
Entra	**Enable report suspicious activity** CIS Entra · NIST IR-6 · ISO 27001 A.6.8 · DORA Art. 10 · NIS2 21.2(b)	L1	Compliant
Entra	**Restrict Microsoft 365 group creation** CIS Entra ID · NIST CM-6 · ISO 27001 A.8.9 · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
Entra	**Configure Entra diagnostic settings to Azure Monitor** CIS Entra ID · NIST AU-2 · ISO 27001 A.8.15 · CISA SCuBA MS.AAD.4.1 · ANSSI Journalisation · DORA Art. 10 · NIS2 21.2(b)	L1	Compliant
Entra	**Use restricted management administrative units** NIST AC-6 · ISO 27001 A.8.2 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
Entra	**Eliminate weak auth methods on privileged accounts** CIS Entra ID 1.1.6 · NIST IA-2(8) · ISO 27001 A.8.5 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(j)	L2	Compliant
Entra	**Limit the number of global administrators to between two and four** → Entra portal > Roles and administrators > Global Administrator: remove superfluous accounts to keep only 2 to 4 holders, and replace permanent assignments with PIM eligibility. CIS Entra ID · NIST AC-6 · ISO 27001 A.8.2 · CISA SCuBA MS.AAD.7.1 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L1	Not assessed
Entra	**Audit high-permission service principals with active credentials** CIS Entra · NIST IA-5 · ISO 27001 A.8.2 · ANSSI Journalisation · DORA Art. 10 · NIS2 21.2(b)	L2	Compliant
Entra	**Use dedicated, cloud-only administrator accounts** CIS Entra ID · NIST AC-6 · ISO 27001 A.8.2 · CISA SCuBA MS.AAD.7.3 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L1	Compliant
Entra	**Prevent non-administrator users from creating tenants** CIS Entra ID · NIST AC-6 · ISO 27001 A.8.2 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i)	L1	Compliant
Entra	**Require MFA for external and guest users** CIS Entra ID · NIST AC-2, AC-12 · ISO 27001 A.8.2, A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j)	L1	Compliant

REFERENTIAL	CONTROL	LVL	STATUS
Entra	**Prevent users from recovering BitLocker keys** CIS Entra · NIST AC-6 · ISO 27001 A.8.2 · DORA Art. 9 · NIS2 21.2(h)	L2	Compliant
Exchange	**Control inbound and outbound mail connectors** → Exchange admin center > Mail flow > Connectors: enforce TLS and restrict source domains or IP addresses. CIS Microsoft 365 6.x · NIST SC-8 · ISO 27001 A.8.20 · DORA Art. 9 · NIS2 21.2(i)	L1	Non-compliant
Exchange	**Enable Safe Attachments** CIS Microsoft 365 · NIST SI-3 · ISO 27001 A.8.7 · DORA Art. 10 · NIS2 21.2(b)	L1	Compliant
Exchange	**Disallow mail flow rules that allowlist domains or IPs** CIS Microsoft 365 · NIST SI-8 · ISO 27001 A.8.12 · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
Exchange	**Disable auto-forwarding via remote domains** CIS Microsoft 365 · NIST AC-4 · ISO 27001 A.8.12 · DORA Art. 9 · NIS2 21.2(i)	L1	Compliant
Exchange	**Inventory mailboxes with forwarding configured** CIS Microsoft 365 · NIST AC-4 · ISO 27001 A.8.12 · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
Exchange	**Enable MailTips for users** → Set-OrganizationConfig -MailTipsAllTipsEnabled $true -MailTipsExternalRecipientsTipsEnabled $true. CIS Microsoft 365 · NIST AT-2 · ISO 27001 A.6.3 · DORA Art. 9 · NIS2 21.2(i)	L2	Warning
Exchange	**Deploy an authentication policy blocking legacy authentication** CIS Microsoft 365 · NIST IA-2 · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(j)	L1	Compliant
Exchange	**Disable legacy protocols per mailbox** CIS Microsoft 365 6.5.x · NIST IA-2 · ISO 27001 A.5.17 · DORA Art. 9 · NIS2 21.2(i)	L1	Compliant
Exchange	**Tag messages coming from outside** → Exchange Online PowerShell: Set-ExternalInOutlook -Enabled $true. CIS Microsoft 365 6.2.3 · NIST SI-8 · ISO 27001 A.5.14 · DORA Art. 9 · NIS2 21.2(i)	L1	Warning

REFERENTIAL	CONTROL	LVL	STATUS
Exchange	**Enable litigation hold on sensitive mailboxes** → Exchange admin center > Mailboxes > Features: enable litigation hold on sensitive accounts. NIST SI-12 · ISO 27001 A.5.33 · DORA Art. 9 · NIS2 21.2(i)	L2	Warning
Intune	**Analyze configuration profile assignments** → Configure this in the Microsoft Intune admin center. CIS Intune · NIST CM-6 · ISO 27001 A.8.9 · DORA Art. 9 · NIS2 21.2(i)	L2	Non-compliant
Intune	**Enumerate non-compliant devices** → Configure this in the Microsoft Intune admin center. CIS Intune · NIST CM-6 · ISO 27001 A.8.9 · DORA Art. 9 · NIS2 21.2(h)	L1	Non-compliant
Intune	**Require multi-admin approval for destructive actions** CIS Intune · NIST AC-6 · ISO 27001 A.8.2 · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
Intune	**Deploy app protection policies** CIS Intune · NIST AC-19 · ISO 27001 A.8.1 · DORA Art. 9 · NIS2 21.2(i)	L1	Compliant
Intune	**Review deployed PowerShell scripts** CIS Intune · NIST CM-7 · ISO 27001 A.8.19 · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
OneDrive	**Enforce app-enforced restrictions on unmanaged devices** CIS Microsoft 365 · CISA SCuBA · NIST AC-3 · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(h)	L2	Compliant
OneDrive	**Notify OneDrive owners of external shares** CIS Microsoft 365 · NIST AC-21 · ISO 27001 A.5.14 · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
OneDrive	**Set a default OneDrive storage limit** CIS Microsoft 365 · NIST PM-1 · ISO 27001 A.5.1 · DORA Art. 10 · NIS2 21.2(b)	L2	Compliant
Purview	**Enable the unified audit log** CIS Microsoft 365 · NIST AU-2 · ISO 27001 A.8.15 · CISA SCuBA MS.DEFENDER.6.1 · ANSSI Journalisation · DORA Art. 10 · NIS2 21.2(b)	L1	Compliant
Purview	**Enable auto-labelling of sensitive documents** CIS Microsoft 365 3.5 · NIST MP-3 · ISO 27001 A.5.12 · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
Purview	**Publish retention labels** CIS Microsoft 365 · NIST SI-12 · ISO 27001 A.5.33 · DORA Art. 9 · NIS2 21.2(h)	L2	Compliant

REFERENTIAL	CONTROL	LVL	STATUS
Purview	**Set a blocking action on DLP rules** CIS Microsoft 365 3.2 · NIST AC-4 · ISO 27001 A.8.12 · CISA SCuBA MS.DEFENDER.4.2 · DORA Art. 9 · NIS2 21.2(h)	L1	Compliant
SharePoint	**Hide the site creation UI** → SharePoint admin center > Settings > Site creation: hide the 'Create site' command from users. Microsoft Secure Score · NIST PM-1 · ISO 27001 A.5.1 · DORA Art. 9 · NIS2 21.2(i)	L2	Non-compliant
SharePoint	**Limit SharePoint access from unmanaged devices** CIS Microsoft 365 · NIST AC-3 · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(h)	L2	Compliant
SharePoint	**Set a default storage limit for new sites** Microsoft Secure Score · NIST PM-1 · ISO 27001 A.5.1 · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
SharePoint	**Sign out idle sessions** CIS Microsoft 365 · NIST AC-12 · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(i)	L1	Compliant
SharePoint	**Restrict external sharing domains** CIS Microsoft 365 · NIST AC-21 · ISO 27001 A.5.14 · CISA SCuBA MS.SHAREPOINT.1.3 · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
Teams	**Limit public teams** → Review public teams and switch non-legitimate ones to 'Private' (team settings or Set-Team - Visibility Private). CIS Microsoft 365 · NIST AC-3 · ISO 27001 A.5.15 · DORA Art. 9 · NIS2 21.2(i)	L2	Warning
Teams	**Control channel sharing with external users** CIS Microsoft 365 · NIST AC-3 · ISO 27001 A.5.14 · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
Teams	**Block personal-scope RSC consent for Teams apps** CIS Microsoft 365 · NIST AC-6 · ISO 27001 A.8.2 · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
Teams	**Block guest access to group content** CIS Microsoft 365 · NIST AC-21 · ISO 27001 A.5.14 · DORA Art. 9 · NIS2 21.2(i)	L2	Compliant
Teams	**Define guest usage guidelines** → Group.Unified directory setting: set GuestUsageGuidelinesUrl to your guest usage guidelines page. CIS Microsoft 365 · NIST AC-21 · ISO 27001 A.5.14 · DORA Art. 9 · NIS2 21.2(i)	L2	Warning
Teams	**Control anonymous user access to meetings**	L2	Compliant

REFERENTIAL	CONTROL	LVL	STATUS
	CIS Microsoft 365 · NIST AC-14 · ISO 27001 A.8.3 · DORA Art. 9 · NIS2 21.2(i)		