SAS PEREZ

AUDITED COMPANY

test

Test Tenant 1

m365expertise.com

SECURITY AUDIT REPORT

Microsoft 365 Security

Executive summary for management and CISO

REPORT DATE

13/08/2026

SCOPE

Entra ID

APPLIED BASELINE

Standard — 136 controls run

WEIGHTED COMPLIANCE SCORE

53 %

- 50 compliant
- 20 warnings
- 43 non-compliant
- 23 not assessed

Executive summary

COMPLIANCE	COMPLIANT	WARNINGS	NON-COMP.	NOT ASSESSED	CONTROLS
53 %	50	20	43	23	136

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

Compliance by referential

Breakdown of compliant, warning and non-compliant controls

Entra 44%

50 compliant · 20 warnings · 43 non-compliant · 23 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. **Protect Microsoft admin portals with Conditional Access**
   Entra · L1
   Create a Conditional Access policy on the Microsoft Admin Portals application requiring at least strong MFA, ideally a compliant device.
4. **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.
5. **Prohibit the OAuth implicit flow on applications**
   Entra · L1
   Disable implicit access-token issuance on each application (manifest: web.implicitGrantSettings) and migrate clients to the code flow with PKCE.
6. **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.
7. **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.
8. **Disable weak authentication methods**
   Entra · L1
   Protection > Authentication methods: disable SMS and Voice call, and favor Microsoft Authenticator, FIDO2 and Windows

Hello.

Controls detail

REFERENTIAL	CONTROL	LVL	STATUS
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 · ISO 27001 A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	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 · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(j) · MCSB IM	L1	Non-compliant
Entra	ENTRA-ADV-014 **Protect Microsoft admin portals with Conditional Access** No policy targets the Microsoft Admin Portals application. → Create a Conditional Access policy on the Microsoft Admin Portals application requiring at least strong MFA, ideally a compliant device. CIS Entra ID · NIST AC-6 · ISO 27001 A.8.2 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-2	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) · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L2	Non-compliant
Entra	ENTRA-ADV-013 **Cover all users with risk-based policies** No risk-based Conditional Access policy. → Extend risk-based Conditional Access policies (sign-in and user risk) to all users, with break-glass exclusions only. NIST SI-4 · ISO 27001 A.8.16 · DORA Art. 10 · NIS2 21.2(b) · MCSB LT	L2	Non-compliant
Entra	ENTRA-WKL-002 **Limit application credential lifetimes** 7 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 · 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** 6 ownerless application(s). → Assign at least one owner to every application, or delete orphaned applications that are no longer needed. NIST AC-2 · ISO 27001 A.5.16 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM-1	L2	Non-compliant
Entra	ENTRA-WKL-008 **Prohibit the OAuth implicit flow on applications** 2 application(s) with the implicit flow enabled. → Disable implicit access-token issuance on each application (manifest: web.implicitGrantSettings) and migrate clients to the code flow with PKCE. NIST SC-8 · ISO 27001 A.8.26 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	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 · 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 · ISO 27001 A.8.5 · CISA SCuBA MS.AAD.3.2 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) ·	L1	Non-compliant

REFERENTIAL	CONTROL	LVL	STATUS
	MCSB IM-6		
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-2 · 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-2 · 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 · 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-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 · ISO 27001 A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Non-compliant
Entra	ENTRA-012 **Provide break-glass emergency access accounts** No account excluded from policies — provide emergency access accounts. → Create two cloud-only emergency accounts excluded from Conditional Access policies, with dedicated monitoring and alerts. CIS Entra ID · NIST AC-6 · ISO 27001 A.8.2 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1	L1	Non-compliant
Entra	ENTRA-014 **Prevent non-administrator users from creating tenants** Users can create tenants. → Entra portal > Users > User settings > Tenant settings: set "Users can create tenants" to No. CIS Entra ID · NIST AC-6 · ISO 27001 A.8.2 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1	L1	Non-compliant
Entra	ENTRA-015 **Restrict user consent to applications** Users can consent to applications. → Enterprise applications > Consent and permissions: set user consent to "Do not allow" or limit it to verified publishers and low-impact permissions. CIS Entra ID · NIST CM-7, AC-6 · ISO 27001 A.8.19 · CISA SCuBA MS.AAD.5.2 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L1	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 · 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 · 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 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) · MCSB IM-6	L1	Non-compliant
Entra	ENTRA-027 **Require MFA for access to Microsoft Azure Management**	L1	Non-compliant

REFERENTIAL	CONTROL	LVL	STATUS
	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 · ISO 27001 A.8.2, A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6		
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-2, 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-2, AC-12 · 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-031 **Require MFA for risky sign-ins** No sign-in-risk-based policy. → Conditional Access + Identity Protection: a sign-in-risk-based policy requiring MFA when risk is medium or high. CIS Entra ID · NIST SI-4 · ISO 27001 A.8.16 · CISA SCuBA MS.AAD.2.3 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB LT	L2	Non-compliant
Entra	ENTRA-032 **Require remediation for high-risk users** No user-risk-based policy. → Conditional Access + Identity Protection: a user-risk-based policy requiring MFA and password change. CIS Entra ID · NIST SI-4 · ISO 27001 A.8.16 · CISA SCuBA MS.AAD.2.1 · DORA Art. 10 · NIS2 21.2(b) · MCSB LT	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 · ISO 27001 A.5.16 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	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 · ISO 27001 A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Non-compliant
Entra	ENTRA-039 **Prefer certificates over secrets for applications and service principals** 7 application(s) use a client secret (prefer certificates). → Inventory app registrations using a client secret and migrate them to certificate authentication; then remove the secrets. CIS Entra ID · NIST CM-7, AC-6 · ISO 27001 A.8.19 · 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 · 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 · ISO 27001 A.5.16 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Non-compliant
Entra	ENTRA-042 **Restrict default user permissions** Permissive default permissions (apps: False, groups: False, tenants: True). → Users > User settings: harden the default user role (creating apps, groups, tenants, reading other users). CIS Entra ID · NIST CM-6 · ISO 27001 A.8.9 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L1	Non-compliant
Entra	ENTRA-045 **Restrict Microsoft 365 group creation**	L2	Non-compliant

REFERENTIAL	CONTROL	LVL	STATUS
	All users can create Microsoft 365 groups. → Groups > General: restrict Microsoft 365 group creation to an authorized security group (EnableGroupCreation setting). CIS Entra ID · NIST CM-6 · ISO 27001 A.8.9 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM		
Entra	ENTRA-046 **Block directory access via MSOnline PowerShell** Directory access via MSOnline PowerShell is not blocked. → Via Graph (authorizationPolicy): set blockMsolPowerShell to true to prohibit the legacy MSOnline module. CIS Entra ID · NIST CM-6 · ISO 27001 A.8.9 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Non-compliant
Entra	ENTRA-047 **Disable email-based self-service subscriptions** Email-based self-service subscriptions are allowed. → Disable self-service subscriptions (Set-MsolCompanySettings -AllowAdHocSubscriptions $false). CIS Entra ID · NIST CM-6 · ISO 27001 A.8.9 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Non-compliant
Entra	ENTRA-051 **Require MFA for external and guest users** No MFA policy targeting guests/externals. → Conditional Access: create a policy targeting guest/external users with the "Require MFA" grant. 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) · MCSB IM-6	L1	Non-compliant
Entra	ENTRA-052 **Cover all cloud applications with Conditional Access** No policy targets all cloud applications. → Conditional Access: have at least one baseline policy targeting "All cloud apps" (with controlled exclusions). 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) · MCSB IM-6	L1	Non-compliant
Entra	ENTRA-053 **Restrict access by location via Conditional Access** No location-based policy. → Define named locations (Protection > Named locations) then a location-based Conditional Access policy. 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) · MCSB IM-6	L2	Non-compliant
Entra	ENTRA-054 **Require an approved app or an app protection policy** No approved app / app protection requirement. → Conditional Access: add the "Require approved client app" or "Require app protection policy" grant for mobile access. CIS Entra ID · NIST AC-2, AC-12 · ISO 27001 A.8.2, A.8.5 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Non-compliant
Entra	ENTRA-055 **Enable app-enforced session restrictions** No app-enforced session restriction. → Conditional Access: enable "App enforced restrictions" or the Defender for Cloud Apps integration in session controls. CIS Entra ID · NIST AC-2, AC-12 · ISO 27001 A.8.2, A.8.5 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Non-compliant
Entra	ENTRA-056 **Ensure applications have an owner** 6 application(s) without an owner (sample). → App registrations > (application) > Owners: assign at least one owner to orphaned applications. CIS Entra ID · NIST CM-7, AC-6 · ISO 27001 A.8.19 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Non-compliant
Entra	ENTRA-079 **Remove disabled conditional access policies** No Conditional Access policy defined. → Entra portal > Protection > Conditional Access: delete disabled policies or document them explicitly. NIST CM-6 · ISO 27001 A.8.9 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L2	Non-compliant
Entra	ENTRA-080 **Move conditional access policies out of report-only mode** No Conditional Access policy defined. → Entra portal > Protection > Conditional Access: switch validated policies from Report-only to On. NIST CM-6 · ISO 27001 A.8.9 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Non-compliant
Entra	ENTRA-082 **Block the device code authentication flow** The device code flow is not blocked: it lets an attacker have a token approved by a legitimate user. → 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) · MCSB IM-6		
Entra	ENTRA-ADV-008 **Do not trust external tenants' MFA and devices by default** No external claim trusted by default. NIST IA-2 · ISO 27001 A.5.15 · DORA Art. 9 · NIS2 21.2(j) · MCSB IM	L2	Compliant
Entra	ENTRA-ADV-007 **Constrain B2B Direct Connect** B2B Direct Connect blocked by default, inbound and outbound. NIST AC-3 · ISO 27001 A.5.15 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L1	Compliant
Entra	ENTRA-ADV-006 **Harden the default cross-tenant access policy** Inbound B2B collaboration open by default to every tenant. → In External Identities > Cross-tenant access settings, restrict the defaults and create explicit partner configurations. NIST AC-3 · ISO 27001 A.5.15 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Warning
Entra	ENTRA-ADV-001 **Complete the migration to the authentication methods policy** Migration complete: the unified policy is authoritative. CIS Entra ID · NIST IA-2 · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Compliant
Entra	ENTRA-ADV-002 **Enable FIDO2 passkeys** FIDO2 passkeys are enabled. CIS Entra ID · NIST IA-2(1) · ISO 27001 A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Compliant
Entra	ENTRA-ADV-003 **Constrain the Temporary Access Pass** TAP enabled with one-time use or a short lifetime. NIST IA-5 · ISO 27001 A.5.17 · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L2	Compliant
Entra	ENTRA-ADV-009 **Review trust granted to cross-tenant partners** No partner with extended inbound trust. NIST AC-3 · ISO 27001 A.5.19 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Compliant
Entra	ENTRA-FED-001 **Inventory domains and their authentication type** 2 domain(s), all using managed (cloud) authentication — no federation to monitor. CIS Entra ID · NIST IA-8 · ISO 27001 A.5.17 · ANSSI Hybridation · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Compliant
Entra	ENTRA-FED-002 **Monitor federation certificate validity** No federated domain — no federation certificate to validate. CIS Entra ID · NIST IA-5 · ISO 27001 A.8.24 · ANSSI Hybridation · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L1	Compliant
Entra	ENTRA-ADV-011 **Deploy token protection** No policy requires token protection. → Add the 'Require token protection' session control to a Conditional Access policy covering supported platforms. NIST SC-23 · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(j) · MCSB DP	L2	Warning
Entra	ENTRA-ADV-012 **Preserve Continuous Access Evaluation (CAE)** No policy disables Continuous Access Evaluation. NIST AC-3 · ISO 27001 A.8.5 · DORA Art. 10 · NIS2 21.2(b) · MCSB IM	L2	Compliant
Entra	ENTRA-FED-003 **Verify federation certificate issuer/subject consistency** No federated domain — no issuer consistency to verify. MITRE T1484.002 · NIST IA-5 · ISO 27001 A.8.5 · ANSSI Hybridation · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Compliant
Entra	ENTRA-FED-004 **Analyze federation metadata** No federated domain — no federation metadata to analyse. NIST IA-8 · ISO 27001 A.5.17 · ANSSI Hybridation · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Compliant
Entra	ENTRA-FED-008 **Verify Pass-Through Authentication (PTA) agent status** Not assessed — the Pass-Through Authentication (PTA) agent status lives on the AD FS server / on-premises agents, not exposed by Microsoft Graph. → Deploy at least two PTA agents and monitor their health. NIST CP-2 · ISO 27001 A.5.29 · ANSSI Hybridation · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L2	Not assessed

REFERENTIAL	CONTROL	LVL	STATUS
Entra	ENTRA-FED-009 **Assess AD FS configuration** No federated domain — no AD FS configuration to assess. MITRE T1484.002 · NIST CM-6 · ISO 27001 A.8.9 · ANSSI Hybridation · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Compliant
Entra	ENTRA-FED-010 **Verify AD FS extranet lockout** No federated domain — AD FS extranet lockout not applicable. NIST AC-7 · ISO 27001 A.8.5 · ANSSI Hybridation · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Compliant
Entra	ENTRA-FED-005 **Assess Azure AD Connect configuration** No on-premises synchronization enabled (cloud-only tenant) — no Azure AD Connect configuration to assess. CIS Entra ID · NIST CM-6 · ISO 27001 A.8.9 · ANSSI Hybridation · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Compliant
Entra	ENTRA-FED-007 **Verify password hash synchronization status** No on-premises synchronization — password hash synchronization is not applicable. CIS Entra ID · NIST IA-5 · ISO 27001 A.8.5 · ANSSI Hybridation · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Compliant
Entra	ENTRA-FED-006 **Restrict synchronization scope** No on-premises synchronization — sync scope not applicable. NIST AC-6 · ISO 27001 A.8.2 · ANSSI Hybridation · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Compliant
Entra	ENTRA-FED-011 **Assess device hybrid join** No device returned — hybrid join not assessable. → Inventory hybrid-joined devices and base Conditional Access on them. NIST IA-3 · ISO 27001 A.8.1 · ANSSI Hybridation · DORA Art. 9 · NIS2 21.2(h) · MCSB ES	L2	Not assessed
Entra	ENTRA-FED-012 **Analyze cloud-only vs synced account distribution** 2 account(s): 2 cloud-only, 0 synced from on-premises AD. NIST AC-2 · ISO 27001 A.5.18 · ANSSI Hybridation · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Compliant
Entra	ENTRA-FED-013 **Verify Entra Connect sync client currency** No on-premises synchronization — sync client version not applicable. NIST SI-2 · ISO 27001 A.8.8 · ANSSI Hybridation · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Compliant
Entra	ENTRA-PIM-003 **Eliminate permanent privileged assignments** Check error: Graph 400 : The tenant needs to have Microsoft Entra ID P2 or Microsoft Entra ID Governance license. → In PIM, replace active assignments with eligible assignments requiring temporary activation. 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) · MCSB PA-2	L2	Error
Entra	ENTRA-PIM-005 **Prohibit synced accounts in privileged roles** No on-premises-synced account in a privileged role. CIS Entra ID 1.1.2 · NIST AC-6 · ISO 27001 A.8.2 · CISA SCuBA MS.AAD.7.3 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-2	L1	Compliant
Entra	ENTRA-PIM-008 **Remove disabled accounts from privileged roles** No disabled account retains a privileged role. NIST AC-2 · ISO 27001 A.5.18 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-2	L1	Compliant
Entra	ENTRA-PIM-004 **Prohibit guests in privileged roles** No guest account in a privileged role. CIS Entra ID 1.1.3 · NIST AC-6 · ISO 27001 A.5.15 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-2	L1	Compliant
Entra	ENTRA-PIM-002 **Inventory all privileged role assignments** 2 privileged role assignment(s) across 2 distinct principal(s). CIS Entra ID 1.1 · NIST AC-2 · ISO 27001 A.5.18 · CISA SCuBA MS.AAD.7.2 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-2	L1	Compliant
Entra	ENTRA-PIM-001 **Enumerate Global Administrators** 2 Global Administrator(s) — within the recommended range (2 to 4). CIS Entra ID 1.1.1 · NIST AC-6 · ISO 27001 A.8.2 · CISA SCuBA MS.AAD.7.1 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-2	L1	Compliant

REFERENTIAL	CONTROL	LVL	STATUS
Entra	ENTRA-PIM-012 **Validate break-glass accounts** No identifiable break-glass account — create at least two, cloud-only, excluded from blocking policies. → Create two cloud-only break-glass accounts, monitor their use, and exclude them from blocking CA. CIS Entra ID 1.1.7 · NIST CP-2 · ISO 27001 A.5.29 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-2	L1	Warning
Entra	ENTRA-PIM-013 **Enforce separate admin accounts** 2 privileged account(s) with an active mailbox — prefer dedicated admin accounts separate from daily mail. → Create dedicated admin accounts without a mail licence. NIST AC-6(5) · ISO 27001 A.8.2 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-2	L2	Warning
Entra	ENTRA-PIM-006 **Require MFA for all privileged accounts** Check error: Graph 403 : Tenant is not a B2C tenant and doesn't have premium license → Enroll a strong MFA method on every privileged account and enforce MFA via Conditional Access. CIS Entra ID 1.1.5 · NIST IA-2(1) · ISO 27001 A.8.5 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(j) · MCSB PA-2	L1	Error
Entra	ENTRA-PIM-007 **Eliminate weak auth methods on privileged accounts** Check error: Graph 403 : Tenant is not a B2C tenant and doesn't have premium license → Roll out FIDO2 keys or Microsoft Authenticator 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) · MCSB PA-2	L2	Error
Entra	ENTRA-PIM-011 **Retain PIM activation history** Check error: Graph 403 : {"errorCode":"PermissionScopeNotGranted","message":"Authorization failed due to missing permission scope RoleAssignmentSchedule.ReadWrite.Directory,RoleManagement.ReadWrite.Directory,RoleAssignmentSch… → Verify PIM history access and retain audit logs. NIST AU-2 · ISO 27001 A.8.15 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-2	L2	Error
Entra	ENTRA-WKL-001 **Identify applications still holding expired secrets** No application holds an expired credential. NIST IA-5 · ISO 27001 A.5.17 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM-3	L1	Compliant
Entra	ENTRA-PIM-009 **Enumerate never-signed-in privileged accounts** Check error: Graph 403 : Tenant is not a B2C tenant and doesn't have premium license → Review and disable dormant privileged accounts. NIST AC-2(3) · ISO 27001 A.5.18 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-2	L2	Error
Entra	ENTRA-WKL-003 **Enforce an application credential management policy** Policy enabled but without application secret restrictions. → Enable the default app management policy and add passwordCredentials restrictions (ban or maximum lifetime). NIST CM-6 · ISO 27001 A.8.9 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM-3	L2	Warning
Entra	ENTRA-PIM-010 **Configure PIM settings for privileged roles** Check error: Graph 400 : The tenant needs to have Microsoft Entra ID P2 or Microsoft Entra ID Governance license. → Configure PIM role settings (max activation, MFA, justification, approval). CIS Entra ID 1.1.4 · NIST AC-6(1) · ISO 27001 A.8.2 · CISA SCuBA MS.AAD.7.8 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-2	L2	Error
Entra	ENTRA-PIM-014 **Enable role assignment notifications** Check error: Graph 400 : The tenant needs to have Microsoft Entra ID P2 or Microsoft Entra ID Governance license. → Enable notification rules in the PIM settings of sensitive roles. NIST AU-6 · ISO 27001 A.5.25 · CISA SCuBA MS.AAD.7.7 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-2	L2	Error
Entra	ENTRA-WKL-005 **Prohibit guest accounts as application owners** No guest account owns an application. NIST AC-6 · ISO 27001 A.8.2 · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1	L1	Compliant
Entra	ENTRA-WKL-009 **Ban insecure redirect URIs** No insecure redirect URI. NIST SC-8 · ISO 27001 A.8.26 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L1	Compliant

REFERENTIAL	CONTROL	LVL	STATUS
Entra	ENTRA-WKL-010 **Review multi-tenant applications carrying credentials** No multi-tenant application carrying credentials. NIST AC-3 · ISO 27001 A.5.15 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Compliant
Entra	ENTRA-005 **Enable number matching in Microsoft Authenticator** Microsoft Authenticator enabled (number matching enforced by Microsoft). 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) · MCSB IM-6	L1	Compliant
Entra	ENTRA-007 **Deploy phishing-resistant methods** FIDO2 / passkeys enabled. CIS Entra ID · NIST IA-2 · ISO 27001 A.8.5 · CISA SCuBA MS.AAD.3.1 · DORA Art. 10 · NIS2 21.2(b) · MCSB IM	L2	Compliant
Entra	ENTRA-004 **Ensure all member accounts are MFA-capable** Check error: Graph 403 : Tenant is not a B2C tenant and doesn't have premium license → Track the method registration report (Protection > Authentication methods > Activity) and have non-capable users register a strong method. CIS Entra ID · NIST IA-2 · ISO 27001 A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Error
Entra	ENTRA-010 **Limit the number of global administrators to between two and four** 2 administrateur(s) général(aux) — recommandé : 2 à 4. 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) · MCSB PA-1	L1	Compliant
Entra	ENTRA-011 **Use dedicated, cloud-only administrator accounts** No global administrator synchronized from on-premises AD. 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) · MCSB PA-1	L1	Compliant
Entra	ENTRA-WKL-007 **Identify service principals carrying their own credentials** 1 service principal(s) carry their own credentials: review them. → Move credentials to the app registration, or document and rotate legitimate exceptions. NIST IA-5 · ISO 27001 A.5.17 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM-3	L2	Warning
Entra	ENTRA-017 **Prevent users from registering applications** Application registration by users is prohibited. CIS Entra ID · NIST CM-7, AC-6 · ISO 27001 A.8.19 · CISA SCuBA MS.AAD.5.1 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L1	Compliant
Entra	ENTRA-020 **Restrict guest user permissions** Guest access at the default level (hardening recommended). → Users > User settings > External collaboration settings: set guest access to "most restrictive". CIS Entra ID · NIST AC-2, AC-21 · ISO 27001 A.5.14 · CISA SCuBA MS.AAD.8.1 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L1	Warning
Entra	ENTRA-021 **Limit who can invite guest users** All members can invite guests. → External collaboration settings: limit sending invitations to administrators and delegated roles (not "everyone"). CIS Entra ID · NIST AC-2, AC-21 · ISO 27001 A.5.14 · CISA SCuBA MS.AAD.8.2 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L1	Warning
Entra	ENTRA-019 **Monitor expiring application credentials** No application credential expires within 30 days (sample). CIS Entra ID · NIST CM-7, AC-6 · ISO 27001 A.8.19 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Compliant
Entra	ENTRA-018 **Review high-privilege application permissions** No high-privilege Graph application permission granted. CIS Entra ID · NIST CM-7, AC-6 · ISO 27001 A.8.19 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Compliant
Entra	ENTRA-022 **Review and limit guest accounts** No guest account in the tenant. CIS Entra ID · NIST AC-2, AC-21 · ISO 27001 A.5.14 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Compliant
Entra	ENTRA-013	L2	Error

REFERENTIAL	CONTROL	LVL	STATUS
	Enable just-in-time privileged access via PIM Check error: Graph 400 : The tenant needs to have Microsoft Entra ID P2 or Microsoft Entra ID Governance license. → Identity Governance > Privileged Identity Management: make privileged roles eligible (on-demand, time-limited activation with justification/approval). CIS Entra ID · NIST AC-6 · ISO 27001 A.8.2 · CISA SCuBA MS.AAD.7.4 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1		
Entra	ENTRA-025 **Align the password expiration policy** Passwords do not expire (aligned with MFA). CIS Entra ID · NIST IA-5 · ISO 27001 A.5.17 · CISA SCuBA MS.AAD.6.1 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L2	Compliant
Entra	ENTRA-016 **Enable the admin consent request workflow** Admin consent request workflow enabled. CIS Entra ID · NIST CM-7, AC-6 · ISO 27001 A.8.19 · CISA SCuBA MS.AAD.5.3 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1	L1	Compliant
Entra	ENTRA-WKL-006 **Identify service principals with no sign-in activity** 489 service principal(s) with no sign-in for 90 days: review them. → Review principals inactive for more than 90 days; disable then delete those no longer needed. NIST AC-2 · ISO 27001 A.5.16 · DORA Art. 10 · NIS2 21.2(b) · MCSB IM-1	L2	Warning
Entra	ENTRA-030 **Enable continuous access evaluation (CAE)** CAE not explicitly configured (may be active by default). → Conditional Access: keep continuous access evaluation enabled (default) and avoid disabling it in policies. CIS Entra ID · NIST AC-2, AC-12 · ISO 27001 A.8.2, A.8.5 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Warning
Entra	ENTRA-033 **Enable sign-in and audit logs** Check error: Graph 403 : Tenant is not a B2C tenant and doesn't have premium license → Retain sign-in and audit logs and export them (diagnostic settings) to a Log Analytics / Microsoft Sentinel workspace for retention. CIS Entra ID · NIST SI-4 · ISO 27001 A.8.16 · ANSSI Journalisation · DORA Art. 10 · NIS2 21.2(b) · MCSB LT	L1	Error
Entra	ENTRA-041 **Disable user creation via email verification** User creation via email verification is disabled. CIS Entra ID · NIST AC-2, AC-21 · ISO 27001 A.5.14 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L1	Compliant
Entra	ENTRA-043 **Control federation relationships and ADFS configuration** No federated domain (cloud authentication). CIS Entra ID · NIST CM-6 · ISO 27001 A.8.9 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1	L2	Compliant
Entra	ENTRA-044 **Restrict security group creation to administrators** Security group creation is restricted to administrators. CIS Entra ID · NIST CM-6 · ISO 27001 A.8.9 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1	L2	Compliant
Entra	ENTRA-035 **Automate the identity lifecycle** Check error: Graph 403 : Insufficient license to complete this operation. User workflows require an Entra ID Governance license. Agent-related workflows require a Microsoft Agent 365 or Microsoft 365 E7 license. See https://a… → Identity Governance > Lifecycle Workflows: create joiner / mover / leaver workflows to automate onboarding and offboarding. CIS Entra ID · NIST AC-2 · ISO 27001 A.5.16 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Error
Entra	ENTRA-048 **Configure technical and security notification contacts** Technical notification contacts are configured. CIS Entra ID · NIST CM-6 · ISO 27001 A.8.9 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L1	Compliant
Entra	ENTRA-050 **Enable Temporary Access Pass for secure onboarding** Temporary Access Pass is enabled. CIS Entra ID · NIST IA-2 · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Compliant
Entra	ENTRA-038 **Detect direct or hidden privileged role assignments** Check error: Graph 400 : The tenant needs to have Microsoft Entra ID P2 or Microsoft Entra ID	L2	Error

REFERENTIAL	CONTROL	LVL	STATUS
	Governance license. → Review permanent privileged role assignments and convert them to PIM eligibility; remove unjustified direct assignments. CIS Entra ID · NIST AC-6 · ISO 27001 A.8.2 · CISA SCuBA MS.AAD.7.5 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1		
Entra	ENTRA-057 **Prohibit insecure redirect URIs (HTTP)** No insecure redirect URI detected (sample). CIS Entra ID · NIST CM-7, AC-6 · ISO 27001 A.8.19 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Compliant
Entra	ENTRA-060 **Govern cross-tenant access (B2B) settings** Automatic cross-tenant consent disabled (default settings controlled). CISA SCuBA MS.AAD.8.3 · CIS Entra · NIST AC-21 · ISO 27001 A.5.14 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Compliant
Entra	ENTRA-063 **Enable self-service password reset (SSPR)** Self-service password reset (SSPR) is enabled. Microsoft Secure Score · NIST IA-5 · ISO 27001 A.5.17 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L2	Compliant
Entra	ENTRA-062 **Clean up stale devices in the directory** No enabled device registered in the directory. CIS Entra · NIST CM-8 · ISO 27001 A.5.9 · DORA Art. 9 · NIS2 21.2(h) · MCSB ES	L2	Compliant
Entra	ENTRA-064 **Prevent users from recovering BitLocker keys** Users can recover BitLocker keys for their owned devices. → Entra > Devices > Settings: 'Restrict users from recovering BitLocker keys' = Yes. CIS Entra · NIST AC-6 · ISO 27001 A.8.2 · DORA Art. 9 · NIS2 21.2(h) · MCSB DP	L2	Warning
Entra	ENTRA-065 **Show sign-in context in Microsoft Authenticator** Context shown in Authenticator: application and location. CIS Entra · NIST IA-2 · ISO 27001 A.8.5 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L1	Compliant
Entra	ENTRA-066 **Enable report suspicious activity** Report suspicious activity is not enabled — users cannot report fraudulent MFA prompts. → Entra > Protection > Authentication methods > Settings: 'Report suspicious activity' = Enabled. CIS Entra · NIST IR-6 · ISO 27001 A.6.8 · DORA Art. 10 · NIS2 21.2(b) · MCSB LT	L1	Warning
Entra	ENTRA-061 **Disable inactive Entra accounts** Check error: Graph 403 : Tenant is not a B2C tenant and doesn't have premium license → Inventory accounts with no sign-in for 90 days (signInActivity), disable then remove them after validation. CISA SCuBA · CIS Entra · NIST AC-2 · ISO 27001 A.5.16 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Error
Entra	ENTRA-067 **Enforce an application credential management policy** App management policy enabled. CIS Entra · Microsoft Secure Score · NIST IA-5 · ISO 27001 A.5.17 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Compliant
Entra	ENTRA-058 **Configure named locations** No named location defined for Conditional Access. → Entra > Protection > Conditional Access > Named locations: define trusted IPs and countries. CIS Entra ID · NIST AC-3 · ISO 27001 A.8.5 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L1	Warning
Entra	ENTRA-049 **Control self-service sign-up** Self-service sign-up is enabled — verify this is intentional. → External collaboration settings / user flow: govern or disable self-service sign-up. CIS Entra ID · NIST AC-2, AC-21 · ISO 27001 A.5.14 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1	L2	Warning
Entra	ENTRA-068 **Restrict access to the Entra admin portal** Standard users can read the directory — restrict admin portal and directory data access. → Entra > User settings: restrict access to the admin portal and harden default user permissions. CIS Entra · NIST AC-6 · ISO 27001 A.8.2 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1	L2	Warning
Entra	ENTRA-069 **Restrict B2B invitations to administrators** B2B invitations are broadly open (adminsGuestInvitersAndAllMembers) — restrict to admins and	L1	Warning

REFERENTIAL	CONTROL	LVL	STATUS
	delegated inviters. → Entra > External Identities > External collaboration settings: 'Restrict invitations to users with inviter roles'. CIS Entra · CISA SCuBA MS.AAD.8.2 · NIST AC-21 · ISO 27001 A.5.14 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1		
Entra	ENTRA-070 **Block LinkedIn account synchronization** Check error: Graph 400 : Resource not found for the segment 'settings'. → M365 admin center > Settings > Org settings > LinkedIn account connections: disable. CIS Entra · NIST AC-21 · ISO 27001 A.5.14 · DORA Art. 9 · NIS2 21.2(i) · MCSB IM	L2	Error
Entra	ENTRA-073 **Require justification when activating a PIM role** Check error: Graph 400 : The tenant needs to have Microsoft Entra ID P2 or Microsoft Entra ID Governance license. → Entra > Identity Governance > Privileged Identity Management > Microsoft Entra roles > Role settings > Activation: enable 'Require justification'. CIS Entra ID · NIST AC-2 · ISO 27001 A.5.15 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1	L1	Error
Entra	ENTRA-074 **Require approval when activating a PIM role** Check error: Graph 400 : The tenant needs to have Microsoft Entra ID P2 or Microsoft Entra ID Governance license. → Entra > PIM > Role settings > Activation: enable 'Require approval to activate' and set approvers. CIS Entra ID · NIST AC-6 · ISO 27001 A.5.15 · CISA SCuBA MS.AAD.7.6 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1	L2	Error
Entra	ENTRA-075 **Limit the maximum PIM role activation duration** Check error: Graph 400 : The tenant needs to have Microsoft Entra ID P2 or Microsoft Entra ID Governance license. → 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) · MCSB PA-1	L2	Error
Entra	ENTRA-076 **Export sign-in and audit logs to durable storage** Azure Resource Manager connection failed: Aucun abonnement accessible (rôle RBAC « Reader » manquant sur l'abonnement ?). → Entra > Monitoring > Diagnostic settings: add a setting sending SignInLogs and AuditLogs to Log Analytics / storage / Event Hub. CIS Entra ID · NIST AU-6 · ISO 27001 A.8.15 · CISA SCuBA MS.AAD.4.1 · ANSSI Journalisation · DORA Art. 10 · NIS2 21.2(b) · MCSB LT	L1	Error
Entra	ENTRA-077 **Configure Entra diagnostic settings to Azure Monitor** Azure Resource Manager connection failed: Aucun abonnement accessible (rôle RBAC « Reader » manquant sur l'abonnement ?). → Entra > Monitoring > Diagnostic settings: create a setting covering AuditLogs, SignInLogs, and available risk categories. 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) · MCSB LT	L1	Error
Entra	ENTRA-078 **Alert on Conditional Access policy changes** Azure Resource Manager connection failed: Aucun abonnement accessible (rôle RBAC « Reader » manquant sur l'abonnement ?). → Route AuditLogs to Log Analytics then create an alert rule on 'Update/Add/Delete conditional access policy' operations. CIS Entra ID · NIST AU-6 · ISO 27001 A.8.15 · ANSSI MFA · DORA Art. 10 · NIS2 21.2(b) · MCSB LT	L2	Error
Entra	ENTRA-072 **Configure access reviews for PIM eligible roles** Check error: Graph 400 : The tenant needs to have Microsoft Entra ID P2 or Microsoft Entra ID Governance license. → Entra > Identity Governance > Access reviews: create a periodic review targeting PIM eligible roles. CIS Entra · NIST AC-2 · ISO 27001 A.5.18 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1	L2	Error
Entra	ENTRA-081 **Exclude emergency access accounts from blocking policies** No active blocking policy. CIS Microsoft 365 1.1.x · NIST CP-2 · ISO 27001 A.5.29 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1	L1	Compliant
Entra	ENTRA-083 **Use restricted management administrative units** No restricted management administrative unit: sensitive accounts remain modifiable by any administrator holding the role.	L2	Warning

REFERENTIAL	CONTROL	LVL	STATUS
	→ Entra portal > Roles and administrators > Administrative units: create a restricted management unit for sensitive accounts. NIST AC-6 · ISO 27001 A.8.2 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1		
Entra	ENTRA-084 **Deploy certificate-based authentication** Certificate-based authentication is disabled: it is however the phishing-resistant method best suited to administrative accounts. → Entra portal > Protection > Authentication methods: enable certificate-based authentication and target it at administrators. NIST IA-2(1) · ISO 27001 A.5.17 · ANSSI MFA · DORA Art. 9 · NIS2 21.2(j) · MCSB IM-6	L2	Warning
Entra	ENTRA-085 **Audit privileged roles assigned to service principals** 9 service principal(s) hold a directory role: these identities escape MFA and PIM, their justification must be documented. → Entra portal > Roles and administrators: inventory service principals holding a role and remove those not justified. NIST AC-2 · ISO 27001 A.5.16 · ANSSI Administration · DORA Art. 10 · NIS2 21.2(b) · MCSB LT	L1	Warning
Entra	ENTRA-071 **Audit high-permission service principals with active credentials** 1 service principal(s) carry a client secret — review their Graph permissions and prefer certificates. → Review service principals with secrets; prefer certificates and remove unnecessary permissions. CIS Entra · NIST IA-5 · ISO 27001 A.8.2 · ANSSI Journalisation · DORA Art. 10 · NIS2 21.2(b) · MCSB LT	L2	Warning
Entra	ENTRA-059 **Disallow guests in administrative roles** No guests in administrative roles. CIS Entra ID · NIST AC-6 · ISO 27001 A.8.2 · ANSSI Administration · DORA Art. 9 · NIS2 21.2(i) · MCSB PA-1	L1	Compliant