SAMPLE REPORT · FICTITIOUS COMPANY AND DATA, FOR ILLUSTRATION ONLY

Microsoft 365 Security Assessment

Findings Report

Prepared for: Sample Company, Inc. · **Ref:** SAMPLE-M365-0000 · **Date:** November 19, 2026

Scope: Read-only review of the Microsoft 365 tenant (11111111-1111-1111-1111-111111111111). No settings were changed.

> We evaluated 82 security controls across your Microsoft 365 environment. 40 issues need attention, including 4 critical and 10 high severity issues.
>
> This report lists each item that needs attention, sorted by severity, with what we found and why it matters. We will walk you through it together and discuss how to address each item.

AT A GLANCE

OVERALL RATING	SECURITY SCORE	CRITICAL	HIGH	MEDIUM	LOW
High risk	52 / 100	4	10	18	8

41 of 82 security controls passed. Microsoft Secure Score at the time of the assessment: 30.0 of 100.0 (30%).

Area	Critical	High	Medium	Low
Applications and Consent		1	2	
Conditional Access	3	2	4	
Email Domain Protection (SPF, DKIM, DMARC)		4	2	3
External Identities			2	1
Identity Security	1		3	
Privileged Access		1	1	
Security Monitoring and Audit Logging				1
SharePoint and OneDrive		2	3	1
Threat Detection (Microsoft Defender)				1
User Account Security			1	1
Total	**4**	**10**	**18**	**8**

FINDINGS BY SEVERITY

#	Severity	Area	Finding	Affected
001	CRITICAL	Conditional Access	MFA is not enforced for 14 administrative role(s): Application Administrator, Authentication Administrator, Billing…	14
002	CRITICAL	Conditional Access	No enabled Conditional Access policy requires MFA for all users.	-

SAMPLE

003	CRITICAL	Identity Security	Security Defaults are disabled and no enabled Conditional Access policy enforces MFA or blocks sign-ins.	-
004	CRITICAL	Conditional Access	No enabled Conditional Access policy blocks legacy authentication.	-
005	HIGH	Conditional Access	Phishing-resistant MFA is not enforced for 14 administrative role(s): Application Administrator, Authentication Administrator…	14
006	HIGH	Email Domain Protection (SPF, DKIM, DMARC)	Domain(s) can be spoofed: neither SPF hard fail nor DMARC enforcement on: contoso.example.	1
007	HIGH	Applications and Consent	Users can consent to any application requesting any permission (legacy default consent policy)	1
008	HIGH	SharePoint and OneDrive	Legacy authentication protocols are enabled for SharePoint Online (bypasses modern auth / MFA for legacy clients)	-
009	HIGH	Email Domain Protection (SPF, DKIM, DMARC)	No valid DMARC record on: contoso.example.	1
010	HIGH	Email Domain Protection (SPF, DKIM, DMARC)	1 domain(s) publish no SPF record: contoso.example.	1
011	HIGH	SharePoint and OneDrive	SharePoint external sharing is 'externalUserAndGuestSharing': 'Anyone' (anonymous) links are permitted tenant-wide.	-
012	HIGH	Email Domain Protection (SPF, DKIM, DMARC)	DMARC policy not enforced on: contoso.example.	1
013	HIGH	Privileged Access	Only 1 Global Administrator(s): no redundancy if the account is lost (PIM eligibility not readable: count reflects…	1
014	HIGH	Conditional Access	No enabled policy requires MFA from guest / external users for all apps.	-
015	MEDIUM	Email Domain Protection (SPF, DKIM, DMARC)	Microsoft 365 DKIM signing not configured on: contoso.example.	1
016	MEDIUM	Email Domain Protection (SPF, DKIM, DMARC)	SPF does not end in hard fail on: contoso.example.	1
017	MEDIUM	External Identities	Anyone in the organisation, including guests, can invite external users.	1
018	MEDIUM	Applications and Consent	Any user can register applications in the tenant.	1
019	MEDIUM	External Identities	Guests have the same directory access as members.	1
020	MEDIUM	Applications and Consent	Admin consent request workflow is disabled or has no reviewers; users have no sanctioned path to request app consent.	1
021	MEDIUM	Conditional Access	No enabled policy requires a compliant / hybrid-joined device for administrative roles.	-
022	MEDIUM	Identity Security	Authentication method 'Sms' is enabled; expected disabled.	1
023	MEDIUM	Conditional Access	No enabled policy targets the 'Register security information' user action.	-
024	MEDIUM	Conditional Access	No enabled policy configures sign-in frequency for admins.	-
025	MEDIUM	Identity Security	Microsoft Authenticator additional context is not enabled: displayAppInformationRequiredState…	1
026	MEDIUM	Privileged Access	0 privileged account(s) have not signed in for more than 60 days; 1 have no recorded sign-in (may be break-glass or never used)	1

SAMPLE

027	MEDIUM	User Account Security	0 enabled account(s) have not signed in for more than 90 days; 1 enabled account(s) older than 90 days have no recorded sign-in.	1
028	MEDIUM	Conditional Access	No enabled policy configures persistent browser session = never for admins.	-
029	MEDIUM	Identity Security	No custom banned password list is configured.	1
030	MEDIUM	SharePoint and OneDrive	External sharing is enabled without any domain allow/block list (sharingDomainRestrictionMode=none)	-
031	MEDIUM	SharePoint and OneDrive	External users (guests) are allowed to reshare content they do not own.	-
032	MEDIUM	SharePoint and OneDrive	Sharing invitations can be accepted by any account (invited and accepting user need not match)	-
033	LOW	Email Domain Protection (SPF, DKIM, DMARC)	DMARC subdomain policy not enforced on: contoso.example.	1
034	LOW	Email Domain Protection (SPF, DKIM, DMARC)	DMARC aggregate reporting (rua) not configured on: contoso.example.	1
035	LOW	External Identities	Email-verified users can self-join the organisation (viral tenant join)	1
036	LOW	Security Monitoring and Audit Logging	Audit retention is limited to 180 days (unified audit log) and 30 days (Entra audit/sign-in logs); incidents discovered later...	1
037	LOW	Email Domain Protection (SPF, DKIM, DMARC)	MTA-STS (enforce) and/or TLS-RPT not published on: contoso.example.	1
038	LOW	SharePoint and OneDrive	Idle session sign-out for unmanaged devices is disabled.	-
039	LOW	Threat Detection (Microsoft Defender)	Microsoft Secure Score is 30.0% (30.0/100.0), below the 40% threshold.	-
040	LOW	User Account Security	1 enabled member account(s) have no licence (service, shared-mailbox or orphaned accounts.	1

FINDING DETAILS

001. MFA is not enforced for 14 administrative role(s): Application Administrator, Authentication Administrator, Billing...

CRITICAL Conditional Access · Control checked: MFA is required for administrative roles · Confirmed from configuration

What we found: MFA is not enforced for 14 administrative role(s): Application Administrator, Authentication Administrator, Billing Administrator, Cloud Application Administrator, Conditional Access Administrator, Exchange Administrator, Global Administrator, Helpdesk Administrator, Password Administrator, Privileged Authentication Administrator, Privileged Role Administrator, Security Administrator, SharePoint Administrator, User Administrator.

Why it matters: A compromised administrator account yields full tenant control.

Affected (14): Global Administrator, Privileged Role Administrator, Privileged Authentication Administrator, Security Administrator, Exchange Administrator, SharePoint Administrator, Conditional Access Administrator, Application Administrator, Cloud Application Administrator, User Administrator, and 4 more

Related standards: CIS M365 Foundations v4 5.2.2.1 · NIST CSF 2.0 PR.AA-03 · NIST SP 800-53 IA-2(1) · NIST SP 800-171 3.5.3

002. No enabled Conditional Access policy requires MFA for all users.

CRITICAL Conditional Access · Control checked: MFA is required for all users · Confirmed from configuration

What we found: No enabled Conditional Access policy requires MFA for all users.

Why it matters: MFA stops the vast majority of credential-based account compromises.

Related standards: CIS M365 Foundations v4 5.2.2.2 · NIST CSF 2.0 PR.AA-03 · NIST SP 800-53 IA-2(1) · NIST SP 800-171 3.5.3

SAMPLE

003. Security Defaults are disabled and no enabled Conditional Access policy enforces MFA or blocks sign-ins.

CRITICAL Identity Security · Control checked: Tenant-wide MFA enforcement baseline (Security Defaults or Conditional Access) · Confirmed from configuration

What we found: Security Defaults are disabled and no enabled Conditional Access policy enforces MFA or blocks sign-ins.

Why it matters: Without Security Defaults or Conditional Access, accounts are protected by a password alone. Password spray, credential stuffing and phishing lead directly to account takeover.

Related standards: CIS M365 Foundations v4 5.1.2.2 · NIST CSF 2.0 PR.AA-03 · NIST SP 800-53 IA-2(1) · NIST SP 800-171 3.5.3

004. No enabled Conditional Access policy blocks legacy authentication.

CRITICAL Conditional Access · Control checked: Legacy authentication is blocked · Confirmed from configuration

What we found: No enabled Conditional Access policy blocks legacy authentication.

Why it matters: Legacy protocols bypass MFA entirely; over 97% of password-spray attacks target them.

Related standards: CIS M365 Foundations v4 5.2.2.3 · NIST CSF 2.0 PR.AA-03 · NIST SP 800-53 IA-2(1) · NIST SP 800-171 3.5.3

005. Phishing-resistant MFA is not enforced for 14 administrative role(s): Application Administrator, Authentication Administrator...

HIGH Conditional Access · Control checked: Phishing-resistant MFA is required for administrators · Confirmed from configuration

What we found: Phishing-resistant MFA is not enforced for 14 administrative role(s): Application Administrator, Authentication Administrator, Billing Administrator, Cloud Application Administrator, Conditional Access Administrator, Exchange Administrator, Global Administrator, Helpdesk Administrator, Password Administrator, Privileged Authentication Administrator, Privileged Role Administrator, Security Administrator, SharePoint Administrator, User Administrator.

Why it matters: Push/SMS MFA is defeated by adversary-in-the-middle phishing kits (Evilginx) and MFA fatigue.

Affected (14): Global Administrator, Privileged Role Administrator, Privileged Authentication Administrator, Security Administrator, Exchange Administrator, SharePoint Administrator, Conditional Access Administrator, Application Administrator, Cloud Application Administrator, User Administrator, and 4 more

Related standards: CIS M365 Foundations v4 5.2.2.1 · NIST SP 800-63B AAL3 · NIST SP 800-53 IA-2(1)

006. Domain(s) can be spoofed: neither SPF hard fail nor DMARC enforcement on: contoso.example.

HIGH Email Domain Protection (SPF, DKIM, DMARC) · Control checked: Domain spoofing exposure - no SPF hard fail and no DMARC enforcement · Confirmed from configuration

What we found: Domain(s) can be spoofed: neither SPF hard fail nor DMARC enforcement on: contoso.example.

Why it matters: Anyone can send mail as the organisation's domain to customers, partners and staff with a high probability of inbox delivery.

Affected (1): contoso.example

Related standards: CIS Microsoft 365 Foundations Benchmark v4.0 2.1.8, 2.1.10 · NIST SP 800-53 Rev. 5 SC-8, SC-20 · NIST CSF 2.0 PR.DS-02 · CMMC 2.0 Level 2 SC.L2-3.13.8

007. Users can consent to any application requesting any permission (legacy default consent policy)

HIGH Applications and Consent · Control checked: User consent to applications is restricted · Confirmed from configuration

What we found: Users can consent to any application requesting any permission (legacy default consent policy)

Why it matters: OAuth consent phishing bypasses MFA and password resets.

Affected (1): authorizationPolicy

Related standards: CIS M365 Foundations v4 5.1.5.2 · NIST SP 800-53 AC-6

008. Legacy authentication protocols are enabled for SharePoint Online (bypasses modern auth / MFA for legacy clients)

HIGH SharePoint and OneDrive · Control checked: Legacy authentication protocols are enabled for SharePoint Online · Confirmed from configuration

What we found: Legacy authentication protocols are enabled for SharePoint Online (bypasses modern auth / MFA for legacy clients)

Why it matters: Legacy clients authenticate with username/password only; MFA and device-based Conditional Access are not enforced.

Related standards: CIS M365 Foundations v4.0 7.2.1 · NIST SP 800-53 r5 IA-2(1), AC-17 · NIST SP 800-171 r2 3.5.3 · CMMC L2 IA.L2-3.5.3

009. No valid DMARC record on: contoso.example.

HIGH Email Domain Protection (SPF, DKIM, DMARC) · Control checked: DMARC record published · Confirmed from configuration

What we found: No valid DMARC record on: contoso.example.

Why it matters: Without DMARC, SPF and DKIM results are not tied to the From: header, so display-name and exact domain spoofing succeed even when SPF/DKIM exist, and the organisation receives no visibility into who is sending as its domain.

Affected (1): contoso.example

Related standards: CIS Microsoft 365 Foundations Benchmark v4.0 2.1.10 (Ensure DMARC Records for all Exchange Online domains are published) · NIST SP 800-53 Rev. 5 SC-8, SC-20 · NIST CSF 2.0 PR.DS-02 · CMMC 2.0 Level 2 SC.L2-3.13.8

SAMPLE

010. 1 domain(s) publish no SPF record: contoso.example.

HIGH Email Domain Protection (SPF, DKIM, DMARC) · Control checked: SPF record published for every email-enabled domain · Confirmed from configuration

What we found: 1 domain(s) publish no SPF record: contoso.example.

Why it matters: Attackers can send mail that appears to originate from the organisation's domain; SPF-based filtering at the recipient cannot reject or flag it, and DMARC cannot be enforced without an SPF or DKIM pass.

Affected (1): contoso.example

Related standards: CIS Microsoft 365 Foundations Benchmark v4.0 2.1.8 (Ensure SPF records are published for all Exchange Domains) · NIST SP 800-53 Rev. 5 SC-8, SC-20 · NIST CSF 2.0 PR.DS-02 · CMMC 2.0 Level 2 SC.L2-3.13.8

011. SharePoint external sharing is 'externalUserAndGuestSharing': 'Anyone' (anonymous) links are permitted tenant-wide.

HIGH SharePoint and OneDrive · Control checked: SharePoint external sharing permits 'Anyone' (anonymous) links · Confirmed from configuration

What we found: SharePoint external sharing is 'externalUserAndGuestSharing': 'Anyone' (anonymous) links are permitted tenant-wide.

Why it matters: Anonymous links expose files to anyone holding the URL; access cannot be attributed, revoked per person, or governed by Conditional Access.

Related standards: CIS M365 Foundations v4.0 7.2.3 · NIST SP 800-53 r5 AC-3, AC-21 · NIST SP 800-171 r2 3.1.20, 3.1.22 · CMMC L2 AC.L2-3.1.22

012. DMARC policy not enforced on: contoso.example.

HIGH Email Domain Protection (SPF, DKIM, DMARC) · Control checked: DMARC policy enforced (p=quarantine pct=100 or p=reject) · Confirmed from configuration

What we found: DMARC policy not enforced on: contoso.example.

Why it matters: Receivers deliver spoofed mail that fails authentication; the organisation's customers and partners remain exposed to exact-domain impersonation.

Affected (1): contoso.example

Related standards: CIS Microsoft 365 Foundations Benchmark v4.0 2.1.10 · NIST SP 800-53 Rev. 5 SC-8, SC-20 · NIST CSF 2.0 PR.DS-02 · CMMC 2.0 Level 2 SC.L2-3.13.8

013. Only 1 Global Administrator(s): no redundancy if the account is lost (PIM eligibility not readable: count reflects...

HIGH Privileged Access · Control checked: Number of Global Administrators · Indicated by configuration

What we found: Only 1 Global Administrator(s): no redundancy if the account is lost (PIM eligibility not readable: count reflects permanent/active members only)

Why it matters: Each GA account is a single point of total compromise.

Affected (1): admin@contoso.example

Related standards: CIS M365 Foundations v4 1.1.3 · NIST SP 800-53 AC-6(5) · NIST SP 800-171 3.1.5 · CMMC L2 AC.L2-3.1.5

014. No enabled policy requires MFA from guest / external users for all apps.

HIGH Conditional Access · Control checked: Guest and external users are required to use MFA · Confirmed from configuration

What we found: No enabled policy requires MFA from guest / external users for all apps.

Why it matters: Compromised partner accounts access shared SharePoint/Teams data without MFA.

Related standards: CIS M365 Foundations v4 5.2.2.2 · NIST SP 800-53 IA-8

015. Microsoft 365 DKIM signing not configured on: contoso.example.

MEDIUM Email Domain Protection (SPF, DKIM, DMARC) · Control checked: DKIM signing enabled for Microsoft 365 (selector1/selector2 CNAMEs published) · Indicated by configuration

What we found: Microsoft 365 DKIM signing not configured on: contoso.example.

Why it matters: Without aligned DKIM, DMARC relies on SPF alone; forwarded or mailing-list mail fails DMARC and message integrity cannot be verified by receivers.

Affected (1): contoso.example

Related standards: CIS Microsoft 365 Foundations Benchmark v4.0 2.1.9 (Ensure DKIM is enabled for all Exchange Online Domains) · NIST SP 800-53 Rev. 5 SC-8, SC-20 · NIST CSF 2.0 PR.DS-02 · CMMC 2.0 Level 2 SC.L2-3.13.8

016. SPF does not end in hard fail on: contoso.example.

MEDIUM Email Domain Protection (SPF, DKIM, DMARC) · Control checked: SPF record ends with hard fail (-all) · Confirmed from configuration

What we found: SPF does not end in hard fail on: contoso.example.

Why it matters: With soft fail, neutral or pass, spoofed messages are delivered (possibly to junk) instead of being rejected, weakening SPF as a spoofing control.

Affected (1): contoso.example

Related standards: CIS Microsoft 365 Foundations Benchmark v4.0 2.1.8 · NIST SP 800-53 Rev. 5 SC-8, SC-20 · NIST CSF 2.0 PR.DS-02 · CMMC 2.0 Level 2 SC.L2-3.13.8

SAMPLE

017. Anyone in the organisation, including guests, can invite external users.

MEDIUM External Identities · Control checked: Guest invitations restricted to admins and guest inviters · Confirmed from configuration

What we found: Anyone in the organisation, including guests, can invite external users.

Why it matters: Uncontrolled external access growth.

Affected (1): authorizationPolicy

Related standards: CIS M365 Foundations v4 5.1.6.2 · NIST SP 800-53 AC-2

018. Any user can register applications in the tenant.

MEDIUM Applications and Consent · Control checked: Users cannot register applications · Confirmed from configuration

What we found: Any user can register applications in the tenant.

Why it matters: Shadow apps with secrets; consent-phishing infrastructure inside the tenant.

Affected (1): authorizationPolicy

Related standards: CIS M365 Foundations v4 5.1.2.3 · NIST SP 800-53 CM-7

019. Guests have the same directory access as members.

MEDIUM External Identities · Control checked: Guest user access is restricted · Confirmed from configuration

What we found: Guests have the same directory access as members.

Why it matters: Guests can enumerate the directory for phishing target lists.

Affected (1): authorizationPolicy

Related standards: CIS M365 Foundations v4 5.1.6.1 · NIST SP 800-53 AC-6

020. Admin consent request workflow is disabled or has no reviewers; users have no sanctioned path to request app consent.

MEDIUM Applications and Consent · Control checked: Admin consent request workflow is enabled · Confirmed from configuration

What we found: Admin consent request workflow is disabled or has no reviewers; users have no sanctioned path to request app consent.

Why it matters: Ad-hoc admin consents without review.

Affected (1): Admin consent requests

Related standards: CIS M365 Foundations v4 5.1.5.3

021. No enabled policy requires a compliant / hybrid-joined device for administrative roles.

MEDIUM Conditional Access · Control checked: Administrators must use a compliant or hybrid-joined device · Confirmed from configuration

What we found: No enabled policy requires a compliant / hybrid-joined device for administrative roles.

Why it matters: Admin credentials and tokens can be used from unmanaged or infected devices.

Related standards: NIST CSF 2.0 PR.AA-05 · NIST SP 800-53 AC-6(2)

022. Authentication method 'Sms' is enabled; expected disabled.

MEDIUM Identity Security · Control checked: SMS authentication method is disabled · Confirmed from configuration

What we found: Authentication method 'Sms' is enabled; expected disabled.

Why it matters: SMS codes can be intercepted or socially engineered from carriers.

Affected (1): Sms

Related standards: NIST SP 800-63B 5.1.3.3 (restricted authenticator)

023. No enabled policy targets the 'Register security information' user action.

MEDIUM Conditional Access · Control checked: Security information registration is protected · Confirmed from configuration

What we found: No enabled policy targets the 'Register security information' user action.

Why it matters: Attackers who obtain a password before first MFA registration can enrol their own device.

Related standards: NIST SP 800-63B 6.1.2 Binding

024. No enabled policy configures sign-in frequency for admins.

MEDIUM Conditional Access · Control checked: Sign-in frequency is enforced for administrators · Confirmed from configuration

What we found: No enabled policy configures sign-in frequency for admins.

Why it matters: Long-lived admin sessions extend the window for token replay.

Related standards: NIST SP 800-63B 7.2 Reauthentication · NIST SP 800-53 AC-12

SAMPLE

025. Microsoft Authenticator additional context is not enabled: displayAppInformationRequiredState...

MEDIUM Identity Security · Control checked: Microsoft Authenticator shows application and location context · Confirmed from configuration

What we found: Microsoft Authenticator additional context is not enabled: displayAppInformationRequiredState, displayLocationInformationRequiredState.

Why it matters: Users approve fraudulent pushes when they cannot see context.

Affected (1): Microsoft Authenticator

Related standards: CIS M365 Foundations v4 5.2.3.1

026. 0 privileged account(s) have not signed in for more than 60 days; 1 have no recorded sign-in (may be break-glass or never used)

MEDIUM Privileged Access · Control checked: Stale administrator accounts (no sign-in for 60+ days) · Confirmed from configuration

What we found: 0 privileged account(s) have not signed in for more than 60 days; 1 have no recorded sign-in (may be break-glass or never used)

Why it matters: Unmonitored privileged accounts.

Affected (1): admin@contoso.example

Related standards: NIST SP 800-53 AC-2(3) · CIS M365 Foundations v4 1.1.x

027. 0 enabled account(s) have not signed in for more than 90 days; 1 enabled account(s) older than 90 days have no recorded sign-in.

MEDIUM User Account Security · Control checked: Dormant enabled accounts · Confirmed from configuration

What we found: 0 enabled account(s) have not signed in for more than 90 days; 1 enabled account(s) older than 90 days have no recorded sign-in.

Why it matters: Dormant accounts are targeted by password spray and are not watched by an owner.

Affected (1): admin@contoso.example

Related standards: NIST SP 800-53 AC-2(3) · NIST SP 800-171 3.1.1 · CMMC L2 AC.L2-3.1.1 · CIS M365 Foundations v4 1.1.x

028. No enabled policy configures persistent browser session = never for admins.

MEDIUM Conditional Access · Control checked: Persistent browser sessions are disabled for administrators · Confirmed from configuration

What we found: No enabled policy configures persistent browser session = never for admins.

Why it matters: Browser cookie theft yields a long-lived admin session.

Related standards: CIS M365 Foundations v4 5.2.2.x (session controls) · NIST SP 800-53 AC-12

029. No custom banned password list is configured.

MEDIUM Identity Security · Control checked: Banned password protection (custom list and on-premises enforcement) · Indicated by configuration

What we found: No custom banned password list is configured.

Why it matters: Weak/company-themed passwords are the first guesses in password spray.

Affected (1): Password Rule Settings

Related standards: NIST SP 800-63B 5.1.1.2 (blocklist) · CIS M365 Foundations v4 5.2.3.x

030. External sharing is enabled without any domain allow/block list (sharingDomainRestrictionMode=none)

MEDIUM SharePoint and OneDrive · Control checked: SharePoint external sharing is not restricted by domain allow/block list · Confirmed from configuration

What we found: External sharing is enabled without any domain allow/block list (sharingDomainRestrictionMode=none)

Why it matters: Without domain restrictions users can share with personal or attacker-controlled domains.

Related standards: CIS M365 Foundations v4.0 7.2.6 · NIST SP 800-53 r5 AC-21 · NIST CSF 2.0 PR.DS-01

031. External users (guests) are allowed to reshare content they do not own.

MEDIUM SharePoint and OneDrive · Control checked: External users can reshare SharePoint/OneDrive content they do not own · Confirmed from configuration

What we found: External users (guests) are allowed to reshare content they do not own.

Why it matters: Loss of control over who ultimately holds access to shared content.

Related standards: CIS M365 Foundations v4.0 7.2.5 · NIST SP 800-53 r5 AC-21 · NIST CSF 2.0 PR.DS-01

032. Sharing invitations can be accepted by any account (invited and accepting user need not match)

MEDIUM SharePoint and OneDrive · Control checked: Sharing invitations can be accepted by an account other than the invited one · Confirmed from configuration

What we found: Sharing invitations can be accepted by any account (invited and accepting user need not match)

Why it matters: Invitation forwarding or interception results in access by a different identity than the one the owner approved.

Related standards: NIST SP 800-53 r5 AC-2, IA-2 · NIST CSF 2.0 PR.AA-01

SAMPLE

033. DMARC subdomain policy not enforced on: contoso.example.

LOW Email Domain Protection (SPF, DKIM, DMARC) · Control checked: DMARC subdomain policy enforced (sp) · Confirmed from configuration

What we found: DMARC subdomain policy not enforced on: contoso.example.

Why it matters: Arbitrary subdomains of the organisation can be spoofed with no DMARC enforcement.

Affected (1): contoso.example

Related standards: CIS Microsoft 365 Foundations Benchmark v4.0 2.1.10 · NIST SP 800-53 Rev. 5 SC-20

034. DMARC aggregate reporting (rua) not configured on: contoso.example.

LOW Email Domain Protection (SPF, DKIM, DMARC) · Control checked: DMARC aggregate reporting configured (rua) · Confirmed from configuration

What we found: DMARC aggregate reporting (rua) not configured on: contoso.example.

Why it matters: No visibility into spoofing attempts or authentication failures of legitimate mail.

Affected (1): contoso.example

Related standards: CIS Microsoft 365 Foundations Benchmark v4.0 2.1.10 · NIST SP 800-53 Rev. 5 SI-4, AU-6 · NIST CSF 2.0 DE.CM-01

035. Email-verified users can self-join the organisation (viral tenant join)

LOW External Identities · Control checked: Email-verified users cannot self-join the tenant · Confirmed from configuration

What we found: Email-verified users can self-join the organisation (viral tenant join)

Why it matters: Unmanaged self-service accounts appear in the directory.

Affected (1): authorizationPolicy

Related standards: NIST SP 800-53 AC-2

036. Audit retention is limited to 180 days (unified audit log) and 30 days (Entra audit/sign-in logs); incidents discovered later...

LOW Security Monitoring and Audit Logging · Control checked: Audit log retention window · Confirmed from configuration

What we found: Audit retention is limited to 180 days (unified audit log) and 30 days (Entra audit/sign-in logs); incidents discovered later than that cannot be reconstructed.

Why it matters: Investigations of older intrusions have no evidence; regulatory retention requirements may be unmet.

Affected (1): Audit log retention

Related standards: NIST SP 800-53 Rev. 5 AU-11, AU-4 · NIST CSF 2.0 PR.PS-04, DE.CM-01 · CMMC 2.0 Level 2 AU.L2-3.3.1

037. MTA-STS (enforce) and/or TLS-RPT not published on: contoso.example.

LOW Email Domain Protection (SPF, DKIM, DMARC) · Control checked: MTA-STS (enforce) and TLS-RPT published · Confirmed from configuration

What we found: MTA-STS (enforce) and/or TLS-RPT not published on: contoso.example.

Why it matters: Inbound mail can be intercepted or downgraded to cleartext by an on-path attacker or a rogue MX record; TLS failures go unreported.

Affected (1): contoso.example

Related standards: NIST SP 800-53 Rev. 5 SC-8 · NIST CSF 2.0 PR.DS-02 · CMMC 2.0 Level 2 SC.L2-3.13.8

038. Idle session sign-out for unmanaged devices is disabled.

LOW SharePoint and OneDrive · Control checked: Idle session sign-out for SharePoint/OneDrive is disabled · Confirmed from configuration

What we found: Idle session sign-out for unmanaged devices is disabled.

Why it matters: Abandoned browser sessions on shared or public devices remain usable.

Related standards: CIS M365 Foundations v4.0 1.3.x (idle session timeout) · NIST SP 800-53 r5 AC-11, AC-12 · NIST SP 800-171 r2 3.1.10, 3.1.11 · NIST CSF 2.0 PR.AA-03

039. Microsoft Secure Score is 30.0% (30.0/100.0), below the 40% threshold.

LOW Threat Detection (Microsoft Defender) · Control checked: Microsoft Secure Score level · Confirmed from configuration

What we found: Microsoft Secure Score is 30.0% (30.0/100.0), below the 40% threshold.

Why it matters: Low scores correlate with missing MFA, legacy auth and weak mail protection.

Related standards: NIST CSF 2.0 ID.RA-01 · NIST SP 800-53 Rev. 5 CA-7

040. 1 enabled member account(s) have no licence (service, shared-mailbox or orphaned accounts.

LOW User Account Security · Control checked: Unlicensed enabled member accounts · Confirmed from configuration

What we found: 1 enabled member account(s) have no licence (service, shared-mailbox or orphaned accounts.

Why it matters: Shared-mailbox accounts with passwords and no MFA are a classic foothold.

Affected (1): admin@contoso.example

Related standards: NIST SP 800-53 AC-2 · CIS M365 Foundations v4 1.2.x

SAMPLE

ITEMS TO REVIEW TOGETHER

These items cannot be fully confirmed from configuration alone. We will go through them with you during the review meeting.

- Accounts matching service/test/admin naming patterns (manual review)
- Anonymous ('Anyone') link expiration and permissions require manual validation
- Default sharing link type and permission require manual validation
- Emergency access (break-glass) accounts documented and present
- Legacy per-user MFA state (manual review)
- Microsoft Authenticator registration campaign is enabled
- Preset security policies (Standard/Strict) enabled
- Report suspicious activity is enabled
- System-preferred multifactor authentication is enabled
- Unmanaged device access to SharePoint/OneDrive requires manual validation
- eDiscovery Manager role group membership requires manual validation

WHAT IS ALREADY IN GOOD SHAPE

Area	Controls passed
Applications and Consent	7
Security Monitoring and Audit Logging	7
Privileged Access	6
Threat Detection (Microsoft Defender)	6
Conditional Access	5
User Account Security	5
Email Domain Protection (SPF, DKIM, DMARC)	4
Identity Security	1

SAMPLE

SCOPE

Areas assessed: Applications and Consent, Conditional Access, Email Domain Protection (SPF, DKIM, DMARC), External Identities, Identity Security, Privileged Access, Security Monitoring and Audit Logging, SharePoint and OneDrive, Threat Detection (Microsoft Defender), User Account Security

Not available with your current Microsoft 365 licences:

- Insider Risk Management not configured
- Microsoft Defender for Endpoint connector requires manual validation
- Microsoft Defender for Endpoint licensed
- Privileged roles use PIM eligibility rather than permanent assignment
- Recent risk detections / sign-in anomalies (last 30 days)
- Safe Documents disabled or allows opening before scan
- Sensitivity labels not defined or not published
- Sign-in risk policy responds to high and medium risk sign-ins
- User risk policy requires password change for high-risk users
- Users with unresolved risk (Identity Protection)

Not assessed with the access granted (number of controls per area; we will review these with you):

Area	Controls
Applications and Consent	5
Data Protection and Compliance	4
Device Management	10
Exchange Online (Email)	38
External Identities	4

Identity Security	6
Microsoft Teams	13
Privileged Access	1
Security Monitoring and Audit Logging	1
SharePoint and OneDrive	2
User Account Security	1

About this assessment

This is a point-in-time, read-only review of the configuration visible with the access granted. It is not a penetration test, does not establish regulatory compliance or certification, and the security score shown is Pro Link's own measure, distinct from Microsoft Secure Score. No settings were changed during the assessment.

NEXT STEP

Pro Link Systems will walk you through these results, explain the business risk of each item and answer your questions.

Each issue has a specific, tested correction. Pro Link can plan, quote and carry out the corrections in a follow-on engagement, prioritised by severity and with minimal disruption to your users.

After the review, you may remove Pro Link's read-only access, or keep it in place if you engage Pro Link for remediation and ongoing monitoring.

Your Pro Link Systems account team

SAMPLE