

MICROSOFT 365 SECURITY ASSESSMENT · EXECUTIVE REPORT

Microsoft 365 Tenant Assessment

Prepared for Contoso Group Ltd

ASSESSED
19 Oct 2026

PRIMARY DOMAIN
contoso.com

POSTURE SCORE
21 / 100 · Grade E

PREPARED BY
Demo Consulting

POSTURE SCORE



WEAK · GRADE E · GOAL 85

OPEN FINDINGS

139



SCORE · LAST 3 CHECKS



Down 17 since 22 Apr 2026 · goal 85, dashed

CRITICAL OR
HIGH SEVERITY

30

ESTIMATED HANDS-ON
TIME TO FIX

116.5 h

 CONTENTS

What is in this report

This assessment reviews the configuration of the Contoso Group Ltd Microsoft 365 tenant against 187 controls covering identity, privileged access, devices, collaboration, threat protection, licensing and governance. Every finding states what was observed, why it matters and what to do about it.

01 Executive summary

The score, what it means, and the five things that matter most.

02 Score over the period

How the score moved, and what was fixed, found and changed.

03 Security posture by domain

How each area of the tenant scores, its trend, and the biggest gap in each.

04 Remediation roadmap

Every open finding, sequenced into a 30-day, 3-month and 6-month plan.

05 Cyber Essentials readiness

How close the tenant is to the UK Cyber Essentials requirements.

06 Licensing and cost

What the tenant pays for, what is unused, and what could be recovered.

07 Appendix

Scope, method, data coverage and the full control catalogue.

How to read this report

The posture score

The share of the controls we could assess that the tenant passes, weighted by severity. A pass earns a control's full weight, a warning half, a failure nothing. Weights: Critical 10, High 6, Medium 3, Low 1.



Severity

-  **Critical** Could be used now to take over accounts or reach data. Fix first.
-  **High** A gap in a control most organisations treat as baseline. Close within a month.
-  **Medium** Weakens defence in depth. Schedule into planned change.
-  **Low** Hygiene and good practice. Fold into routine work.

Results

- Pass** The control is in place.
- Warning** Partly in place; earns half its weight.
- Fail** Not in place.
- Not assessed** We could not read the data, so it counts neither way — never as a pass.
- Unconfirmed** Only Microsoft Secure Score says it is not done, and we could not read the setting to confirm it; it counts neither way.

Effort and change risk

Effort is the work to make the change. Low fits a single change window; medium needs planning or testing; high is a small project, often with user communication.

Change risk is the chance the change disrupts users while it is made — not the risk of leaving the gap open.

01 EXECUTIVE SUMMARY

Where this tenant stands

The tenant is exposed on multiple fronts and needs remediation planned immediately.

21

out of 100

Weak · Grade E

Goal 85 · 64 to go
87% of the control catalogue evaluated

21 of 158

Controls passed

Fully in place today.

139

Findings to address

3 critical, 27 high.

116.5 h

Estimated effort

Hands-on time by hand: about 16 engineer days.

£32,218

Recoverable a year

Unused and duplicate licences.

What the score means

A score of 21 puts Contoso Group Ltd in the **Weak** band. Of the 158 controls we could assess, 21 pass, 26 pass with warnings and 111 fail. 2 further open items are advisory and do not change the score.

Fixing the 30 critical and high findings would lift the score to about 51 (Weak).

Open findings by severity

139 open

Critical

3

High

27

Medium

73

Low

36

Score by domain

Licensing & Cost

11

Collaboration & Sharing

13

Privileged Access

15

Data Protection

15

Device & Endpoint

20

Governance & Operations

22

Threat Protection

26

Identity & Authentication

31

Headlines

- 3 critical issues need attention before anything else — these are the gaps an attacker would use first.
- 27 high-severity gaps were identified across identity, access and data protection.
- An indicative £32,218 a year of licence spend appears to be unused and recoverable.

The five things that matter most

- 1

1 privileged account has no registered multi-factor authentication method.

NL-ACC-001 · Administrators without registered multi-factor authentication. A privileged account without MFA is a complete tenant takeover waiting for one phishing email.

Critical

Effort: low
- 2

1 user is flagged as high risk and unremediated, with 2 at risk in total.

NL-THR-002 · Unresolved risky users. Each unremediated risky user is an account Microsoft believes may already be compromised.

Critical

Effort: medium

- 3 **No Conditional Access policy blocks legacy authentication, so MFA can be bypassed by using a legacy protocol.** . Critical
Effort: medium
NL-IDN-003 · Blocking of legacy authentication. Legacy protocols cannot present a second factor.
-
- 4 **1 disabled account still has an admin role or external mail forwarding, and 7 leavers in all are not fully offboarded.** . High
Effort: low
NL-GOV-005 · Leavers not fully offboarded. Disabling a leaver is only the first step.
-
- 5 **1 domain has missing or permissive SPF: contoso.co.uk (no SPF record).** . High
Effort: low
NL-EML-001 · SPF record on every custom domain. Without a strict SPF record, anyone can send email that appears to come from the organisation, and receiving servers have no basis to reject it.

Quick wins

Low-effort changes that close meaningful gaps. Each can typically be done in a single change window.

 **Administrators without registered multi-factor authentication**
Register strong authentication for every privileged account today, then enforce it with Conditional Access.

 **Leavers not fully offboarded**
Finish offboarding each listed leaver: remove admin roles, stop external forwarding, convert the mailbox to shared if it must be kept, then remove the paid licences.

 **SPF record on every custom domain**
Publish one SPF TXT record per domain, including Microsoft 365, ending in -all (or ~all with an enforcing DMARC policy).

 **Mail forwarded outside the organisation**
Review each forwarding rule with the mailbox owner, remove any that are not approved, and block automatic external forwarding.

 **BitLocker, firewall and antivirus required on Windows**
Require BitLocker, firewall, antivirus and real-time protection in the Windows compliance policy, and assign it to all users or devices.

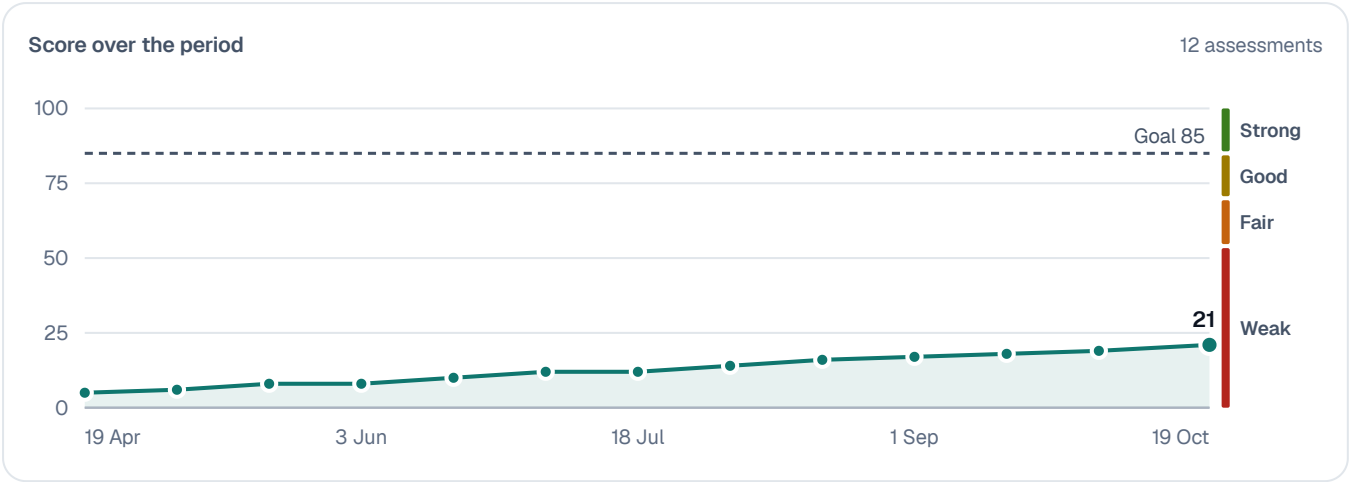
 **Sign-in to shared mailboxes**
Block sign-in for every shared mailbox account.

02 SCORE OVER THE PERIOD

Score over the last 6 months

Over the last 6 months, from 19 Apr 2026 to 19 Oct 2026, the score rose 16 points, from 5 to 21.

5 / 100 At the start As it stood on 19 Apr 2026.	21 / 100 Now 19 Oct 2026	+16 Change in score 16 points up over the last 6 months.
---	---	---



What changed

In that time: 14 findings fixed and confirmed, 3 improved, 23 changes made in the tenant, 4 new findings and 1 got worse, over 12 assessments.

14 Fixed and confirmed Re-read from the live tenant.	3 Improved Better, not yet fully passing.	23 Changes made Approved changes that ran in the tenant.	5 New or worse 4 new findings, 1 worse.
---	--	---	--

03 SECURITY POSTURE BY DOMAIN

Score by assessment domain

Each domain is scored on the controls that could be evaluated for this tenant. A control that could not be assessed is left out in both directions, so a narrow assessment never flatters a score.

Score by domain



How to read the chart

Each bar is one domain, scored from 0 on the left to 100 on the right. An even set of long bars is a balanced tenant; a short bar is where an attacker would look first. The tick marks the goal of 85.

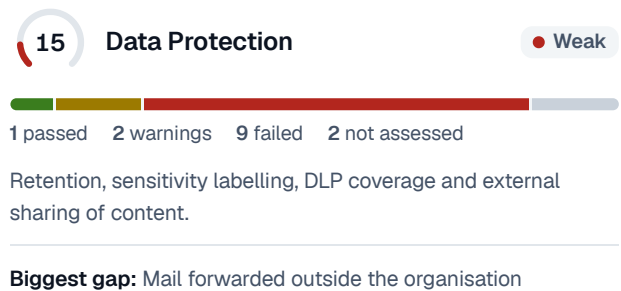
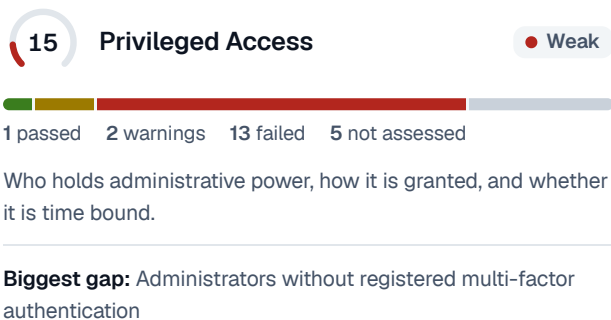
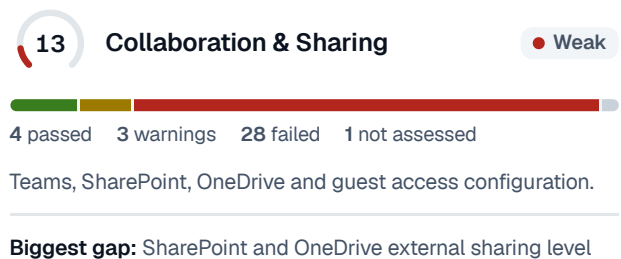
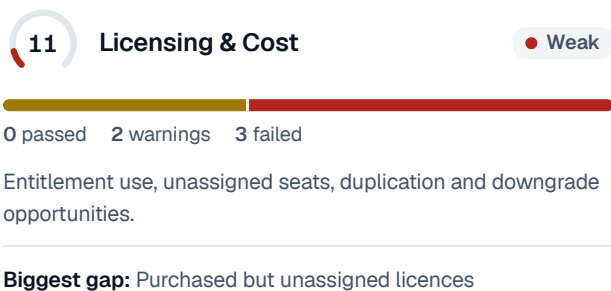
Weakest domain

Licensing & Cost · 11 / 100

Strongest domain

Identity & Authentication · 31 / 100

Domain by domain



20 Device & Endpoint

● Weak


1 passed 5 warnings 14 failed

Enrolment, compliance, update rings and endpoint protection posture.

Biggest gap: Unsupported operating systems in use

22 Governance & Operations

● Weak


2 passed 0 warnings 4 failed 1 not assessed

Lifecycle, ownership, documentation, audit retention and change control.

Biggest gap: Leavers not fully offboarded

26 Threat Protection

● Weak


6 passed 5 warnings 22 failed 9 not assessed

Defender coverage, alerting, risk detections and incident readiness.

Biggest gap: Unresolved risky users

31 Identity & Authentication

● Weak


6 passed 7 warnings 18 failed 5 not assessed

How accounts prove who they are: MFA coverage, passwordless adoption, legacy protocols.

Biggest gap: Blocking of legacy authentication

■ Passed ■ Warning ■ Failed ■ Not assessed

04 REMEDIATION ROADMAP

What to do, and in what order

Findings are sequenced by exposure first and effort second. The estimates are for a competent engineer familiar with the tenant and exclude change-approval time.

The plan at a glance

Today

30 days

3 months

6 months

Immediate

19 actions · ~15.5h · 0–30 days

Near term

84 actions · ~79h · 1–3 months

Ongoing

36 actions · ~22h · 3–6 months

Severity against effort

Critical	1	2	–
High	16	9	2
Medium	43	28	2
Low	29	6	1
	Low	Medium	High

Effort to fix →

⚡ Where to start

Each circle counts the open findings with that severity and effort; bigger is more. The dashed corner, top left, holds the severe findings that take little effort: **17 findings** here. Close these first; they give the biggest reduction in risk for the least work.

Work then moves right and down: severe items that need planning, then hygiene that can join routine work.

⚙️ How the phases are chosen

Immediate holds every critical finding and the quick high ones. **Near term** holds the remaining high and medium findings, which need planning, testing or user communication. **Ongoing** is hygiene, cost and lifecycle work for business as usual.

1

Immediate · 0–30 days

19 actions · ~15.5h

Critical exposure, or high-severity gaps that can be closed quickly with little disruption.

Action	Severity	Effort	Change risk
☐ Administrators without registered multi-factor authentication Register strong authentication for every privileged account today, then enforce it with Conditional Access.	Critical	Low	Low
☐ Unresolved risky users Triage every risky user: confirm compromise, reset credentials, revoke sessions, then dismiss or remediate the risk.	Critical	Medium	Low
☐ Blocking of legacy authentication Create a Conditional Access policy blocking legacy authentication clients for all users.	Critical	Medium	High

Sample report · demo data: Contoso Group Ltd is a made-up client, not a real tenant.

8

Action	Severity	Effort	Change risk
☐ Leavers not fully offboarded Finish offboarding each listed leaver: remove admin roles, stop external forwarding, convert the mailbox to shared if it must be kept, then remove the paid licences.	 High	Low	Low
☐ SPF record on every custom domain Publish one SPF TXT record per domain, including Microsoft 365, ending in -all (or ~all with an enforcing DMARC policy).	 High	Low	Medium
☐ Mail forwarded outside the organisation Review each forwarding rule with the mailbox owner, remove any that are not approved, and block automatic external forwarding.	 High	Low	Low
☐ BitLocker, firewall and antivirus required on Windows Require BitLocker, firewall, antivirus and real-time protection in the Windows compliance policy, and assign it to all users or devices.	 High	Low	Medium
☐ Sign-in to shared mailboxes Block sign-in for every shared mailbox account.	 High	Low	Low
☐ Disabled or dormant accounts holding privileged roles Remove privileged roles from disabled and dormant accounts, and add a quarterly access review.	 High	Low	Low
☐ Teams chat with personal (unmanaged) accounts Turn off communication with Teams users not managed by an organisation.	 High	Low	Low
☐ Personal Teams accounts starting conversations Stop unmanaged Teams accounts starting conversations with your people.	 High	Low	Low
☐ Accounts bypassing mailbox auditing Turn off audit bypass for every account listed.	 High	Low	Low
☐ Mail flow rules that skip spam filtering for a domain Disable or delete mail flow rules that set SCL -1 for sender domains; use connectors or the Tenant Allow/Block List instead.	 High	Low	Medium
☐ User consent to third-party applications Restrict user consent to verified publishers and low-impact permissions, and enable the admin consent workflow.	 High	Low	Medium
☐ Application registration by non-administrators Set "Users can register applications" to No, and delegate the Application Developer role where it is genuinely needed.	 High	Low	Low
☐ Emergency access (break-glass) accounts Create two cloud-only emergency access accounts, exclude them from Conditional Access, and monitor their use.	 High	Low	Low
☐ SharePoint and OneDrive external sharing level Move tenant-wide sharing to "New and existing guests", which turns off Anyone links on every site.	 High	Low	Medium
☐ Device code sign-in blocked Block the device code flow with Conditional Access, excluding only the accounts that genuinely need it.	 High	Low	Medium

Action	Severity	Effort	Change risk
☐ Automatic forwarding to other domains Turn automatic forwarding off in the outbound spam policy, with exceptions only for mailboxes that need it.	 High	Low	Medium

2 Near term · 1–3 months 84 actions · ~79h

Material gaps that need planning, testing or user communication before enforcement.

Action	Severity	Effort	Change risk
☐ Unsupported operating systems in use Update each listed device to a supported release, or replace it where the hardware cannot be upgraded.	 High	Medium	Medium
☐ Multi-factor authentication registration coverage Drive registration to 100% of enabled member accounts, then enforce it with Conditional Access.	 High	Medium	Medium
☐ Number of Global Administrators Reduce standing Global Administrators to two to four, and move the rest to least-privilege roles.	 High	Medium	Medium
☐ Applications holding high-privilege Graph permissions Review every high-privilege application grant, remove what is unused and scope the rest.	 High	Medium	Medium
☐ Risky apps with access to company data Review each high-risk app with its owner, and block the ones nobody recognises.	 High	Medium	Medium
☐ DMARC policy enforced Publish DMARC with reporting, monitor, then move to p=quarantine and p=reject.	 High	Medium	Medium
☐ Tenant-wide consent grants carrying high-risk scopes Review every tenant-wide grant with a high-risk scope and revoke the ones without a clear owner.	 High	Medium	Medium
☐ Teams chat and calls with other organisations Allow external access only to the domains of organisations you work with.	 High	Medium	Medium
☐ Device compliance policy coverage Create compliance policies for every platform in use, then require compliance in Conditional Access.	 High	Medium	Medium
☐ Phishing-resistant authentication for administrators Require the "Phishing-resistant MFA" authentication strength for all privileged roles.	 High	High	Medium
☐ Device compliance requirement in Conditional Access Require a compliant or hybrid-joined device for access to Microsoft 365 from desktop platforms.	 High	High	High
☐ Mailbox audit actions Add the missing audit actions to every user mailbox.	 Medium	Low	Low
☐ Comprehensive attachment filtering Add the CIS list of file types to the default anti-malware policy's common attachments filter.	 Medium	Low	Medium
☐ Purchased but unassigned licences Reduce seat counts at the next billing anniversary, or reassign the spare seats.	 Medium	Low	Low

Action	Severity	Effort	Change risk
☐ Windows LAPS for local administrator passwords Turn on Windows LAPS in Entra ID and deploy an Intune LAPS policy that backs passwords up to Entra ID.	 Medium	Low	Low
☐ Self-service password reset registration Enable SSPR for all users and require registration at next sign-in.	 Medium	Low	Low
☐ Licences assigned to disabled accounts Reclaim licences from disabled accounts, converting mailboxes to shared where the data must stay reachable.	 Medium	Low	Medium
☐ Third-party cloud storage in Teams Turn off every third-party storage provider the business has not approved.	 Medium	Low	Low
☐ Outbound spam limits Set the outbound limits to 500 external, 1,000 internal and 1,000 daily, and restrict the sender when they are reached.	 Medium	Low	Medium
☐ Preset security policies for everyone Turn on the standard and strict preset security policies and apply standard (at least) to all recipients.	 Medium	Low	Medium
☐ Retention policies keep email and files Create a retention policy that keeps Exchange email, SharePoint sites and OneDrive accounts for everyone, for as long as the business must keep its records.	 Medium	Low	Low
☐ Administrators told about outbound spam Turn on the copy of suspicious outbound messages and the notification of blocked senders, both to a monitored mailbox.	 Medium	Low	Low
☐ Conditional Access policies left in report-only or disabled state Review each non-enforcing policy: promote it to On, or delete it.	 Medium	Low	Low
☐ Apps users consented to that read mail or files Review the apps users have consented to, block what is not needed, and send future requests to an administrator.	 Medium	Low	Low
☐ Devices with no compliance policy counted as compliant Mark devices with no compliance policy assigned as not compliant.	 Medium	Low	Medium
☐ Teams contact with trial-only organisations Block external access with trial-only tenants.	 Medium	Low	Low
☐ Anonymous people joining Teams meetings Stop anonymous people joining meetings; invite guests or partners by their accounts instead.	 Medium	Low	Medium
☐ Who bypasses the Teams meeting lobby Let only people in the organisation bypass the lobby.	 Medium	Low	Low
☐ Alert policies for compromised mail accounts Switch the built-in alert policies back on and make sure their emails reach someone who acts on them.	 Medium	Low	Low
☐ Exchange Online hardening Work through the Exchange Online improvement actions in Secure Score.	 Medium	Low	Low

Action	Severity	Effort	Change risk
☐ External access defaults for Teams and B2B Keep B2B direct connect blocked by default and allow it only for named partner organisations; trust inbound MFA from partners you work with.	 Medium	Low	Medium
☐ Spam filtering skipped for listed senders Empty the IP allow list and turn off the safe list; set up the senders that need it with SPF or a connector.	 Medium	Low	Medium
☐ Domains allowed to skip spam filtering Remove every allowed domain from the inbound anti-spam policies; use the Tenant Allow/Block List for genuine false positives.	 Medium	Low	Medium
☐ Resharing of content by external users Disable resharing by external users.	 Medium	Low	Low
☐ Restrictions on who can invite guests Restrict invitations to members assigned the Guest Inviter role, or to administrators.	 Medium	Low	Low
☐ Restriction of OneDrive sync to managed devices Restrict the sync client to Entra-joined or hybrid-joined devices.	 Medium	Low	Medium
☐ Security and compliance notification contacts Set the technical and security notification addresses to monitored distribution lists, not individuals.	 Medium	Low	Low
☐ Sign-in details shown in Microsoft Authenticator Turn on "Show application name" and "Show geographic location" for Microsoft Authenticator.	 Medium	Low	Low
☐ Security info registration protected Require MFA, or a trusted location, to register security info.	 Medium	Low	Low
☐ Admin consent workflow Turn on admin consent requests, with administrators as reviewers.	 Medium	Low	Low
☐ Group and team owners consenting to apps Do not allow group owner consent; send owners through the admin consent workflow instead.	 Medium	Low	Low
☐ Guests accept invitations with the invited account Require guests to accept with the account the invitation was sent to.	 Medium	Low	Low
☐ Legacy sign-in to SharePoint and OneDrive Block apps that do not use modern authentication.	 Medium	Low	Medium
☐ External sender tag in Outlook Turn on the External tag in Outlook.	 Medium	Low	Low
☐ Calendar and contact sharing with other organisations Share only free/busy times with other organisations, and no contacts.	 Medium	Low	Low
☐ Idle session timeout for Microsoft 365 on the web Turn on the idle session timeout at three hours or less, and a Conditional Access policy using app-enforced restrictions.	 Medium	Low	Low
☐ Who can join devices to Entra ID Allow only a selected group, such as IT, to join devices to Entra ID; use Autopilot for everyone else.	 Medium	Low	Medium

Action	Severity	Effort	Change risk
☐ Global Administrators made local administrators on joined devices Turn off "Global administrator role is added as local administrator on the device during Microsoft Entra join"; use Windows LAPS or a dedicated device administrator role instead.	 Medium	Low	Medium
☐ Windows LAPS switched on in Entra ID Turn on "Enable Microsoft Entra Local Administrator Password Solution (LAPS)", then deploy a LAPS policy from Intune.	 Medium	Low	Low
☐ Administrator sign-in frequency and browser sessions Create a Conditional Access policy for administrator roles with a sign-in frequency of four hours or less and persistent browser session set to never.	 Medium	Low	Low
☐ Managed device required to register security info Require a compliant or hybrid-joined device to register security information.	 Medium	Low	Medium
☐ Intune enrolment signs in every time Create a Conditional Access policy for Microsoft Intune Enrollment requiring MFA with sign-in frequency every time.	 Medium	Low	Low
☐ Administrators told about internal senders of malware Turn on "Notify an admin about undelivered messages from internal senders" in the default anti-malware policy, with a monitored address.	 Medium	Low	Low
☐ Exchange Online: basic authentication for SMTP AUTH is being retired Read MC1101245 and act by 2026-12-03.	 Medium	Low	Low
☐ Device end of life and replacement planning Replace end-of-life hardware, update operating systems that are merely out of date, and budget now for devices reaching end of life in the next twelve months.	 Medium	Medium	Low
☐ Migrate to Microsoft Authenticator Migrate to Microsoft Authenticator	 Medium	Medium	Medium
☐ Sensitivity labels on Teams, groups and sites Enable sensitivity labels for groups and sites, and label every team, starting with those holding confidential material.	 Medium	Medium	Low
☐ Device compliance rate Work the non-compliant list down and fix the policies that no device can satisfy.	 Medium	Medium	Low
☐ Unmanaged devices in the directory Enrol the devices into Intune, or block unmanaged devices with Conditional Access.	 Medium	Medium	Medium
☐ Guest access exposure Remove dormant guests and put a recurring access review in place.	 Medium	Medium	Medium
☐ Public groups and Teams open to every employee Make groups Private unless they are meant for everyone, starting with the largest and most sensitive.	 Medium	Medium	Low
☐ Dormant enabled accounts Disable dormant accounts, reclaim their licences, and connect the joiner-mover-leaver process to the directory.	 Medium	Medium	Medium
☐ Ageing unresolved security alerts Establish a triage rota with a target time to first response, and tune the noisy detections.	 Medium	Medium	Low

Action	Severity	Effort	Change risk
☐ Administrator accounts with application licences Give administrators a separate, unlicensed (or Entra ID P1/P2 only) account for admin work, and remove app licences from their admin accounts.	 Medium	Medium	Medium
☐ Groups and Teams without owners Assign at least two owners to every group, and enable the ownerless group policy.	 Medium	Medium	Low
☐ Personal devices enrolling in Intune Block personally owned devices in the default enrolment restriction; give personal phones access through app protection policies instead.	 Medium	Medium	Medium
☐ Expired or expiring application credentials Rotate credentials before expiry and delete the ones already expired.	 Medium	Medium	Medium
☐ Which Teams apps people can install Allow only approved third-party and custom apps; keep Microsoft apps allowed.	 Medium	Medium	Medium
☐ Text message, voice call and email codes for sign-in Turn off text message, voice call and email codes once everyone has Microsoft Authenticator or a stronger method.	 Medium	Medium	Medium
☐ External sharing limited to approved domains Limit external sharing to the domains of approved partners.	 Medium	Medium	Medium
☐ DLP policies switched on Enforce a DLP policy for the sensitive data the business holds, after reviewing its matches in test mode.	 Medium	Medium	Medium
☐ DLP across email, files, Teams and devices Apply an enforced DLP policy to Exchange, SharePoint, OneDrive, Teams and devices, for all accounts and sites.	 Medium	Medium	Medium
☐ DLP rules block sharing Set each enforced DLP rule to block sharing with everyone, with an override for business need where appropriate.	 Medium	Medium	Medium
☐ Sensitivity labels published Publish a small set of sensitivity labels (for example Public, Internal, Confidential) to everyone.	 Medium	Medium	Low
☐ Sensitivity labels Create a small set of sensitivity labels (for example Public, Internal, Confidential) and publish them to all users.	 Medium	Medium	Low
☐ Data loss prevention policies Start with Microsoft's DLP templates for the data you hold (for example UK financial or personal data), in test mode, then turn them on.	 Medium	Medium	Medium
☐ Microsoft Secure Score against peer average Work the highest-value Secure Score improvement actions, starting with identity.	 Medium	Medium	Low
☐ SMTP AUTH turned off Turn SMTP AUTH off for the organisation and give the scanner or app that needs it its own exception.	 Medium	Medium	Medium
☐ People made local administrator of the devices they join Set "Registering user is added as local administrator on the device during Microsoft Entra join" to Selected or None.	 Medium	Medium	Medium

Action	Severity	Effort	Change risk
☐ Password protection for on-premises Active Directory Install the Entra password protection agents and set the on-premises mode to Enforced.	 Medium	Medium	Medium
☐ Client secrets on applications Turn on the app management policy, block password addition, or at least restrict password lifetime to 180 days.	 Medium	Medium	Medium
☐ Direct Send rejected Move devices and apps that send by Direct Send to an authenticated connector, then reject Direct Send.	 Medium	Medium	Medium
☐ Privileged roles held by synchronised on-premises accounts Move privileged roles onto cloud-only accounts that have no on-premises counterpart.	 Medium	High	Medium
☐ Managed device required for every sign-in Require a compliant or hybrid-joined device for all users on all resources.	 Medium	High	High

3 Ongoing · 3–6 months

Hygiene, cost optimisation and lifecycle work that should move into business as usual.

36

actions · ~22h

Action	Severity	Effort	Change risk
☐ Stale device records Clean up device records that have not checked in, and automate it going forward.	 Low	Low	Medium
☐ Accounts without a usage location Set a usage location on every account, ideally from the HR source of truth.	 Low	Low	Low
☐ Stale groups and Teams Enable the Microsoft 365 group expiration policy with owner renewal.	 Low	Low	Medium
☐ POP and IMAP for new mailboxes Turn POP and IMAP off in every mailbox plan, and on existing mailboxes that do not use them.	 Low	Low	Low
☐ Unused apps still holding permissions Block unused apps, then delete them once nobody has asked for them back.	 Low	Low	Low
☐ Office Store and self-service trials Turn off access to the Office Store and self-service trials for users.	 Low	Low	Low
☐ Email into Teams channels Turn off email into channels.	 Low	Low	Low
☐ Anonymous people in Teams meeting chat Turn meeting chat on for everyone except anonymous people.	 Low	Low	Low
☐ Who can present in Teams meetings Make "Only organisers and co-organisers" the default for who can present.	 Low	Low	Low
☐ Meeting chat with untrusted organisations Turn off chat in meetings hosted by untrusted organisations.	 Low	Low	Low
☐ Teams meeting recording by default Turn cloud recording off in the Global meeting policy and give it, through a custom policy, to those who need it.	 Low	Low	Medium

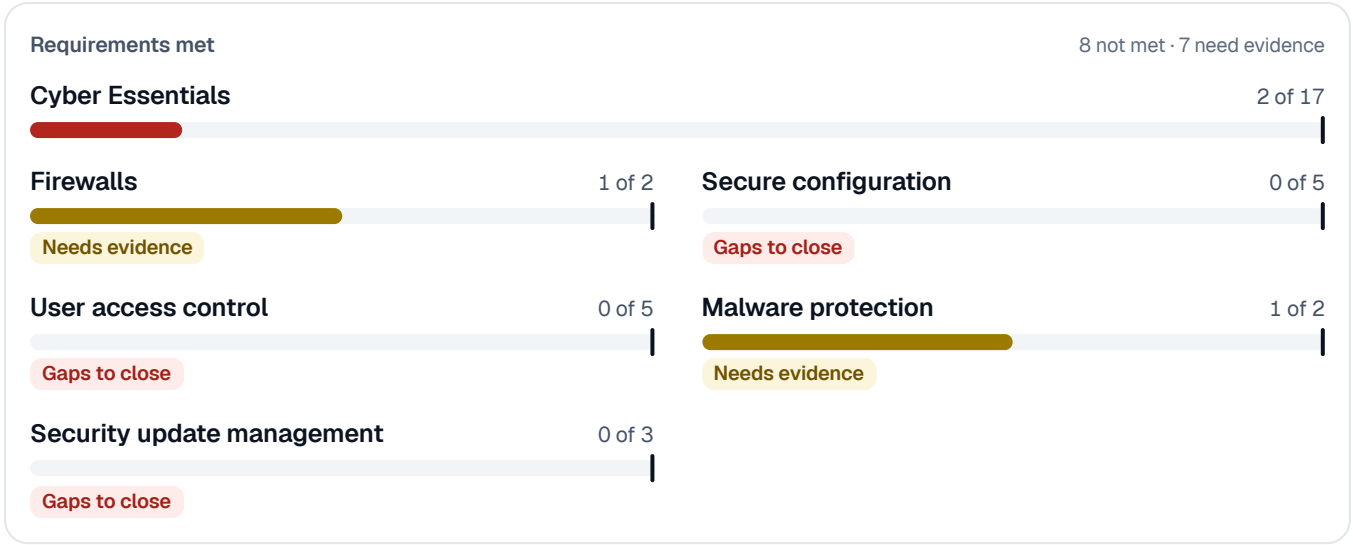
Action	Severity	Effort	Change risk
☐ Overlapping subscriptions Cancel standalone add-ons that are already covered by a suite the organisation holds.	 Low	Low	Medium
☐ People installing Outlook add-ins Remove the add-in roles from every role assignment policy, and deploy needed add-ins centrally.	 Low	Low	Low
☐ Third-party storage in Outlook on the web Turn off additional storage providers in every Outlook on the web policy.	 Low	Low	Low
☐ Guest access to the directory Set guest user access to "restricted to properties and memberships of their own directory objects".	 Low	Low	Low
☐ Self-service sign-up to the tenant Turn off email-verified joining and self-service subscription sign-up, and buy or assign licences centrally.	 Low	Low	Low
☐ Named locations for Conditional Access Define the organisation's egress IP ranges as trusted named locations.	 Low	Low	Low
☐ Third-party storage in Microsoft 365 on the web Turn off "Let users open files stored in third-party storage services in Microsoft 365 on the web".	 Low	Low	Low
☐ Dynamic group of guest accounts Create a dynamic security group with the rule (user.userType -eq "Guest").	 Low	Low	Low
☐ Users creating security groups Set "Users can create security groups in Azure portals, API or PowerShell" to No.	 Low	Low	Low
☐ Device limit per user Set "Maximum number of devices per user" to 20 or fewer.	 Low	Low	Low
☐ People reading BitLocker keys of their own devices Set "Restrict users from recovering the BitLocker key(s) for their owned devices" to Yes.	 Low	Low	Low
☐ Custom banned password list Turn on "Enforce custom list" and add the organisation's own words.	 Low	Low	Low
☐ Authentication methods migration complete Finish the migration and set Manage migration to "Migration Complete".	 Low	Low	Medium
☐ Application certificate lifetime Restrict the maximum certificate lifetime to 365 days.	 Low	Low	Low
☐ Calendar sharing with people outside the organisation Turn off "Let your users share their calendars with people outside of your organization".	 Low	Low	Low
☐ Shared Bookings pages Allow only selected users to create shared Bookings pages.	 Low	Low	Low
☐ MailTips Turn on all MailTips, the external recipients tip and group metrics.	 Low	Low	Low
☐ Microsoft Teams: retention setting for meeting recaps Read MC1098834 and act by 2026-11-08.	 Low	Low	Low

Action	Severity	Effort	Change risk
☐ Licences assigned to dormant accounts Review dormant licensed accounts with the business, then reclaim or downgrade the licence.	 Low	Medium	Medium
☐ DMARC at reject, with report addresses Move each domain to p=reject once reports show only genuine senders pass, and add rua and ruf addresses.	 Low	Medium	Medium
☐ DLP rules tell people why Turn on user notifications and policy tips in each enforced DLP rule.	 Low	Medium	Medium
☐ Retention labels published Create retention labels for the records the business must keep, and publish them to the places those records live.	 Low	Medium	Low
☐ MTA-STS for inbound mail Publish an MTA-STS policy for each receiving domain, starting in testing mode.	 Low	Medium	Low
☐ Guest invitations limited to allowed domains Allow invitations only to the domains of approved partners.	 Low	Medium	Medium
☐ Phishing-resistant MFA for everyone Roll out passkeys or Windows Hello for Business, then require the "Phishing-resistant MFA" authentication strength for everyone.	 Low	High	Medium

05 CYBER ESSENTIALS READINESS

Gaps to close: 2 of 17 requirements met

Cyber Essentials is the UK government-backed baseline scheme. Where Microsoft 365 can show a control, this assessment is the evidence; firewalls, anti-malware and patching timelines are confirmed by the consultant.



This is a readiness view
It shows how close the tenant is to the requirements, not a certification. Certification is awarded by an IASME certification body after its own assessment. A check that could not run is treated as needing evidence, never as met.

To close before an assessment

Control	Requirement	Why
Secure configuration	Devices meet a defined secure configuration, enforced and reported by device management.	Failing: Device compliance policy coverage; Device compliance rate; Unmanaged devices in the directory
Secure configuration	Company data is only reachable from devices that meet that configuration.	Failing: Device compliance requirement in Conditional Access
Secure configuration	Cloud services have insecure defaults turned off: legacy authentication, unmanaged app consent and app registration by any user.	Failing: Blocking of legacy authentication; User consent to third-party applications; Application registration by non-administrators
User access control	Multi-factor authentication protects every account on cloud services.	Failing: Multi-factor authentication registration coverage
User access control	Every administrator uses multi-factor authentication, preferably phishing-resistant.	Failing: Administrators without registered multi-factor authentication; Phishing-resistant authentication for administrators
User access control	Administrative rights are held by as few people as possible, using separate cloud-only admin accounts.	Failing: Number of Global Administrators; Privileged roles held by synchronised on-premises accounts
User access control	Accounts no longer needed, including privileged ones, are removed or disabled promptly.	Failing: Disabled or dormant accounts holding privileged roles; Dormant enabled accounts; Leavers not fully offboarded

Control	Requirement	Why
Security update management	Every device runs an operating system that still receives security updates.	Failing: Unsupported operating systems in use

Evidence still needed

- ☐ **Firewalls:** The software firewall is on for every laptop and other device used outside the office.
- ☐ **Secure configuration:** Devices have unnecessary software and accounts removed, default passwords changed, and auto-run of downloaded content disabled.
- ☐ **Secure configuration:** Every device requires a PIN, password or biometric to unlock, with lockout or throttling after failed attempts.
- ☐ **User access control:** Joiners, movers and leavers follow an approval process, and admin accounts are used only for administration.
- ☐ **Malware protection:** Web protection blocks known malicious sites (e.g. Defender SmartScreen or network protection).
- ☐ **Security update management:** Automatic updates are on, and critical or high-risk security updates are applied within 14 days (e.g. Intune update rings with deadlines).
- ☐ **Security update management:** All installed software is licensed and still supported by its vendor; unsupported software has been removed.

06 LICENSING AND COST

What the tenant is paying for

Seat counts are taken from the tenant's own subscription data. Costs are indicative UK list prices, excluding VAT, used to size the opportunity — substitute the contracted rates before treating any figure as a quote.

£

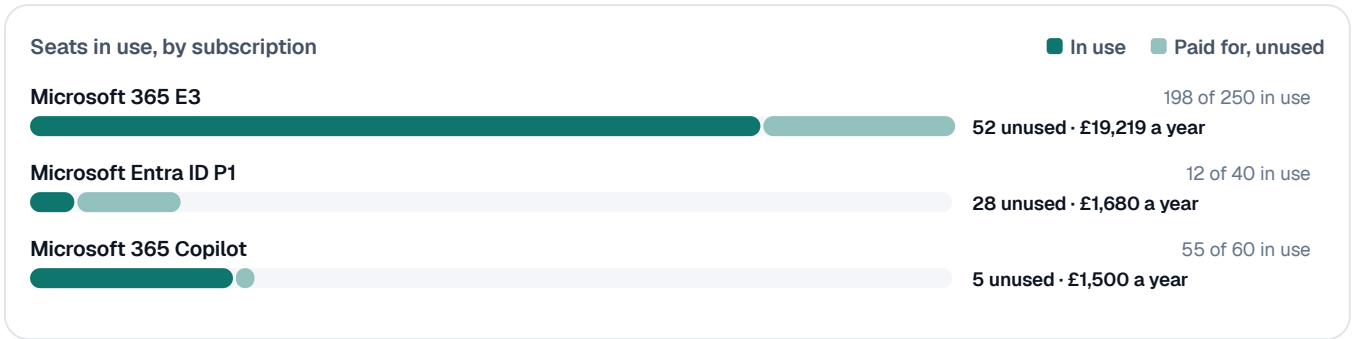
£32,218

a year

Indicative recoverable spend

From unassigned seats, licences on disabled accounts and overlapping subscriptions. The licensing findings give the breakdown.

3 Paid subscriptions	265 of 350 Seats in use	85 Seats unused 24% of what is paid for.
--	---	---



Subscription	Purchased	Assigned	Unassigned	Unassigned cost a year
Microsoft 365 E3	250	198	52	£19,219
Microsoft Entra ID P1	40	12	28	£1,680
Microsoft 365 Copilot	60	55	5	£1,500

Prices are indicative UK list in pounds sterling, per seat per month, annual commitment, excluding VAT. They are not a quotation.

07 APPENDIX

Scope, method and coverage

Tenant profile

Organisation	Primary domain	Verified domains
Contoso Group Ltd	contoso.com	3
Country	Member accounts	Enabled members
GB	207	197
Guest accounts	Groups and Teams	Devices
38	67	180
Conditional Access policies	Directory synchronisation	Microsoft Secure Score
2	Hybrid (synchronised)	274 / 612 (45%)

Method



What we read

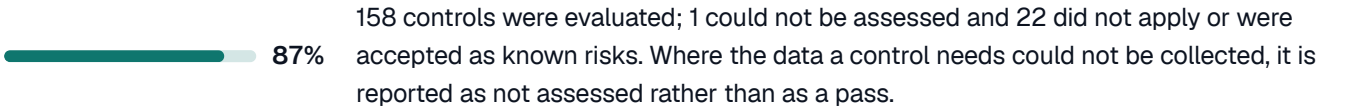
Configuration, read from Microsoft Graph by an application a tenant administrator granted read-only consent. Each control is evaluated against that configuration.



What we never read

No message content, file content or chat content, and no personal data beyond directory attributes. No changes were made to the tenant.

Data coverage



These data sources were incomplete. Findings that depend on them are marked as not assessed.

Data source	Status	Reason
Privileged role assignments	Partial	PIM eligible assignments could not be read (Microsoft Entra ID P2 required).
Defender for Endpoint security recommendations	Skipped	Defender for Endpoint security recommendations needs Microsoft Defender for Endpoint Plan 2 or Defender for Business, which this tenant does not have (it has Microsoft 365 E3, Microsoft Entra ID P1, Microsoft 365 Copilot). It comes with Microsoft 365 E5, E5 Security, Business Premium (Defender for Business), or Defender for Endpoint Plan 2.

Control catalogue

Reference	Control	Result
NL-ACC-001	Administrators without registered multi-factor authentication	Fail
NL-IDN-003	Blocking of legacy authentication	Fail
NL-THR-002	Unresolved risky users	Fail
NL-GOV-005	Leavers not fully offboarded	Fail
NL-ACC-002	Number of Global Administrators	Fail

Reference	Control	Result
NL-ACC-006	Disabled or dormant accounts holding privileged roles	Fail
NL-ACC-007	Applications holding high-privilege Graph permissions	Fail
NL-COL-001	SharePoint and OneDrive external sharing level	Fail
NL-DEV-008	Unsupported operating systems in use	Fail
NL-EML-002	DMARC policy enforced	Fail
NL-IDN-001	Multi-factor authentication registration coverage	Fail
NL-IDN-006	Phishing-resistant authentication for administrators	Fail
NL-IDN-010	Application registration by non-administrators	Fail
NL-TMS-103	Teams chat and calls with other organisations	Fail
NL-ACC-009	Tenant-wide consent grants carrying high-risk scopes	Fail
NL-ACC-011	Risky apps with access to company data	Fail
NL-DEV-003	Device compliance requirement in Conditional Access	Fail
NL-EML-001	SPF record on every custom domain	Fail
NL-EML-005	Mail forwarded outside the organisation	Fail
NL-EML-011	Automatic forwarding to other domains	Fail
NL-EXO-101	Sign-in to shared mailboxes	Fail
NL-IDN-009	User consent to third-party applications	Fail
NL-IDN-017	Device code sign-in blocked	Fail
NL-TMS-104	Teams chat with personal (unmanaged) accounts	Fail
NL-TMS-105	Personal Teams accounts starting conversations	Fail
NL-EXO-118	Accounts bypassing mailbox auditing	Fail
NL-EXO-119	Mail flow rules that skip spam filtering for a domain	Fail
NL-ACC-008	Expired or expiring application credentials	Fail
NL-COL-003	Groups and Teams without owners	Fail
NL-COL-004	Guest access exposure	Fail
NL-COL-015	Legacy sign-in to SharePoint and OneDrive	Fail
NL-DEV-006	Device end of life and replacement planning	Fail
NL-DEV-010	Windows LAPS for local administrator passwords	Fail
NL-EML-007	SMTP AUTH turned off	Fail
NL-GOV-001	Dormant enabled accounts	Fail
NL-IDN-015	Text message, voice call and email codes for sign-in	Fail
NL-IDN-018	Security info registration protected	Fail
NL-IDN-116	Administrator sign-in frequency and browser sessions	Fail
NL-IDN-120	Managed device required for every sign-in	Fail
NL-INT-101	Devices with no compliance policy counted as compliant	Fail
NL-LIC-001	Purchased but unassigned licences	Fail

Reference	Control	Result
NL-LIC-002	Licences assigned to disabled accounts	Fail
NL-PVW-101	DLP policies switched on	Fail
NL-PVW-106	Sensitivity labels published	Fail
NL-THR-001	Microsoft Secure Score against peer average	Fail
NL-THR-003	Ageing unresolved security alerts	Fail
NL-TMS-106	Teams contact with trial-only organisations	Fail
NL-ACC-003	Privileged roles held by synchronised on-premises accounts	Fail
NL-ACC-012	Apps users consented to that read mail or files	Fail
NL-COL-002	Resharing of content by external users	Fail
NL-COL-005	Restrictions on who can invite guests	Fail
NL-COL-007	Restriction of OneDrive sync to managed devices	Fail
NL-COL-012	Public groups and Teams open to every employee	Fail
NL-COL-014	Guests accept invitations with the invited account	Fail
NL-EML-008	External sender tag in Outlook	Fail
NL-EML-009	Calendar and contact sharing with other organisations	Fail
NL-EXO-106	Administrators told about internal senders of malware	Fail
NL-EXO-109	Administrators told about outbound spam	Fail
NL-EXO-112	Comprehensive attachment filtering	Fail
NL-EXO-113	Domains allowed to skip spam filtering	Fail
NL-EXO-114	Outbound spam limits	Fail
NL-EXO-117	Mailbox audit actions	Fail
NL-EXO-124	Direct Send rejected	Fail
NL-EXO-125	Preset security policies for everyone	Fail
NL-IDN-016	Sign-in details shown in Microsoft Authenticator	Fail
NL-IDN-101	Administrator accounts with application licences	Fail
NL-IDN-102	Idle session timeout for Microsoft 365 on the web	Fail
NL-IDN-108	Who can join devices to Entra ID	Fail
NL-IDN-110	Global Administrators made local administrators on joined devices	Fail
NL-IDN-111	People made local administrator of the devices they join	Fail
NL-IDN-112	Windows LAPS switched on in Entra ID	Fail
NL-IDN-121	Managed device required to register security info	Fail
NL-IDN-122	Intune enrolment signs in every time	Fail
NL-IDN-124	Password protection for on-premises Active Directory	Fail
NL-IDN-131	Client secrets on applications	Fail
NL-INT-102	Personal devices enrolling in Intune	Fail
NL-PVW-103	DLP across email, files, Teams and devices	Fail

Reference	Control	Result
NL-PVW-104	DLP rules block sharing	Fail
NL-PVW-107	Alert policies for compromised mail accounts	Fail
NL-PVW-108	Retention policies keep email and files	Fail
NL-SP0-101	External sharing limited to approved domains	Fail
NL-TMS-101	Third-party cloud storage in Teams	Fail
NL-TMS-107	Which Teams apps people can install	Fail
NL-TMS-108	Anonymous people joining Teams meetings	Fail
NL-TMS-110	Who bypasses the Teams meeting lobby	Fail
NL-ENR-useAuthenticatorApp	Migrate to Microsoft Authenticator	Fail
NL-LIC-003	Licences assigned to dormant accounts	Fail
NL-EX0-102	Calendar sharing with people outside the organisation	Fail
NL-EX0-104	Shared Bookings pages	Fail
NL-EX0-120	People installing Outlook add-ins	Fail
NL-EX0-122	MailTips	Fail
NL-EX0-123	Third-party storage in Outlook on the web	Fail
NL-EX0-127	DMARC at reject, with report addresses	Fail
NL-IDN-103	Third-party storage in Microsoft 365 on the web	Fail
NL-IDN-104	Office Store and self-service trials	Fail
NL-IDN-106	Dynamic group of guest accounts	Fail
NL-IDN-107	Users creating security groups	Fail
NL-IDN-109	Device limit per user	Fail
NL-IDN-113	People reading BitLocker keys of their own devices	Fail
NL-IDN-114	Guest invitations limited to allowed domains	Fail
NL-IDN-123	Custom banned password list	Fail
NL-IDN-126	Authentication methods migration complete	Fail
NL-IDN-132	Application certificate lifetime	Fail
NL-PVW-105	DLP rules tell people why	Fail
NL-PVW-110	Retention labels published	Fail
NL-TMS-102	Email into Teams channels	Fail
NL-TMS-112	Anonymous people in Teams meeting chat	Fail
NL-TMS-113	Who can present in Teams meetings	Fail
NL-TMS-115	Meeting chat with untrusted organisations	Fail
NL-TMS-116	Teams meeting recording by default	Fail
NL-GOV-002	Named locations for Conditional Access	Fail
NL-DEV-001	Device compliance policy coverage	Warning
NL-DEV-009	BitLocker, firewall and antivirus required on Windows	Warning

Reference	Control	Result
NL-ACC-005	Emergency access (break-glass) accounts	Warning
NL-COL-008	External access defaults for Teams and B2B	Warning
NL-COL-009	Sensitivity labels	Warning
NL-COL-010	Data loss prevention policies	Warning
NL-DEV-002	Device compliance rate	Warning
NL-EML-006	Exchange Online hardening	Warning
NL-COL-013	Sensitivity labels on Teams, groups and sites	Warning
NL-DEV-005	Unmanaged devices in the directory	Warning
NL-EML-010	Spam filtering skipped for listed senders	Warning
NL-IDN-005	Self-service password reset registration	Warning
NL-IDN-008	Conditional Access policies left in report-only or disabled state	Warning
NL-IDN-020	Admin consent workflow	Warning
NL-IDN-021	Group and team owners consenting to apps	Warning
NL-THR-004	Security and compliance notification contacts	Warning
NL-MSG-MC1101245	Exchange Online: basic authentication for SMTP AUTH is being retired	Warning
NL-ACC-013	Unused apps still holding permissions	Warning
NL-COL-006	Stale groups and Teams	Warning
NL-DEV-004	Stale device records	Warning
NL-EML-013	POP and IMAP for new mailboxes	Warning
NL-IDN-019	Phishing-resistant MFA for everyone	Warning
NL-LIC-004	Overlapping subscriptions	Warning
NL-EML-004	MTA-STS for inbound mail	Warning
NL-IDN-012	Guest access to the directory	Warning
NL-IDN-013	Self-service sign-up to the tenant	Warning
NL-LIC-005	Accounts without a usage location	Warning
NL-MSG-MC1098834	Microsoft Teams: retention setting for meeting recaps	Warning
NL-IDN-002	Enforcement of multi-factor authentication for all users	Pass
NL-IDN-115	MFA required for administrator roles by Conditional Access	Pass
NL-IDN-004	Identity baseline: security defaults or Conditional Access	Pass
NL-THR-006	Unified audit log	Pass
NL-THR-008	Mailbox auditing	Pass
NL-EXO-121	Modern authentication for Exchange Online	Pass
NL-ENR-switchFromPerUserMFA	Convert from per-user MFA to Conditional Access MFA	Pass
NL-DEV-007	Devices without disk encryption	Pass
NL-EML-003	DKIM keys published for domains that receive mail	Pass
NL-EML-012	Dangerous attachment types blocked	Pass

Reference	Control	Result
NL-EX0-111	DKIM signing turned on in Exchange Online	Pass
NL-GOV-003	Directory synchronisation health	Pass
NL-IDN-125	System-preferred multifactor authentication	Pass
NL-TMS-109	Anonymous people and dial-in callers starting Teams meetings	Pass
NL-TMS-114	External participants controlling shared screens	Pass
NL-IDN-105	Phishing protection in Microsoft Forms	Pass
NL-PVW-109	Retention policies applied without errors	Pass
NL-IDN-011	Password expiration policy	Pass
NL-TMS-111	Dial-in callers bypassing the Teams lobby	Pass
NL-GOV-004	Verified custom domain	Pass
NL-TMS-117	Teams live events always recorded	Pass
NL-SSR-mdo_antiphishingpolicies	Anti-phishing policy	Pass
NL-SSR-mdo_zaphish	Zero-hour auto purge	Pass
NL-COL-011	Purview retention labels Not checked: Secure Score does not track retention for this tenant, and Microsoft Graph does not let apps list retention labels or policies. Where Purview is set up for the tenant, NL-PVW-108 to NL-PVW-110 read them directly; otherwise check Microsoft Purview → Data lifecycle management → Retention policies.	Not assessed
NL-THR-005	Defender for Office 365 protections	Not applicable
NL-ACC-004	Just-in-time privileged access (PIM)	Not applicable
NL-EX0-105	Safe Links for email, Teams and Office apps	Not applicable
NL-EX0-107	Safe Attachments policy	Not applicable
NL-EX0-110	Anti-phishing policy with impersonation protection	Not applicable
NL-IDN-007	Identity Protection risk policies	Not applicable
NL-IDN-117	User risk policy (secure password change for high risk)	Not applicable
NL-IDN-118	Sign-in risk policy (MFA for medium and high risk)	Not applicable
NL-IDN-127	Approval to activate Global Administrator and Privileged Role Administrator	Not applicable
NL-EX0-108	Safe Attachments for SharePoint, OneDrive and Teams, and Safe Documents	Not applicable
NL-IDN-119	Medium and high-risk sign-ins blocked	Not applicable
NL-ACC-010	Conditional Access for workload identities	Not applicable
NL-EX0-115	Priority accounts in the strict preset policy	Not applicable
NL-EX0-116	Zero-hour auto purge for Teams	Not applicable
NL-EX0-126	Impersonation protection in the preset policies	Not applicable
NL-IDN-128	Alerts on privileged role assignment and activation	Not applicable
NL-IDN-129	Access reviews for guests	Not applicable
NL-IDN-130	Access reviews for privileged roles	Not applicable

Reference	Control	Result
NL-PVW-102	DLP for Microsoft Teams	Not applicable
NL-THR-007	Audit log retention	Not applicable
NL-TMS-118	Reporting suspicious Teams messages	Not applicable
NL-EXO-103	Customer Lockbox	Not applicable
NL-SSR-mdo_safeattachments	Safe Attachments	Not applicable
NL-SSR-mdo_safelinksforemail	Safe Links for email	Not applicable

Report generated 19 Oct 2026, 23:48 · Assessment 00000000-1111-2222-3333-444444444444 · Demo Consulting

Demo Consulting

Prepared by Demo Consulting

This report reflects the configuration of Contoso Group Ltd's Microsoft 365 tenant on 19 Oct 2026. Every finding comes from a rule applied to that configuration, read with read-only access; nothing in the tenant was changed to produce it.

1

Agree the priorities

Start with the Immediate items in the roadmap. Most are quick and low risk.

2

Make the changes

In planned change windows, following the steps in each finding.

3

Re-assess to confirm

A follow-up assessment re-reads the tenant, so every fix is confirmed rather than assumed.