



WEAK · GRADE E · GOAL 85

MICROSOFT 365 CLIENT REVIEW

Client Review

Prepared for Contoso Group Ltd

REVIEW PERIOD	POSTURE SCORE	GRADE	PREPARED BY
19 Oct 2026	21 / 100	E	Demo Consulting

ISSUES FIXED AND
CONFIRMED



POSTURE SCORE

21

FINDINGS STILL OPEN

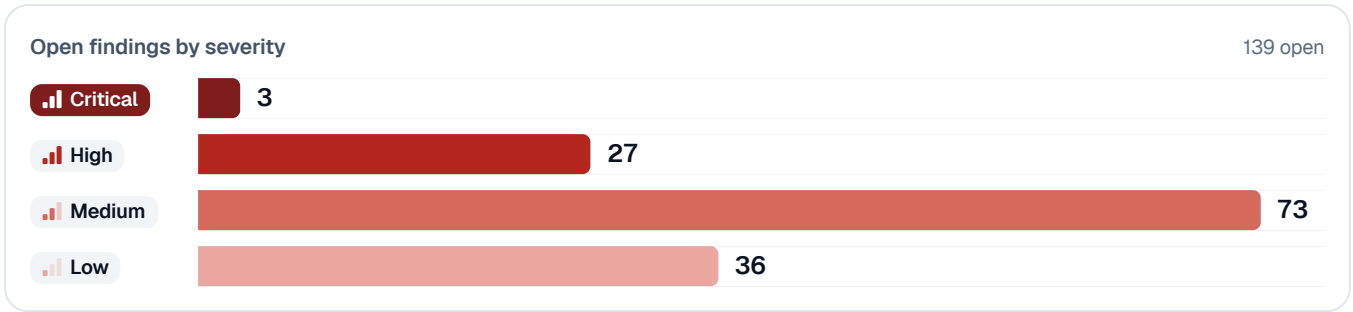
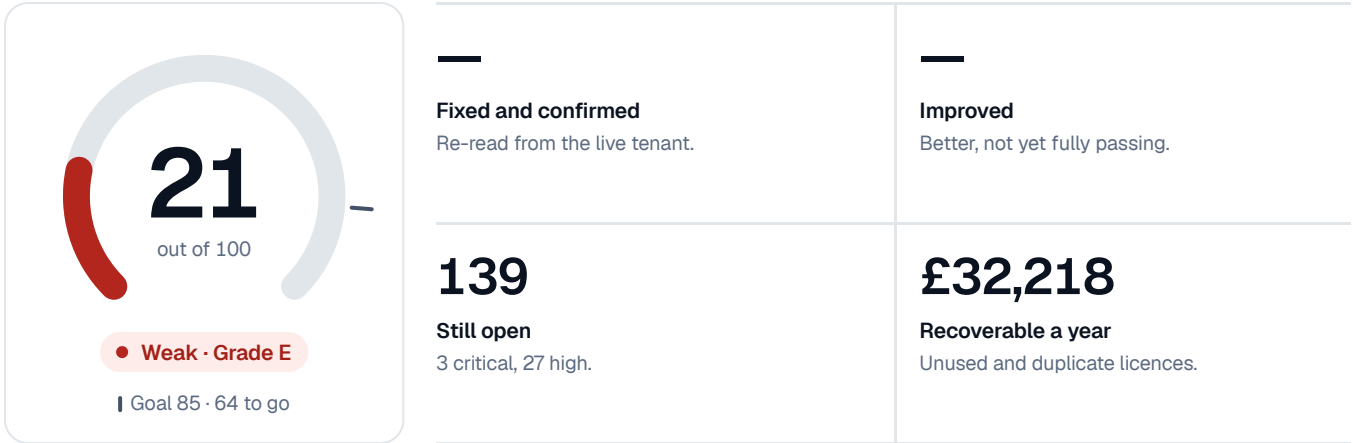
139



01 AT A GLANCE

Where the tenant stands

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



Headlines

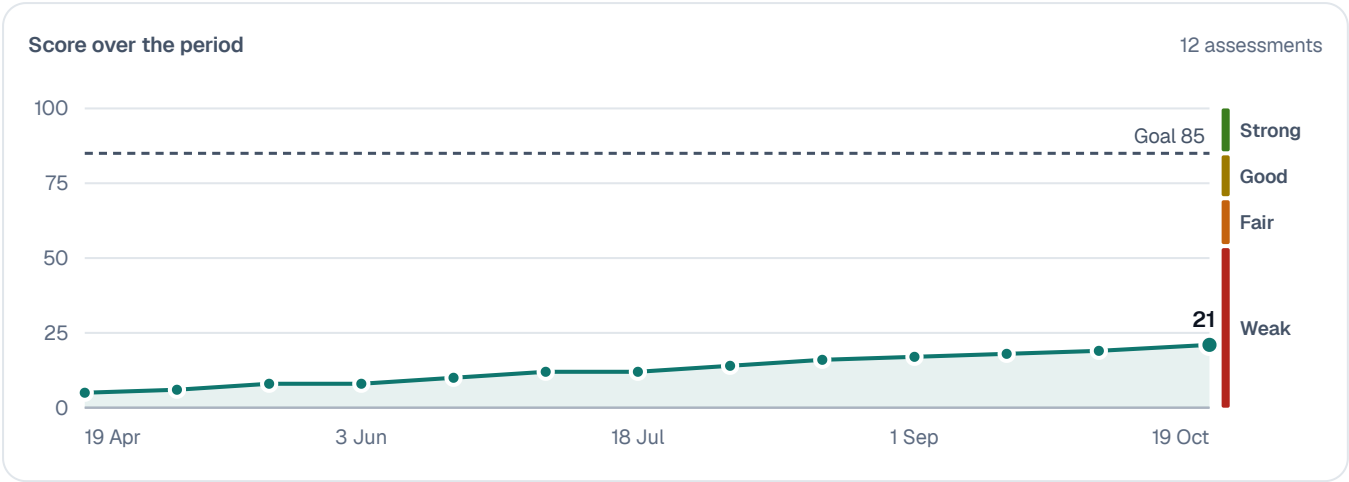
- ⚠ 3 critical issues need attention before anything else — these are the gaps an attacker would use first.
- 🛡 27 high-severity gaps were identified across identity, access and data protection.
- £ An indicative £32,218 a year of licence spend appears to be unused and recoverable.

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 WHAT WE DELIVERED

Changes made and confirmed

**Confirmed, not taken on trust**

Every item below was confirmed by re-reading the live tenant. A finding marked as done still has to pass the check before it counts as fixed.

This is the first review for this tenant. From the next one, this section lists every change made and confirmed since.

04 WHAT NEEDS ATTENTION

The risks still open

Highest risks still open

- 1

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

 Critical

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

Effort: low
- 2

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

 Critical

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

Effort: medium
- 3

No Conditional Access policy blocks legacy authentication, so MFA can be bypassed by using a legacy protocol.

 Critical

NL-IDN-003 · Blocking of legacy authentication. Legacy protocols cannot present a second factor.

Effort: medium
- 4

1 disabled account still has an admin role or external mail forwarding, and 7 leavers in all are not fully offboarded.

 High

NL-GOV-005 · Leavers not fully offboarded. Disabling a leaver is only the first step.

Effort: low
- 5

1 domain has missing or permissive SPF: contoso.co.uk (no SPF record).

 High

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.

Effort: low

05 RECOMMENDED NEXT STEPS

What we recommend next

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

#	Action	Severity	Time
1	Administrators without registered multi-factor authentication Register strong authentication for every privileged account today, then enforce it with Conditional Access.	 Critical	1.5 h
2	Unresolved risky users Triage every risky user: confirm compromise, reset credentials, revoke sessions, then dismiss or remediate the risk.	 Critical	1 h
3	Blocking of legacy authentication Create a Conditional Access policy blocking legacy authentication clients for all users.	 Critical	2 h
4	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	45 min
5	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	30 min
6	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	45 min

About 6.5 h of hands-on work in total for these 6.



£32,218

 a year

Licence spend that appears unused and recoverable

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.