SAMPLE · SYNTHETIC DATA · NOT A REAL CLIENT · REDACTED FOR DEMONSTRATION

TUFFOUR LABS · SAMPLE REPORT

Access Evidence Report

A read-only review of who can access what, who owns it, and what to fix, mapped to SOC 2 and ISO/IEC 27002:2022.

CLIENT	ENVIRONMENT	USERS REVIEWED	REPORT DATE
Acme SaaS Ltd.	**Microsoft 365 / Entra**	**48 · 6 systems**	**25 Nov 2026**

01 · MANAGEMENT SUMMARY

Ten findings. Three decisions.

This review covered the identity provider and the applications reachable through it. It did not test whether each application enforces the directory correctly, and it did not read mail, files or endpoint data. The evidence is a point-in-time snapshot; the manifest hash below is the integrity anchor.

48	6	61	10
USERS	SYSTEMS	GRANTS	FINDINGS

Decisions requested at the readout

1. Approve immediate revocation of the 3 former-user grants and the 14 dormant guests.
2. Name an owner for the 4 unowned high-privilege apps and the 2 standing Global Administrators.
3. Approve the 30-day remediation backlog and the quarterly re-run.

What this report proves

- The directory state at the snapshot time, with row-level evidence.
- Which grants have an owner, a review date, and a control reference.
- Which findings are high confidence, which need review, and which lack data.

What it does not prove

- That every application enforces the directory correctly.
- That Conditional Access cannot be bypassed.
- That the data inside each app is correctly classified.

02 · FINDINGS

Ranked by audit risk

CRITICAL

3 former users still hold application access

Owner: none
Confidence: High
Source: HR leaver list + client app export

Three accounts marked as leavers in the HR export are still enabled and still hold app grants. One has access to the finance folder and the CRM.

EVIDENCE ROWS

u_1042 · j.smit@acme.example · disabled: no · last sign-in 2026-10-28 · grants: Salesforce, SharePoint/Finance
u_1088 · m.devries@acme.example · disabled: no · last sign-in 2026-11-02 · grants: Slack, CRM
u_1121 · contractor@acme.example · disabled: no · last sign-in 2026-09-14 · grants: SharePoint/Finance

Control: SOC 2 CC6.2 / CC6.3 · ISO/IEC 27002:2022 5.16 / 5.18

Action: Disable, revoke sessions, remove app grants, transfer data, stamp the leaver date and approver. Effort: 2 hours.

HIGH

2 standing Global Administrators, neither PIM-eligible

Owner: IT
Confidence: High
Source: Microsoft Graph

Two accounts hold the Global Administrator role permanently. Neither is eligible through PIM, so every admin action is standing Tier-0 access.

EVIDENCE ROWS

admin@acme.example · role: Global Administrator · assignment: active/permanent · PIM eligible: no
it-ops@acme.example · role: Global Administrator · assignment: active/permanent · PIM eligible: no

Control: SOC 2 CC6.1 / CC6.3 · ISO/IEC 27002:2022 5.15 / 5.18

Action: Make both eligible, require approval + phishing-resistant MFA, keep one break-glass account excluded and monitored. Effort: 4 hours.

HIGH

14 dormant guests; 3 hold paid licences

Owner: mixed
Confidence: High
Source: Microsoft Graph

Fourteen guest accounts have no sign-in in 90 days. Three hold an E3 licence. Two have no sponsor in the business.

EVIDENCE ROWS

guest_014 · last sign-in 2025-08-12 · licence E3 · sponsor: none
guest_021 · last sign-in 2025-07-30 · licence E3 · sponsor: sales
guest_033 · last sign-in 2025-09-02 · no licence · sponsor: none

Control: SOC 2 CC6.1 · ISO/IEC 27002:2022 5.16

Action: Sponsor or remove. Remove the paid licences first. Effort: 3 hours.

HIGH

5 service principals with credentials expiring in 30 days; 2 already expired

Owner: 3 unowned
Confidence: High
Source: Microsoft Graph

Seven credentials are near or past expiry. Two are already expired, which means the integration is either broken or silently using another path.

EVIDENCE ROWS

sp_201 · secret end 2026-11-20 · expired · owner: none
sp_204 · cert end 2026-12-18 · 23 days · owner: finance
sp_209 · secret end 2027-01-04 · 40 days · owner: none

Control: SOC 2 CC6.1 · ISO/IEC 27002:2022 5.17

Action: Rotate, move to certificate/workload identity, assign an owner, add expiry monitoring. Effort: 4 hours.

HIGH

4 high-privilege apps with no owner and broad delegated scopes

Owner: none
Confidence: High
Source: Microsoft Graph (delegated grants)

Four app registrations hold broad delegated permissions and have no owner. One holds `Mail.Read`; another holds `Directory.ReadWrite.All`.

EVIDENCE ROWS

app_31 · Mail.Read · owners: 0 · last sign-in: no data
app_44 · Directory.ReadWrite.All · owners: 0 · last sign-in: no data
app_52 · Files.Read.All · owners: 0 · last sign-in: no data

Control: SOC 2 CC6.1 / CC6.3 · ISO/IEC 27002:2022 5.15 / 5.18

Action: Assign an owner, remove unused delegated permissions, require review before renewal. Effort: 3 hours.

MEDIUM

2 shared/generic accounts with admin access

Owner: IT
Confidence: High
Source: client export + manual review

Two generic accounts are used by more than one person and hold admin rights. There is no way to attribute an action to a named human.

EVIDENCE ROWS

svc-admin@acme.example · 3 named users · role: Exchange Administrator
backup@acme.example · 2 named users · role: SharePoint Administrator

Control: SOC 2 CC6.1 · ISO/IEC 27002:2022 5.17 / 5.18

Action: Replace with named accounts + PIM, or a managed identity where automation requires it. Effort: 4 hours.

MEDIUM

11 users without phishing-resistant MFA

Owner: IT
Confidence: Review
Source: client authentication-method export

Eleven users rely on SMS or voice. Two of them are in finance. The directory shows method registration, not whether a policy enforces it for every app.

Control: SOC 2 CC6.1 · ISO/IEC 27002:2022 5.17

Action: Enforce authentication strength for admins and finance first, then all users. Verify policy scope. Effort: 3 hours.

MEDIUM

Break-glass account is excluded from CA and used interactively

Owner: IT
Confidence: Review
Source: Graph CA policies + client sign-in export

One account is excluded from all Conditional Access policies. It has interactive sign-ins in the last 30 days outside an emergency. That turns a break-glass control into a standing bypass.

Control: SOC 2 CC6.1 · ISO/IEC 27002:2022 5.15 / 5.17

Action: Restrict to emergency use, store credentials in a vault, alert on any sign-in, review quarterly. Effort: 2 hours.

MEDIUM

21 grants have no reviewer or review date

Owner: mixed
Confidence: High
Source: client access-review export

Twenty-one of 61 grants have no reviewer and no last-reviewed date. The register cannot show who approved the access or when it was last checked.

Control: SOC 2 CC6.3 · ISO/IEC 27002:2022 5.18

Action: Assign reviewers by system owner; run a quarterly review; record decision + date. Effort: 6 hours in the first quarter.

MEDIUM

Overlapping SKUs and an add-on without a base licence

Owner: finance
Confidence: Review
Source: Graph SKUs + client licence export

Six users hold overlapping E3 + EMS E5 assignments. Two hold Copilot without an eligible base licence. This needs manual capability validation before any downgrade recommendation.

Control: Cost / asset management

Action: Validate service-plan usage, then remove overlaps. Do not downgrade without a capability-loss review. Effort: 4 hours.

03 · ACCESS REGISTER (EXCERPT)

Who can reach what

PERSON	SYSTEM	ACCESS	GRANTED	LAST REVIEW	OWNER	FLAG
J. Smit (leaver)	Salesforce	user	2024-02-01	n/a	n/a	ghost
J. Smit (leaver)	SharePoint / Finance	user	2024-02-01	n/a	n/a	ghost
M. de Vries (leaver)	Slack	member	2023-11-10	2025-02-01	Sales	ghost
Admin	Entra ID	Global Administrator	2022-01-01	n/a	IT	standing
IT Ops	Entra ID	Global Administrator	2022-01-01	n/a	IT	standing
Guest 014	Microsoft 365	E3	2024-06-01	n/a	n/a	dormant guest
svc-admin	Exchange	Exchange Administrator	2023-03-01	n/a	IT	shared
A. Bakker	CRM	admin	2025-01-15	2026-01-15	Sales	ok

Excerpt only. The full register has 61 rows. Rows marked “ghost” come from the HR leaver list; rows marked “dormant” come from the sign-in window. Both are evidence, not conclusions. The owner confirms.

04 · REMEDIATION PLAN

Now / 30 days / 90 days

Now (this week)

- Disable the 3 leavers and revoke sessions.
- Remove the 3 paid guest licences.
- Rotate the 2 expired service-principal credentials.
- Restrict the break-glass account to emergency use.

30 days

- Make the 2 Global Admins PIM-eligible.
- Assign owners to the 4 high-privilege apps.
- Remove unused app permissions.
- Enforce phishing-resistant MFA for admins and finance.

90 days

- Quarterly access review with named reviewers.
- Sponsor-or-remove for all guests.
- Replace the 2 shared admin accounts.
- Re-run the evidence pack and diff.

Accept the risk

For each finding, the client can record an accepted risk with a name, a date, a rationale and an expiry. The register records it; the auditor sees it. “Accepted” is not the same as “fixed.”

What the hash proves

Manifest

```
register sha256
9bfe90078887b33d1c76ba72b134303f56ef454427ae3eeed342b8606859867f
```

Canonical JSON over the register, methodology version, counts and timestamp. Any change to the register produces a different hash.

Method

Read-only Graph collection (users, groups, roles, apps, OAuth grants, CA, sign-ins) plus a CSV for systems outside the IdP. Findings are grouped, evidence rows are hashed, and confidence and source are stated per finding. The report is assembled and reviewed by the analyst; the collector is an evidence input, not the final report.

Limitations

This review proves what the directory and the connected applications say about access. It does not prove that every application enforces the directory correctly, that Conditional Access cannot be bypassed, or that the data inside each application is correctly classified. It is not a penetration test, an audit opinion, or a certification. The auditor decides whether the evidence is sufficient. Findings that depend on HR leaver data, per-user authentication methods, access-review records or app-native permissions are verified from client-supplied exports. The Graph collector alone does not produce them.

Data handling

- Processed in the EU.
- No mail, file or endpoint content.
- Raw exports deleted 30 days after the readout.
- Consent revoked on 25 Nov 2026.

Confidence

- **High:** direct directory evidence, no ambiguity.
- **Review:** evidence exists but needs owner confirmation.
- **Insufficient data:** licence, retention or API limit prevents a conclusion.