SAMPLE REPORT — FOR ILLUSTRATIVE PURPOSES ONLY

IT Health Check Executive Risk Report

Prepared for: Acme Professional Services Ltd. (Sample)

Assessment Date: May 2026 | Prepared by: DSIT Professional Services Inc. | Confidential

OVERALL RISK SCORE	MEDIUM-HIGH	Action required within 30 days

3	4	2	48hrs
Critical Findings	Medium Findings	Low Findings	Remediation Start

ASSESSMENT DETAILS

Organization	Acme Professional Services Ltd. (Sample — anonymized)
Industry	Professional Services
Employees	22
Devices Scanned	31 endpoints (24 workstations, 5 servers, 2 network devices)
Scan Date	May 2026
Assessed By	Steven Antoine — DSIT Professional Services Inc.
Report Type	IT Health Check — Executive Risk Report
Classification	CONFIDENTIAL — For authorized recipients only

EXECUTIVE SUMMARY

DSIT Professional Services Inc. conducted a comprehensive IT Health Check across all 31 endpoints and network infrastructure at Acme Professional Services Ltd. The assessment identified 3 critical findings requiring immediate attention, 4 medium-priority items requiring action within 30 days, and 2 lower-priority recommendations for the 90-day planning horizon.

The most significant finding is an unpatched remote access vulnerability on the organization's primary file server that has been exposed to the internet for an estimated 6 months. This represents an immediate and material risk to the confidentiality and integrity of all client data held on that system. Remediation of this finding alone justifies the cost of this assessment.

FINDINGS SUMMARY

ID	Finding	Area	Risk	Priority
F-01	Unpatched remote access vulnerability — primary file server exposed to internet	Network Perimeter	CRITICAL	Immediate
F-02	2 staff credentials found in dark web breach database — password reset required	Access Control	CRITICAL	Immediate
F-03	Backup system last verified 14 months ago — integrity unknown	Backup & DR	CRITICAL	Immediate
F-04	11 of 24 workstations running end-of-life OS (Windows 10 21H2)	Endpoint Security	MEDIUM	30 Days
F-05	No MFA enforced on Microsoft 365 — all accounts password-only	Access Control	MEDIUM	30 Days
F-06	No documented incident response or breach notification procedure	Compliance	MEDIUM	30 Days
F-07	Wi-Fi guest network not segmented from corporate network	Network	MEDIUM	30 Days
F-08	Software licence inventory incomplete — 6 unlicensed applications identified	Asset Management	LOW	90 Days
F-09	No formal IT asset register maintained	Asset Management	LOW	90 Days

CRITICAL FINDINGS — DETAIL

F-01 — Unpatched Remote Access Vulnerability

CRITICAL

The organization's primary file server has an unpatched vulnerability in its remote access service that has been publicly disclosed for approximately 6 months. The service is directly exposed to the internet with no intervening firewall rule. An attacker with basic tooling could exploit this vulnerability to gain unauthorized access to the server and all data stored on it.

Recommended Remediation Steps:

1. Immediately disable the exposed remote access service until patching is complete.
2. Apply the vendor-released security patch.
3. Reconfigure remote access behind VPN with MFA enforced.
4. Review server access logs for the past 6 months for indicators of unauthorized access.

F-02 — Compromised Credentials in Breach Database

CRITICAL

A dark web scan of the organization's email domain identified 2 staff email addresses and associated passwords in publicly available breach databases. Neither password has been changed since the breach. If these credentials are reused across business systems, they represent an active pathway for unauthorized access.

Recommended Remediation Steps:

1. Immediately reset passwords for the 2 affected accounts.
2. Enable MFA on all Microsoft 365 accounts without delay.
3. Brief affected staff on password hygiene and credential reuse risks.
4. Deploy a corporate password manager to prevent future credential reuse.

F-03 — Backup Integrity Unverified for 14 Months

CRITICAL

The organization's backup system has not had a verified restore test performed in 14 months. Backup jobs show as 'completed' in the management console but no one has confirmed that backed-up data can actually be restored. In the event of a ransomware attack or hardware failure, the organization may have no working recovery capability.

Recommended Remediation Steps:

1. Conduct an immediate test restore of a representative data set to verify backup integrity.
2. Document the verified Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
3. Schedule quarterly backup integrity tests going forward.
4. Implement automated backup verification if the current platform supports it.

COMPLIANCE SNAPSHOT — PIPEDA

Requirement	Status	Notes
Privacy Policy published	PARTIAL	Policy exists but has not been updated since 2021

Consent management process	GAP	No documented consent collection or withdrawal process
Data retention policy	GAP	No formal retention schedule defined
Breach notification procedure	GAP	No documented procedure — 72hr OPC notification requirement at risk
Data inventory / mapping	GAP	No inventory of personal information collected or processed
Staff privacy training	PARTIAL	Informal training only — no documented program

PRIORITIZED 90-DAY REMEDIATION ROADMAP

Timeline	Action	Owner	Est. Effort
Week 1	Patch F-01 remote access vulnerability & reconfigure behind VPN	DSIT	4–6 hrs
Week 1	Reset compromised credentials (F-02) & enable MFA on all M365 accounts	DSIT + Client	2–3 hrs
Week 1	Conduct backup restore test & document RTO/RPO (F-03)	DSIT	3–4 hrs
Month 1	Deploy OS updates to 11 end-of-life workstations (F-04)	DSIT	6–8 hrs
Month 1	Segment guest Wi-Fi from corporate network (F-07)	DSIT	2–3 hrs
Month 1	Draft incident response & breach notification procedure (F-06)	DSIT	3–4 hrs
Month 2	Deploy corporate password manager organization-wide	DSIT + Client	4–6 hrs
Month 2	Update Privacy Policy & document consent management process	Client + DSIT	4–5 hrs
Month 3	Complete IT asset register & resolve unlicensed software (F-08, F-09)	DSIT	3–4 hrs
Month 3	Schedule quarterly backup integrity test & compliance review	DSIT	Ongoing

NEXT STEPS

DSIT Professional Services Inc. is prepared to begin remediation immediately upon engagement. All critical findings (F-01, F-02, F-03) can be addressed within the first week of a managed services engagement at no additional project cost under the Professional or Premium plan.

- Schedule your 30-minute debrief call at dsitpro.com/contact to review these findings with your assigned principal
- Review the DSIT Professional or Premium managed services plan — both include immediate remediation of all critical findings
- Share this report with your legal counsel or insurance broker to understand your current exposure