SAM'S IT CONSULTING

IT, Network & Security Assessment

A practical view of risk, reliability, recovery, and infrastructure.

ILLUSTRATIVE SAMPLE	NOT A CLIENT REPORT
Business	Example Office Co. (fictional)
Environment	40 employees / one Ontario office
Report date	October 17, 2026
Version	1.0 / public demonstration

All business details, evidence records, observations, and results are fictional. No live systems were reviewed to create this sample. It shows the structure and depth of a scoped assessment, not a promise that every customer engagement includes every check.

Prepared by Samatar (Sam) Mahamed
sam@samatar.ca | samatar.ca

01 / EXECUTIVE SUMMARY

Address the gaps before buying more technology.

The fictional office has useful foundations: Microsoft 365, an IT provider, endpoint protection, and offsite server copies. The main priorities are privileged access, guest separation, backup administrative exposure, and validating recovery.

HIGH	MEDIUM	LOW	CRITICAL
4	6	2	0 identified in sample

What needs management attention

Approve a controlled review of privileged access and backup permissions. Assign alert ownership. Agree a safe recovery exercise and the business objectives it will test. Plan guest-network separation and current server updates.

What is already working

Offsite server copies are configured: 13 of 14 sampled offsite runs succeeded first time; the failed run succeeded the following day. This confirms job reporting, not restore capability.

Most staff and endpoints have baseline controls: 38 of 40 staff accounts are covered by MFA enforcement; 36 of 40 endpoints have recent protection telemetry. Exceptions remain in scope.

Remote access uses a VPN service: The reviewed firewall rules show no direct internet forwarding to Windows RDP. VPN authentication and access scope still require appropriate review.

Some operational safeguards are in place: The customer has an IT provider, a UPS, and available equipment records. UPS runtime under load was not tested.

Decision requested

Authorize the first phase of access and recovery improvements. Defer a server purchase until host dependencies, support options, and recovery results have been reviewed. No breach, infection, or immediate hardware failure is asserted.

Reading guide

Scope p3 | Environment p4 | Network p5 | Recovery p6 | Findings p7-12 | Roadmap p13 | Projects p14 | Evidence p15

02 / SCOPE AND METHOD

What was reviewed - and what was not.

Illustrative review period: October 12-16, 2026. One office, one tenant, all 40 computer records, one host, two server VMs, six network devices, and one NAS repository. Exports were reviewed as snapshots; a complete physical stocktake is not represented.

Method

Management and provider interviews establish business dependencies. Read-only exports and existing records support the findings. Each observation has an evidence reference, confidence boundary, business impact, action, owner, dependencies, and validation requirement.

Excluded activities

No active vulnerability scanning, penetration testing, packet capture, full endpoint examination, forensic investigation, restore exercise, UPS load test, or configuration change. No formal compliance opinion or certification. Line-of-business SaaS internals and supplier security are outside the sample scope.

Risk and confidence

Priority	How to interpret it
High	Material exposure or critical recovery uncertainty; prompt attention or validation.
Medium	Meaningful reliability or control gap; planned remediation or verification.
Low	Lower-priority documentation or planning improvement.

Unverified is not the same as failed. Priorities reflect context, not a vulnerability scanner score. Newly discovered critical exposure would be escalated immediately rather than waiting for the report meeting.

Effort and timing

Indicative labour: Small usually up to one day; Medium usually one to three days. Exceptions are stated. Estimates are not quotes or elapsed completion promises. Customer input, approvals, procurement, test run time, and maintenance windows affect schedules. No remediation is authorized by this sample.

03 / ENVIRONMENT

A typical office with cloud and local dependencies.

Area	Fictional environment	Review notes
People & endpoints	40 employees; 36 laptops and 4 desktops	All 40 listed; 36 security agents current, 4 stale
Microsoft 365	40 user licenses; 2 named admins; 1 shared legacy admin	One tenant; 38/40 staff covered by MFA enforcement
Local servers	1 physical host; 2 virtual servers	Directory services and shared files; approximately 1.2 TB file data
Network	1 firewall; 2 managed switches; 3 access points	Staff and guest SSIDs; one business internet circuit
Backup & power	1 NAS repository; offsite copy service; 1 UPS	Nightly server jobs; UPS self-test status only reviewed

Operating context

Staff use email, shared documents, video meetings, and browser-based business applications during weekdays. Local shared files and directory services remain important. The office manager coordinates IT; an external provider performs day-to-day support.

Account and device reconciliation

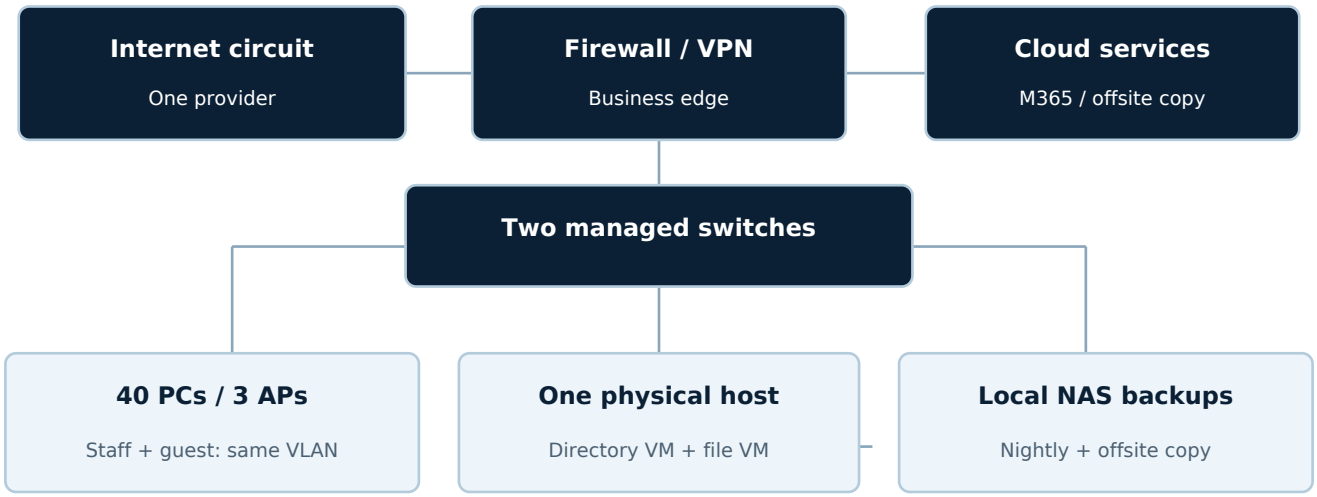
The 40 staff accounts are distinct from two named administrator accounts and one shared legacy administrator. MFA enforcement covers 38 staff; two staff exceptions and the privileged legacy exception require review. There are 40 endpoint records: 36 current and four stale. These counts are not a full device compliance certification.

Business priorities

Keep staff productive, avoid unmanaged access, recover key files reliably, and plan hardware spending without replacing equipment solely because of age.

04 / NETWORK OVERVIEW

See the dependencies and the recovery route.



Key observations

One internet provider is a dependency for cloud access. Staff and guest wireless use the same VLAN in the reviewed configuration (F02). One host supports both local server roles (F07). The NAS holds local backups and has shared administrative exposure with production (F03).

What the drawing does not establish

This is a simplified logical overview, not a cabling map or verified traffic-flow diagram. Switch interconnections, every port, IP addresses, firewall exceptions, and backup transport details are omitted. Active segmentation and failover tests were not performed.

Practical follow-up

Validate device roles and management paths with the provider. Preserve current configuration exports securely and document a recovery contact/access route. Evaluate a secondary internet circuit only against justified outage tolerance and actual carrier/path independence.

05 / BACKUP AND CONTINUITY

Recovery targets need evidence.

Workload	Current fictional arrangement	Evidence boundary
Local directory + file VMs	Nightly backup to NAS; 30 daily points configured; offsite copy with 30-day retention shown.	Console settings and job records only; restore and offsite deletion resistance not verified.
Shared files	Approximately 1.2 TB on the file VM.	Application/file integrity and full restore duration not tested.
Microsoft 365	Native versioning/recycle-bin features; no separate backup policy supplied.	Scenario coverage, retention assumptions, and bulk recovery not mapped.
Network configuration	Exports collected during assessment.	No established customer retention/restore process.

Sample job window: October 3-16

Local server jobs: 14/14 reported success. Offsite copy: 13/14 first-attempt successes; October 7 failed and October 8 completed successfully. A green job status is evidence of console reporting, not evidence of recoverability.

Desired objectives - not verified capabilities

RTO: management wants shared file access restored within four hours. RPO: management proposes no more than one working day of lost file changes. Nightly jobs may align with that RPO only if successful and usable. The RTO has not been demonstrated.

Recovery exercise to scope separately

Agree a safe isolated target, recovery credentials, representative data, and start/stop criteria. Record actual recovery point and elapsed time, validate access and file content, then document limitations and the next exercise. Do not overwrite live data as a demonstration.

06 / DETAILED FINDINGS

Findings 01-02

F01 / HIGH / Identity & security

A shared privileged account is outside MFA enforcement

Evidence (fictional): E02: Three standing privileged cloud accounts were listed: two named administrator accounts and one shared legacy administrator. Policy review showed the shared account excluded from MFA enforcement. No approved emergency-access procedure was provided.

Business impact: A compromised privileged password could allow changes to accounts, security settings, or business data. Shared use also makes actions harder to attribute.

Action: Confirm account ownership and dependencies. Move routine administration to named separate accounts, reduce standing privileges, and design monitored emergency access with appropriate controls before removing legacy access.

Validate closure: Test named administrator sign-in and recovery access in a controlled session. Confirm routine privileged access requires the intended controls; retain an agreed recovery route.

Owner: IT provider + business owner | Effort: Small: 0.5-1 day

When: Prompt review; first 30 days
Dependencies: Authorized access, licensing review, recovery-access plan
Confidence: Configuration observed; no account compromise established

F02 / HIGH / Network & Wi-Fi

Guest Wi-Fi shares the business network

Evidence (fictional): E03: The three access points map the guest and staff SSIDs to the same VLAN. The exported configuration shows no guest isolation control. No active reachability test was performed.

Business impact: A guest device may have network access toward business devices. Actual permitted paths still require validation; the configuration does not demonstrate separation.

Action: Define guest internet-only access, identify any legitimate exceptions, and plan a separate VLAN with firewall rules. Schedule the change and preserve management access.

Validate closure: From an authorized test device, confirm internet works and access to staff, server, and management networks is denied as intended. Validate staff printing and file access separately.

Owner: Network consultant + IT provider | Effort: Medium: 1-2 days

When: First 30 days, after design approval
Dependencies: Switch/AP support, VLAN plan, maintenance window, rollback copy
Confidence: Configuration observed; traffic paths not tested

06 / DETAILED FINDINGS

Findings 03-04

F03 / HIGH / Backups & security

One credential can administer production and local backups

Evidence (fictional): E04/E05: The same named administrator is used for host administration and NAS administration. The local backup repository is on that NAS. Offsite copy jobs appear in the console, but deletion protection was not verified.

Business impact: Compromise of this credential could affect production and its local recovery copies. Offsite deletion resistance must be checked before relying on it as an independent recovery layer.

Action: Separate administrative identities and permissions for backup management. Review offsite retention locks, deletion rights, recovery credentials, and alerting with the backup provider.

Validate closure: Review effective permissions and approved recovery access. Verify protection settings and a safe restore path; do not attempt destructive deletion testing in production.

Owner: Backup provider + IT provider | Effort: Medium: 1-2 days

When: First 30 days
Dependencies: Backup vendor access, supported permissions, approved access transition
Confidence: Shared administrative exposure observed; offsite protection unverified

F04 / HIGH / Recovery & continuity

The desired recovery time has not been demonstrated

Evidence (fictional): E01/E04/E07: Management requested file access within four hours and no more than one working day of data loss. Server jobs run nightly. No completed full-server restore exercise or timed recovery record was provided.

Business impact: Nightly jobs may align with the proposed data-loss tolerance if successful, but there is no evidence the four-hour recovery goal can be met. Missing evidence does not prove recovery will fail.

Action: Confirm the business recovery objectives and outage scenarios. Separately scope a restore exercise with an isolated destination, recovery sequence, acceptance checks, and named decision makers.

Validate closure: Record the actual recovery point, elapsed recovery time, application/file checks, and limitations. Compare results with approved objectives and update the plan.

Owner: Business owner + recovery consultant | Effort: Medium: 1-3 days for a separately scoped exercise

When: Plan in 30 days; exercise by 60 days
Dependencies: Approved targets, storage/compute capacity, credentials, test data handling
Confidence: Recovery capability not verified; high validation priority

06 / DETAILED FINDINGS

Findings 05-06

F05 / MEDIUM / Endpoint security

Four computers have stale protection status

Evidence (fictional): E06: Protection inventory contains 40 devices; four last reported more than 14 days before the sample review. The other 36 reported within 24 hours. These four devices were not examined directly.

Business impact: The console cannot establish current protection for those devices. They may be offline, retired, or experiencing an agent issue; they are not assumed to be unprotected or infected.

Action: Reconcile the four device records against staff and asset ownership. Inspect active devices, correct reporting failures, and retire stale records only after confirmation.

Validate closure: Confirm each active device reports current agent health and its assigned security policy. Record the disposition of retired devices.

Owner: IT provider + office manager | Effort: Small: 0.5-1 day

When: First 30 days
Dependencies: Device access, staff availability, asset ownership
Confidence: Reporting gap observed; local device state unverified

F06 / MEDIUM / Patching & systems

Server update installation and restart ownership are unclear

Evidence (fictional): E05/E07: Both guest-server update reports show pending security updates and a required restart. The provider supplied no completed monthly patch checklist or exception approval for the reviewed period.

Business impact: Updates may remain unapplied longer than intended. A pending restart can delay activation of fixes. No exploitation or specific vulnerability exposure was established.

Action: Agree the update owner, maintenance window, dependency checks, and restart process. Review current vendor advisories before prioritizing the actual deployment.

Validate closure: Confirm installation results, restart completion, service health, and the next reporting date. Record failed updates or approved exceptions.

Owner: IT provider + application owner | Effort: Small: 0.5-1 day, subject to preflight

When: First 30 days; earlier if advisory review requires
Dependencies: Application support, backup checks, access, outage approval
Confidence: Pending state observed; vulnerability exploitation not assessed

06 / DETAILED FINDINGS

Findings 07-08

F07 / MEDIUM / Infrastructure refresh

One aging host carries both local server roles

Evidence (fictional): E05/E08: One six-year-old physical host runs the directory-services VM and file-server VM. No second recovery host is recorded. Warranty expiry is shown as May 2027. No hardware fault was reported.

Business impact: A host failure could interrupt local sign-in services and shared files until repair or restore. Age alone does not prove replacement is urgent; workload dependency and recovery options drive the decision.

Action: Compare retaining with support and a proven recovery route, replacing the host, and retiring suitable local workloads. Assess application, identity, file-access, licensing, and connectivity dependencies first.

Validate closure: Approve an option against business needs and lifecycle costs. Separately design and test migration or recovery; do not retire the host until dependencies and rollback are resolved.

Owner: Business owner + infrastructure consultant | Effort: Small: 1 day for options; delivery quoted separately

When: Options by 60 days; approve a plan by 90 days
Dependencies: Application requirements, budget, warranty verification, recovery test
Confidence: Single-host dependency observed; no immediate failure predicted

F08 / MEDIUM / Network recovery

Current network configuration backups are incomplete

Evidence (fictional): E03/E07: Current read-only exports were obtained for the firewall, two switches, and three access points. The customer had no retained switch or AP configuration copy before the review; its firewall copy was 11 months old.

Business impact: Replacement or rollback may depend on manual reconstruction and provider availability. The new assessment exports help, but an operational backup and retention process is still needed.

Action: Establish secure configuration export/storage, version labels, an owner, and a cadence after changes. Maintain an access route that does not depend entirely on the failed equipment.

Validate closure: Confirm authorized staff can retrieve the right version and follow a vendor-supported restoration procedure. A live restore requires separate approval.

Owner: IT provider | Effort: Small: 0.5-1 day

When: By 60 days
Dependencies: Secure storage, vendor procedures, privileged access restrictions
Confidence: Documentation and backup-process gap observed

06 / DETAILED FINDINGS

Findings 09-10

F09 / MEDIUM / Microsoft 365 recovery

Cloud recovery coverage is not mapped to business needs

Evidence (fictional): E02/E07: Microsoft 365 recycle-bin/versioning capabilities are in use. No approved recovery coverage matrix, separately configured backup policy, or restore-test evidence was supplied for Exchange, SharePoint, and OneDrive.

Business impact: Native recovery features provide useful protection, but the business has not established whether their scope, history, and restoration process meet its scenarios. This is not a claim that Microsoft 365 has no recovery capability.

Action: Document deletion, ransomware, departed-user, and bulk-recovery scenarios. Review applicable native capabilities and compare additional backup options only where a justified gap remains.

Validate closure: Record coverage, permissions, retention assumptions, and a separately agreed sample restore. Confirm exclusions and objectives with management.

Owner: Microsoft 365 provider + business owner | Effort: Small: 0.5-1 day for review

When: By 60 days
Dependencies: Tenant access, license/capability review, business retention requirements
Confidence: Coverage not verified against requirements

F10 / MEDIUM / Monitoring & operations

Backup alerts have no named backup owner

Evidence (fictional): E04/E07: Failed-job notifications target one provider mailbox. No escalation contact or documented holiday cover was supplied. A failed offsite job on October 7 was followed by success on October 8; no impact investigation record was available.

Business impact: An alert may be delivered without timely action. The sampled recovery point recovered after retry, but the review cannot establish consistent response or coverage.

Action: Assign a primary and alternate owner, define expected response and escalation, and include backup and device-health checks in a short operating checklist.

Validate closure: Use a vendor-supported test notification; confirm receipt, acknowledgement, escalation, and evidence retention without intentionally failing production backups.

Owner: IT provider + office manager | Effort: Small: 0.5 day

When: First 30 days
Dependencies: Named contacts, agreed responsibilities, supported notification test
Confidence: Routing observed; response process not evidenced

06 / DETAILED FINDINGS

Findings 11-12

F11 / LOW / Documentation

The environment diagram and provider contacts need updating

Evidence (fictional): E07: The supplied diagram predates the current firewall and contains one retired switch. Provider contact information names a former account representative. A current assessment overview was drafted from the reviewed exports.

Business impact: Routine changes and incident handover may require avoidable rediscovery. There is no evidence that documentation has already caused an outage.

Action: Validate the overview, update vendor contacts and responsibilities, and assign an owner to maintain the records after changes.

Validate closure: Have the provider and office manager confirm the diagram and contact list. Keep a securely accessible offline copy of recovery contacts.

Owner: Office manager + IT provider | Effort: Small: 0.5 day

When: By 90 days
Dependencies: Provider confirmation, approved document storage
Confidence: Outdated records observed

F12 / LOW / Asset lifecycle

Equipment ownership and renewal dates are incomplete

Evidence (fictional): E08: The asset spreadsheet lists all 40 computers, but seven lack an assigned owner and warranty dates are missing for both switches and three access points. Serial numbers were not independently reconciled on every device.

Business impact: Budgeting, replacement planning, and support entitlement checks are harder. Missing fields do not mean equipment is unsupported.

Action: Confirm ownership and support dates, record renewal contacts, and build a simple annual replacement forecast linked to business criticality.

Validate closure: Reconcile missing fields with purchasing records and provider/vendor records. Review the inventory quarterly and after significant changes.

Owner: Office manager + purchasing contact | Effort: Small: 0.5-1 day

When: By 90 days
Dependencies: Purchasing records, vendor entitlement access
Confidence: Inventory completeness gap observed

07 / ROADMAP

Sequence the work around risk and dependencies.

This is a recommended 30/60/90-day plan, not a promise that all work will finish within 90 days. Urgent findings or new evidence are escalated promptly. Larger migrations can sit beyond the roadmap under a separate plan.

Prompt / first 30 days

Related findings: F01-F06, F10

Review privileged access and recovery access first; assign alert ownership; reconcile endpoints; plan guest separation and server updates. Agree recovery objectives and the restore exercise.

Business owner approves; IT provider leads changes. Critical new evidence is escalated immediately.

By 60 days

Related findings: F04, F07-F09

Perform the separately approved restore exercise; compare host refresh options; establish configuration backups; map cloud recovery requirements.

Depends on safe test capacity, application support, and the access-control changes.

By 90 days

Related findings: F07, F11-F12; recheck all

Approve the infrastructure direction, validate completed changes, update documentation and asset records, and close findings only with evidence.

Larger migrations may continue beyond 90 days under a separate project plan.

Close with evidence

The provider supplies policy/configuration results and validation records. The business owner accepts the residual risk or approves further work. Update the register with owner, action, date, evidence, and any remaining dependency. Do not mark a finding closed merely because a product was purchased.

08 / OPTIONAL PROJECTS

An assessment guides work; it does not authorize it.

The customer can use this report with its existing provider. Sam’s IT Consulting can separately scope defined improvements. There is no requirement to purchase remediation or ongoing support.

Identity and network hardening

Findings: F01-F03, F05-F06

Named admin access, guest separation, backup privilege separation, and endpoint/update corrections.

Preconditions: Approved design, maintenance window, configuration snapshots, validation and rollback.

Indicative effort: 1-4 delivery days across agreed windows; final scope required.

Recovery validation and planning

Findings: F04, F08-F10

Isolated server restore exercise, cloud recovery coverage review, configuration backup process, escalation checklist.

Preconditions: Approved test destination, representative data, business acceptance criteria; no live overwrite.

Indicative effort: 2-4 days, dependent on restore duration and scope.

Infrastructure refresh options and delivery

Findings: F07, F11-F12

Compare host replacement, supported retention, and selective cloud migration. Detail the chosen route only after discovery.

Preconditions: Application compatibility, identity/file dependencies, licensing, procurement, migration and rollback plan.

Indicative effort: Options review about 1 day; implementation separately designed and quoted.

Systems refresh decision

Compare supported retention, hardware replacement, and suitable cloud migration against application support, identity/file dependencies, outage tolerance, licensing, and total cost. Detailed migration design and purchasing specifications follow an approved option. No specific hardware is recommended from age alone.

09 / EVIDENCE AND HANDOVER

A traceable record and a usable review meeting.

ID	Fictional record	Coverage
E01	Management interview notes	Working-hours impact, priorities, proposed recovery targets
E02	Identity and Microsoft 365 exports	Accounts, policy assignments, licenses, recovery settings
E03	Network configuration exports	Firewall, switches, APs; no active traffic/path testing
E04	Backup console records, October 3-16	Job history, repositories, retention settings; no restore
E05	Host and guest inventory/update exports	VM placement, hardware, storage, pending updates
E06	Endpoint security status export	40-device status snapshot; no forensic analysis
E07	Provider interview and supplied records	Responsibilities, recovery notes, configuration history
E08	Asset register and purchase records	Ownership, age, support dates; not a physical stocktake

Findings review agenda

Confirm the priorities and evidence limits; agree owners and approvals; discuss retained risks; decide whether to scope implementation; record next actions and a follow-up date. Keep sensitive evidence in agreed secure storage, not in public marketing material. All records in this sample are invented.

General references

Canadian Centre for Cyber Security - baseline controls

Microsoft Learn - Microsoft 365 Backup FAQ

These references inform the approach. This is not a complete control mapping, formal audit, legal opinion, or guarantee of security, availability, compliance, or recovery. Source guidance reviewed October 17, 2026.