

IT & CYBERSECURITY ASSESSMENT

Prepared for: ACME, Corp.

Industry: Retail

Assessment date: October 26, 2026

Assessor: PBCLLC

Employees / users: 150.0

Assessment scope: MSP

WEIGHTED HEALTH SCORE	ASSESSMENT COVERAGE	GAPS IDENTIFIED
51/100	36 of 36 controls	14 failed / 8 partial

Executive overview

The assessed controls produced a weighted health score of 51/100. 14 controls failed and 8 were partially satisfied. 0 controls remain unassessed; they are excluded from the score.

Category results

Category	Score	Assessed	Failed
Cybersecurity	100%	6/6	0
Network Infrastructure	34%	6/6	2
Backup & Disaster Recovery	48%	6/6	3
IT Operations	68%	6/6	0
Compliance & Governance	0%	6/6	6
Cloud & Identity	50%	6/6	3

Executive decision guide

How to read this report

This document is a decision aid, not a technical certification. A control is a safeguard or operating practice that can reduce a specific business risk. Pass means the assessor recorded it as satisfied; Partial means improvement is needed; Fail means the requirement was not met; Not Assessed means no conclusion is available; N/A means it was excluded as not applicable.

What the score means

The health score is a weighted snapshot of assessed controls, not a probability of breach, financial loss estimate, or industry benchmark. High-weight controls contribute more to the score. Controls marked Not Assessed or N/A are excluded. Review assessment coverage alongside the score; a high score with low coverage is not strong assurance.

Questions leadership should ask

- Which findings could stop revenue-generating operations or expose sensitive data?
- What evidence confirms each high-priority finding?
- What must be addressed now, what can be phased, and who owns each decision?
- What downtime and data loss can the business tolerate?
- What are the one-time costs, recurring costs, residual risks, and measures of success?

Business glossary

Control: A technical or procedural safeguard used to manage risk.

MFA: Multi-factor authentication; an extra verification step at sign-in.

RTO: Recovery Time Objective; target maximum time to restore a service.

RPO: Recovery Point Objective; target maximum acceptable amount of lost data measured in time.

EDR: Endpoint Detection and Response; software that detects, investigates and supports response to suspicious activity on computers and servers.

NGFW: Next-Generation Firewall; network security that filters traffic and can inspect applications, threats and unauthorized connections.

SIEM: Security Information and Event Management; centralized collection and correlation of security events to support detection and investigation.

RMM: Remote Monitoring and Management; centralized oversight of device health, patching, alerts and approved remote maintenance.

MDR: Managed Detection and Response; ongoing security monitoring, investigation and response performed by an assigned security team.

SOC: Security Operations Center; the people and processes responsible for monitoring, investigating and coordinating security incidents.

IAM: Identity and Access Management; controls that determine who can access systems and what they are permitted to do.

BUDR: Backup and Disaster Recovery; protection and restoration of business data, systems and operations following disruption.

vCIO: Virtual Chief Information Officer; strategic technology planning, risk oversight and budgeting support for business leadership.

Vulnerability management: The process of identifying, prioritizing, correcting and verifying security weaknesses.

Patch management: The controlled deployment and verification of security and reliability updates.

Least privilege: Giving users only the access required for their responsibilities.

Immutable backup: A backup designed to resist alteration or deletion during its protected retention period.

Residual risk: Risk remaining after planned improvements are implemented.

Assessment status heatmap

Each cell represents one assessed safeguard. Green indicates Pass, yellow indicates Partial, and red indicates Fail. Gray means Not Assessed; white means Not Applicable. Colors reflect recorded results, not independently verified conclusions.

Pass	Partial	Fail	Not Assessed	N/A
------	---------	------	--------------	-----

Cybersecurity

Endpoint protection Pass	MFA coverage Pass	Email protection Pass
Security awareness Pass	Incident response Pass	Vulnerability management Pass

Network Infrastructure

Firewall lifecycle Partial	Network segmentation Partial	Wireless security Partial
Network monitoring Partial	Asset inventory Fail	Remote access Fail

Backup & Disaster Recovery

Backup coverage Fail	Offsite or immutable copy Fail	Restore testing Fail
Recovery objectives Pass	Disaster recovery plan Pass	Backup monitoring Pass

IT Operations

Patch management Pass	Helpdesk processes Pass	Proactive monitoring Partial
Documentation Partial	Lifecycle planning Partial	Change management Partial

Compliance & Governance

Security policies Fail	Risk assessment Fail	Access reviews Fail
Logging and retention Fail	Vendor management Fail	Regulatory mapping Fail

Cloud & Identity

Identity lifecycle Fail	Privileged access Fail	Microsoft 365 security Fail
Cloud backup Pass	Conditional access Pass	Device encryption Pass

Prioritized findings & recommended actions

Backup coverage — Fail (Priority review)

Assessment area: Backup & Disaster Recovery

What this evaluates: Protected copies of important files, applications, and systems.

Expected capabilities: Confirm what is included, how often copies run, and what is excluded.

Potential business consequences: Missing backups can mean permanent data loss.

How PBCLLC can address the finding: Inventory critical workloads and confirm they are protected by a supported backup solution. Review backup schedules, retention, exclusions and failure handling; document any licensing or storage gaps.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Offsite or immutable copy — Fail (Priority review)

Assessment area: Backup & Disaster Recovery

What this evaluates: A separate or tamper-resistant backup copy that an attacker cannot easily erase.

Expected capabilities: Check isolation, retention, and protection against administrative compromise.

Potential business consequences: Ransomware may destroy backups alongside production data.

How PBCLLC can address the finding: Evaluate backup platform support for isolated or immutable copies, access separation, retention and off-site recovery. Configure and validate protections using a suitable client-approved backup product.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Restore testing — Fail (Priority review)

Assessment area: Backup & Disaster Recovery

What this evaluates: Periodic proof that data and systems can actually be recovered from backup.

Expected capabilities: Ask for dated test results, recovery duration, and issue tracking.

Potential business consequences: A successful backup job does not guarantee a successful recovery.

How PBCLLC can address the finding: Schedule isolated recovery exercises using the client backup platform; restore representative files, applications and systems, verify usability, measure elapsed time and document exceptions and retests. Use RMM platform for supported monitoring and follow-up tracking.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Identity lifecycle — Fail (Priority review)

Assessment area: Cloud & Identity

What this evaluates: Creating, changing, and disabling accounts as people join, change roles, or leave.

Expected capabilities: Review approvals, automation, and prompt account removal.

Potential business consequences: Orphaned accounts can enable unauthorized access.

How PBCLLC can address the finding: Define cloud productivity joiner/mover/leaver procedures, approvals and deprovisioning timelines; test sample offboarding events.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Privileged access — Fail (Priority review)

Assessment area: Cloud & Identity

What this evaluates: Special protection for administrator accounts with broad system control.

Expected capabilities: Verify separate admin accounts, MFA, least privilege, and monitoring.

Potential business consequences: Compromised administrator access can affect the entire environment.

How PBCLLC can address the finding: Review administrative accounts, MFA, separate privileged identities, approval controls and audit events in cloud productivity, network security and other supported platforms.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Microsoft 365 security — Fail (Priority review)

Assessment area: Cloud & Identity

What this evaluates: An important technology safeguard.

Expected capabilities: Document the expected control capabilities.

Potential business consequences: Weaknesses can disrupt operations or expose information.

How PBCLLC can address the finding: PBCLLC will validate the finding, agree on an implementation plan, apply suitable monitoring and management capabilities, and document verification results.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Access reviews — Fail (Priority review)

Assessment area: Compliance & Governance

What this evaluates: Periodic confirmation that each person has only the access they need.

Expected capabilities: Review privileged accounts, former employees, and approval records.

Potential business consequences: Excess access increases potential damage from mistakes or compromise.

How PBCLLC can address the finding: Review cloud identity accounts, administrative roles, group memberships and supported application access; coordinate timely removal and periodic owner approval.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Remote access — Fail (Priority review)

Assessment area: Network Infrastructure

What this evaluates: Secure methods for employees and vendors to connect from outside the office.

Expected capabilities: Verify encryption, MFA, least privilege, and access review.

Potential business consequences: Weak remote access can expose internal systems.

How PBCLLC can address the finding: Review network security VPN or supported remote-access controls, require MFA, restrict privileges, and verify logging and offboarding.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Security policies — Fail (Priority review)

Assessment area: Compliance & Governance

What this evaluates: Written expectations for acceptable technology use and protection of information.

Expected capabilities: Verify leadership approval, employee awareness, and regular review.

Potential business consequences: Inconsistent practices create avoidable risk.

How PBCLLC can address the finding: Draft tailored security and acceptable-use policies, align them with applicable requirements, obtain leadership approval and establish annual reviews.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Risk assessment — Fail (Priority review)

Assessment area: Compliance & Governance

What this evaluates: A structured review of threats, weaknesses, likelihood, and business consequences.

Expected capabilities: Look for assigned owners, mitigation decisions, and periodic updates.

Potential business consequences: Leadership may spend on low-priority issues while major risks remain.

How PBCLLC can address the finding: Maintain a risk register with likelihood, business impact, treatment options, ownership and due dates. Review changes during vCIO governance meetings.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Logging and retention — Fail (Priority review)

Assessment area: Compliance & Governance

What this evaluates: Collecting and retaining useful records of security and system activity.

Expected capabilities: Review coverage, retention, alerting, and ability to investigate events.

Potential business consequences: Without records, incidents may be difficult to detect or explain.

How PBCLLC can address the finding: Review network security and supported endpoint logs, SIEM collection and retention settings, alert thresholds and investigation workflows; verify ingestion and searchability.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Regulatory mapping — Fail (Priority review)

Assessment area: Compliance & Governance

What this evaluates: Connecting applicable legal or contractual requirements to actual controls.

Expected capabilities: Identify which rules apply and the evidence required; do not assume certification.

Potential business consequences: Unmet obligations can create contractual or regulatory exposure.

How PBCLLC can address the finding: Identify applicable contractual and regulatory obligations, map evidence to controls and document gaps. PBCLLC can assist with NIST 800-171/CMMC readiness but must not represent self-assessment as third-party certification.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Vendor management — Fail (Priority review)

Assessment area: Compliance & Governance

What this evaluates: Oversight of outside providers that handle systems or sensitive data.

Expected capabilities: Review contracts, access, incident responsibilities, and service dependencies.

Potential business consequences: Third-party failures can disrupt the organization.

How PBCLLC can address the finding: Create an inventory of critical providers, access privileges, service commitments, security responsibilities and escalation contacts; review annually.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Asset inventory — Fail (Priority review)

Assessment area: Network Infrastructure

What this evaluates: An accurate register of computers, servers, networking equipment, and software.

Expected capabilities: Review ownership, age, support status, and completeness.

Potential business consequences: Unknown assets are difficult to secure, maintain, or budget for.

How PBCLLC can address the finding: Build and reconcile an inventory using RMM platform discovery and client procurement records, including device ownership, warranties, software support and lifecycle dates.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Firewall lifecycle — Partial (Improvement required)

Assessment area: Network Infrastructure

What this evaluates: A next-generation firewall (NGFW) controls and inspects network traffic and requires updates, support, and configuration reviews.

Expected capabilities: Check supported firmware, rule reviews, logging, and replacement planning.

Potential business consequences: Obsolete equipment can expose the network or cause outages.

How PBCLLC can address the finding: Review next-generation firewall models, support contracts, firmware advisories, rule sets and configuration backups. Plan validated firmware maintenance and replacement where required.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Proactive monitoring — Partial (Improvement required)

Assessment area: IT Operations

What this evaluates: Automated checks and alerts that identify problems before users report them.

Expected capabilities: Review coverage, thresholds, escalation, and automated remediation safeguards.

Potential business consequences: Preventable failures can interrupt operations.

How PBCLLC can address the finding: Use RMM health checks and carefully approved automation for supported systems; tune alerts and verify that automated actions are safe and auditable.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Change management — Partial (Improvement required)

Assessment area: IT Operations

What this evaluates: A controlled method to plan, approve, test, and reverse important IT changes.

Expected capabilities: Review approvals, rollback plans, and post-change verification.

Potential business consequences: Poorly managed changes can cause outages.

How PBCLLC can address the finding: Define change requests, business approvals, implementation testing, rollback plans and post-change verification for infrastructure and cloud changes.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Network segmentation — Partial (Improvement required)

Assessment area: Network Infrastructure

What this evaluates: Separating sensitive systems and user groups limits how far an incident can spread.

Expected capabilities: Review guest, employee, server, and critical-system boundaries.

Potential business consequences: One compromised device may otherwise affect many systems.

How PBCLLC can address the finding: Assess trusted, guest, server and sensitive-network traffic flows; design next-generation firewall policies and VLAN boundaries with client approval, then test permitted and blocked access.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Wireless security — Partial (Improvement required)

Assessment area: Network Infrastructure

What this evaluates: Controls that protect business Wi-Fi from unauthorized access.

Expected capabilities: Check encryption, guest isolation, credentials, and access-point management.

Potential business consequences: Poorly secured Wi-Fi can expose internal resources.

How PBCLLC can address the finding: Review access-point settings, WPA configuration, guest isolation, credentials and firmware. Coordinate network changes and verify access after implementation.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Network monitoring — Partial (Improvement required)

Assessment area: Network Infrastructure

What this evaluates: Continuous visibility into network availability, errors, and unusual conditions.

Expected capabilities: Confirm alerts, response ownership, and useful trend reporting.

Potential business consequences: Undetected problems can disrupt staff and customers.

How PBCLLC can address the finding: Use RMM platform where supported and network security device telemetry to track connectivity, device health and service degradation; route actionable alerts to documented support workflows.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Documentation — Partial (Improvement required)

Assessment area: IT Operations

What this evaluates: Current records of systems, configurations, vendors, and recovery procedures.

Expected capabilities: Check secure storage, accuracy, ownership, and update cadence.

Potential business consequences: Critical knowledge can be lost when staff or vendors change.

How PBCLLC can address the finding: Develop controlled records of assets, diagrams, configurations, credentials ownership and recovery runbooks; establish secure access and review cycles.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

Lifecycle planning — Partial (Improvement required)

Assessment area: IT Operations

What this evaluates: Budgeting and scheduling replacement of aging hardware and software.

Expected capabilities: Review warranties, support dates, and capital forecasts.

Potential business consequences: Unexpected failures and emergency purchases raise costs.

How PBCLLC can address the finding: Combine RMM platform inventory and purchasing records into replacement schedules, warranty reviews and multiyear technology budget recommendations.

Leadership decision: Confirm business priority, approve scope and budget, designate an owner, and require documented verification of the completed work.

What was assessed — executive reference guide

Each item explains the safeguard, expected capabilities, business consequences, and how PBCLLC can support improvement. Statuses are taken from the Excel workbook; descriptions are general educational guidance, not claims about the client.

Cybersecurity

Protects against malicious activity, fraud, and unauthorized access.

Endpoint protection — Pass

What it is: Security software that detects and blocks malicious activity on computers and servers.

Capabilities to expect: Look for centrally managed protection, alerts, isolation capability, and documented response.

Why it matters: Malware or ransomware can interrupt work and compromise information.

MFA coverage — Pass

What it is: Multi-factor authentication requires another proof of identity beyond a password.

Capabilities to expect: Verify coverage for email, remote access, administrators, and other important systems.

Why it matters: A stolen password alone may otherwise grant an attacker access.

Email protection — Pass

What it is: Filtering and authentication controls reduce phishing, malicious attachments, and impersonation.

Capabilities to expect: Review filtering, domain protections, suspicious-link handling, and reporting.

Why it matters: Fraudulent email can lead to financial loss or account compromise.

Security awareness — Pass

What it is: Practical training helps staff recognize suspicious messages and report incidents.

Capabilities to expect: Look for recurring training, realistic exercises, and simple reporting channels.

Why it matters: Human error can enable scams and data exposure.

Incident response — Pass

What it is: A documented process for identifying, containing, and recovering from a cyber incident.

Capabilities to expect: Verify responsibilities, escalation contacts, communications, and rehearsals.

Why it matters: Slow decisions can increase downtime and financial damage.

Vulnerability management — Pass

What it is: A repeatable process to discover, prioritize, and fix exploitable weaknesses.

Capabilities to expect: Look for scanning, ownership, remediation deadlines, and validation.

Why it matters: Unaddressed weaknesses can become entry points.

Network Infrastructure

Keeps offices, devices, and applications connected reliably and securely.

Firewall lifecycle — Partial

What it is: A next-generation firewall (NGFW) controls and inspects network traffic and requires updates, support, and configuration reviews.

Capabilities to expect: Check supported firmware, rule reviews, logging, and replacement planning.

Why it matters: Obsolete equipment can expose the network or cause outages.

PBCLLC approach: Review next-generation firewall models, support contracts, firmware advisories, rule sets and configuration backups. Plan validated firmware maintenance and replacement where required.

Network segmentation — Partial

What it is: Separating sensitive systems and user groups limits how far an incident can spread.

Capabilities to expect: Review guest, employee, server, and critical-system boundaries.

Why it matters: One compromised device may otherwise affect many systems.

PBCLLC approach: Assess trusted, guest, server and sensitive-network traffic flows; design next-generation firewall policies and VLAN boundaries with client approval, then test permitted and blocked access.

Wireless security — Partial

What it is: Controls that protect business Wi-Fi from unauthorized access.

Capabilities to expect: Check encryption, guest isolation, credentials, and access-point management.

Why it matters: Poorly secured Wi-Fi can expose internal resources.

PBCLLC approach: Review access-point settings, WPA configuration, guest isolation, credentials and firmware. Coordinate network changes and verify access after implementation.

Network monitoring — Partial

What it is: Continuous visibility into network availability, errors, and unusual conditions.

Capabilities to expect: Confirm alerts, response ownership, and useful trend reporting.

Why it matters: Undetected problems can disrupt staff and customers.

PBCLLC approach: Use RMM platform where supported and network security device telemetry to track connectivity, device health and service degradation; route actionable alerts to documented support workflows.

Asset inventory — Fail

What it is: An accurate register of computers, servers, networking equipment, and software.

Capabilities to expect: Review ownership, age, support status, and completeness.

Why it matters: Unknown assets are difficult to secure, maintain, or budget for.

PBCLLC approach: Build and reconcile an inventory using RMM platform discovery and client procurement records, including device ownership, warranties, software support and lifecycle dates.

Remote access — Fail

What it is: Secure methods for employees and vendors to connect from outside the office.

Capabilities to expect: Verify encryption, MFA, least privilege, and access review.

Why it matters: Weak remote access can expose internal systems.

PBCLLC approach: Review network security VPN or supported remote-access controls, require MFA, restrict privileges, and verify logging and offboarding.

Backup & Disaster Recovery

Determines whether essential operations can recover after disruption.

Backup coverage — Fail

What it is: Protected copies of important files, applications, and systems.

Capabilities to expect: Confirm what is included, how often copies run, and what is excluded.

Why it matters: Missing backups can mean permanent data loss.

PBCLLC approach: Inventory critical workloads and confirm they are protected by a supported backup solution. Review backup schedules, retention, exclusions and failure handling; document any licensing or storage gaps.

Offsite or immutable copy — Fail

What it is: A separate or tamper-resistant backup copy that an attacker cannot easily erase.

Capabilities to expect: Check isolation, retention, and protection against administrative compromise.

Why it matters: Ransomware may destroy backups alongside production data.

PBCLLC approach: Evaluate backup platform support for isolated or immutable copies, access separation, retention and off-site recovery. Configure and validate protections using a suitable client-approved backup product.

Restore testing — Fail

What it is: Periodic proof that data and systems can actually be recovered from backup.

Capabilities to expect: Ask for dated test results, recovery duration, and issue tracking.

Why it matters: A successful backup job does not guarantee a successful recovery.

PBCLLC approach: Schedule isolated recovery exercises using the client backup platform; restore representative files, applications and systems, verify usability, measure elapsed time and document exceptions and retests. Use RMM platform for supported monitoring and follow-up tracking.

Recovery objectives — Pass

What it is: Agreed targets for acceptable downtime and data loss: RTO and RPO.

Capabilities to expect: Match targets to business processes and test whether systems can meet them.

Why it matters: Unrealistic targets create costly surprises during outages.

Disaster recovery plan — Pass

What it is: A practical sequence for restoring operations after major disruption.

Capabilities to expect: Verify priorities, contacts, dependencies, alternate processes, and exercises.

Why it matters: Teams may lose valuable time deciding what to restore first.

Backup monitoring — Pass

What it is: Daily oversight of backup failures, capacity, and missed jobs.

Capabilities to expect: Verify alert ownership and documented correction of failures.

Why it matters: Silent backup failures may remain unnoticed until an emergency.

IT Operations

Supports staff productivity and reduces preventable outages.

Patch management — Pass

What it is: Testing and installing security and reliability updates on devices and applications.

Capabilities to expect: Review deadlines, exceptions, reporting, and verification.

Why it matters: Known vulnerabilities can remain exploitable.

Helpdesk processes — Pass

What it is: Defined ways employees request support and issues are prioritized and resolved.

Capabilities to expect: Review response targets, escalation, tracking, and user communication.

Why it matters: Unstructured support prolongs employee downtime.

Proactive monitoring — Partial

What it is: Automated checks and alerts that identify problems before users report them.

Capabilities to expect: Review coverage, thresholds, escalation, and automated remediation safeguards.

Why it matters: Preventable failures can interrupt operations.

PBCLLC approach: Use RMM health checks and carefully approved automation for supported systems; tune alerts and verify that automated actions are safe and auditable.

Documentation — Partial

What it is: Current records of systems, configurations, vendors, and recovery procedures.

Capabilities to expect: Check secure storage, accuracy, ownership, and update cadence.

Why it matters: Critical knowledge can be lost when staff or vendors change.

PBCLLC approach: Develop controlled records of assets, diagrams, configurations, credentials ownership and recovery runbooks; establish secure access and review cycles.

Lifecycle planning — Partial

What it is: Budgeting and scheduling replacement of aging hardware and software.

Capabilities to expect: Review warranties, support dates, and capital forecasts.

Why it matters: Unexpected failures and emergency purchases raise costs.

PBCLLC approach: Combine RMM platform inventory and purchasing records into replacement schedules, warranty reviews and multiyear technology budget recommendations.

Change management — Partial

What it is: A controlled method to plan, approve, test, and reverse important IT changes.

Capabilities to expect: Review approvals, rollback plans, and post-change verification.

Why it matters: Poorly managed changes can cause outages.

PBCLLC approach: Define change requests, business approvals, implementation testing, rollback plans and post-change verification for infrastructure and cloud changes.

Compliance & Governance

Clarifies accountability, obligations, and leadership oversight.

Security policies — Fail

What it is: Written expectations for acceptable technology use and protection of information.

Capabilities to expect: Verify leadership approval, employee awareness, and regular review.

Why it matters: Inconsistent practices create avoidable risk.

PBCLLC approach: Draft tailored security and acceptable-use policies, align them with applicable requirements, obtain leadership approval and establish annual reviews.

Risk assessment — Fail

What it is: A structured review of threats, weaknesses, likelihood, and business consequences.

Capabilities to expect: Look for assigned owners, mitigation decisions, and periodic updates.

Why it matters: Leadership may spend on low-priority issues while major risks remain.

PBCLLC approach: Maintain a risk register with likelihood, business impact, treatment options, ownership and due dates. Review changes during vCIO governance meetings.

Access reviews — Fail

What it is: Periodic confirmation that each person has only the access they need.

Capabilities to expect: Review privileged accounts, former employees, and approval records.

Why it matters: Excess access increases potential damage from mistakes or compromise.

PBCLLC approach: Review cloud identity accounts, administrative roles, group memberships and supported application access; coordinate timely removal and periodic owner approval.

Logging and retention — Fail

What it is: Collecting and retaining useful records of security and system activity.

Capabilities to expect: Review coverage, retention, alerting, and ability to investigate events.

Why it matters: Without records, incidents may be difficult to detect or explain.

PBCLLC approach: Review network security and supported endpoint logs, SIEM collection and retention settings, alert thresholds and investigation workflows; verify ingestion and searchability.

Vendor management — Fail

What it is: Oversight of outside providers that handle systems or sensitive data.

Capabilities to expect: Review contracts, access, incident responsibilities, and service dependencies.

Why it matters: Third-party failures can disrupt the organization.

PBCLLC approach: Create an inventory of critical providers, access privileges, service commitments, security responsibilities and escalation contacts; review annually.

Regulatory mapping — Fail

What it is: Connecting applicable legal or contractual requirements to actual controls.

Capabilities to expect: Identify which rules apply and the evidence required; do not assume certification.

Why it matters: Unmet obligations can create contractual or regulatory exposure.

PBCLLC approach: Identify applicable contractual and regulatory obligations, map evidence to controls and document gaps. PBCLLC can assist with NIST 800-171/CMMC readiness but must not represent self-assessment as third-party certification.

Cloud & Identity

Protects digital identities, cloud services, and business information.

Identity lifecycle — Fail

What it is: Creating, changing, and disabling accounts as people join, change roles, or leave.

Capabilities to expect: Review approvals, automation, and prompt account removal.

Why it matters: Orphaned accounts can enable unauthorized access.

PBCLLC approach: Define cloud productivity joiner/mover/leaver procedures, approvals and deprovisioning timelines; test sample offboarding events.

Privileged access — Fail

What it is: Special protection for administrator accounts with broad system control.

Capabilities to expect: Verify separate admin accounts, MFA, least privilege, and monitoring.

Why it matters: Compromised administrator access can affect the entire environment.

PBCLLC approach: Review administrative accounts, MFA, separate privileged identities, approval controls and audit events in cloud productivity, network security and other supported platforms.

Microsoft 365 security — Fail

What it is: This control supports reliable and secure IT operations.

Capabilities to expect: Confirm the relevant operating capabilities and evidence.

Why it matters: Gaps can affect business continuity or information security.

PBCLLC approach: PBCLLC will validate the finding, agree on an implementation plan, apply suitable monitoring and management capabilities, and document verification results.

Cloud backup — Pass

What it is: Independent recovery protection for cloud-hosted business data where appropriate.

Capabilities to expect: Verify provider responsibilities, retention, and tested recovery.

Why it matters: Cloud availability does not automatically guarantee recovery of deleted data.

Conditional access — Pass

What it is: Policies that adjust sign-in requirements based on identity, device, or risk.

Capabilities to expect: Check MFA enforcement, device requirements, exceptions, and logout safeguards.

Why it matters: High-risk sign-ins may otherwise receive the same access as trusted ones.

Device encryption — Pass

What it is: Protection that makes data on lost or stolen devices harder to read.

Capabilities to expect: Verify encryption coverage and secure recovery-key management.

Why it matters: Lost equipment can expose confidential information.

Leadership action plan

Use this sequence to turn assessment findings into an approved, measurable improvement program.

1. Validate

Confirm the scope, supporting evidence, business dependencies, and unresolved items.

2. Prioritize

Address findings that could cause major interruption, material data exposure, or contractual harm first.

3. Budget

Request itemized one-time implementation costs, ongoing service costs, dependencies, and options.

4. Assign ownership

Designate an executive sponsor and accountable technical owner for each approved action.

5. Verify

Require documented tests and a follow-up assessment to confirm improvements work.

Approval considerations

Before approving a proposal, compare expected risk reduction, operational benefits, total cost, implementation disruption, and remaining risk. Proposed controls should not be represented as implemented until verified. This report does not establish regulatory compliance or guarantee prevention of incidents.

Assessment limitations

This report summarizes manually entered assessment responses. Scores are weighted indicators, not certifications, penetration-test results, or guarantees of security. Not Assessed and N/A controls are excluded from scoring. Findings require supporting verification before remediation decisions. Internal evidence notes are intentionally omitted from this client-facing report.