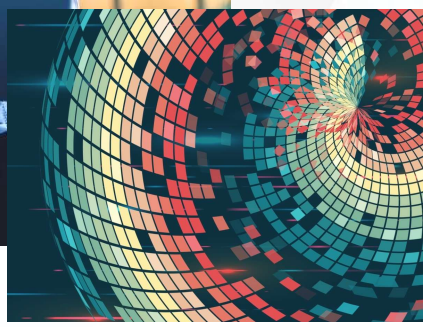
UZADO
COMPLIANCE & CYBER SECURITY SERVICES

Minimum Standards Assessment

[DATE]

Minimum Standards Assessment Report prepared for ACME Inc



Sean Sullivan
ssullivan@Uzado.com
416.459.0530

Table of Contents

Statement of Confidentiality

For the purposes of this document the “Client” is defined as:

ACME Inc
2500 Innovation Parkway
Suite 800
Metropolis, NY 10001
USA

This report contains information that is confidential and proprietary to both UZADO Inc. (“UZADO”) and the Client, including detailed infrastructure and security information (the “Information”). UZADO requires that this information be held in strict confidence by the recipient and be protected with the same degree of care as the recipient uses to protect its own confidential and proprietary information, which in any event shall not be less than a reasonable degree of care.

The recipient shall use the Information solely for internal information and for no other purpose without UZADO ’s prior written consent. The recipient shall not, without the prior written consent of UZADO, disclose the Information to any person or entity except its own authorized employees or agents who require same in connection with evaluating this document and only after such personnel have been advised of the confidential and proprietary nature of the Information and have agreed to protect it with the same degree of care. Any use that a third party makes of the deliverables, and any reliance or decisions made based on it, are the responsibility of such a third party. UZADO accepts no liability or responsibility for any loss or damages suffered by any third party because of decisions made or actions based on the deliverables.

Our services were performed, and this report was developed, in accordance with our contract with the Client and is subject to the terms and conditions included therein. The sufficiency of the procedures is the responsibility of the Client. Consequently, we make no representation regarding the sufficiency of the procedures for the purpose of this engagement or for any other purpose. Our approach does not constitute an examination in accordance with generally accepted accounting standards or attestation standards. As a result, we have not provided an opinion, attestation, or other form of assurance.

Our work was limited to the specific procedures and analysis described herein. Accordingly, changes in circumstances after this date could affect the findings outlined in this report. The projection to the future of any evaluation of the controls to achieve the related control objectives is subject to the risk that controls may become inadequate or fail. Our report must be considered in its entirety by the reader. Selecting and relying on a specific portion of the analysis or factors UZADO considers in isolation may be misleading.

Revision Summary

Version	Date	Description	Author
0.1	[DATE]	Build Template	Ken Dobson
0.2	[DATE]	Update Template to align to Min Stds	Ken Dobson
0.3	[DATE]	Add Findings	Ken Dobson
0.4	[DATE]	Internal Draft	Ken Dobson
0.5	[DATE]	Final for Internal Review	Ken Dobson
0.6	[DATE]	Final for Customer	Ken Dobson

Executive Summary

Uzado Inc. conducted a comprehensive Minimum Standards Security Assessment of ACME Inc between [START DATE] and [END DATE]. The objective was to evaluate the organization's current security posture, operational resilience, governance maturity, and compliance alignment against industry-recognized control frameworks.

This assessment was structured using core control principles derived from:

- PCI DSS (Payment Card Industry Data Security Standard)
- SOC 2 Trust Services Criteria (Security, Availability, Confidentiality, Processing Integrity)

These frameworks were selected as the foundational benchmark because ACME Inc operates in an environment that processes transactional data, customer information, and system integrations that require strong logical access controls, network segmentation, vulnerability management, and operational monitoring. PCI and SOC 2 represent industry-recognized, audit-defensible baselines for organizations in technology-driven, transaction-based industries.

Using these frameworks ensures that Minimum Standards are not arbitrary, but instead reflect tested, regulator-recognized, and audit-ready control expectations.

The assessment identified elevated vulnerability exposure, including 1,390 active vulnerabilities with 48 critical and 803 high severity findings, largely driven by legacy Windows systems and outdated third party software. Network resilience presents additional risk due to improper dual WAN configuration and reliance on a persistent VPN architecture, which has already been impacted by prior fiber disruptions. Monitoring and logging controls require strengthening, as Fortinet reporting is not enabled and formal log review and escalation procedures are not fully documented. Governance maturity is developing but requires improved policy to technical control mapping, formalized vulnerability lifecycle management, and clearer HR to IT evidence workflows to support audit defensibility.

It is also noted that The Client has independently identified a number of vulnerabilities and has begun addressing several of them through manual remediation efforts. While this demonstrates proactive engagement and commitment to risk reduction, formalizing these efforts under a structured Managed VMDR framework will improve prioritization, tracking consistency, and executive visibility.

To address these risks, ACME Inc should formalize a structured vulnerability management program with defined remediation timelines and elimination of end of life systems, correct and test WAN failover configurations to reduce single points of failure, enable and govern centralized monitoring and reporting, and assign documented control ownership across technical and administrative domains. Implementing centralized VMDR oversight and conducting quarterly standards reviews aligned to PCI and SOC 2 principles will materially improve resilience, audit readiness, and overall security maturity.

Conclusion

By executing the recommended actions in this report summary, ACME Inc can significantly reduce operational risk and strengthen audit readiness. These actions include formalizing a structured vulnerability management program with defined remediation timelines and elimination of end of life systems, correcting and validating WAN failover configurations to reduce single points of failure, enabling and governing centralized monitoring and reporting, and assigning documented control ownership across technical and administrative domains. Implementing centralized VMDR oversight and conducting quarterly standards reviews aligned to PCI and SOC 2 principles will materially improve resilience, compliance posture, and overall security maturity.

Remediation Path Forward

Uzado's managed services framework provides the structure, automation, and risk intelligence required to close these gaps quickly and efficiently.

By deploying Managed RMM, **Managed VMDR**, SentinelOne Managed EDR, and the Uzado mGRC Compliance Platform, The Client can establish:

- Continuous visibility, asset discovery, and vulnerability intelligence
- Centralized patching, exposure prioritization, and endpoint defense
- Documented, enforceable governance and risk management policies
- Continuous compliance alignment with PCI DSS and SOC 2 requirements

The addition of Managed VMDR ensures proactive identification, prioritization, and remediation tracking of vulnerabilities across the environment, transforming security from reactive response to measurable, risk-based control.

Next Steps

Uzado recommends initiating a joint remediation planning session to confirm priorities, responsibilities, and scheduling for all critical activities identified in this report.

Immediate focus should include, in order of priority:

1. **Remediation of Critical and Known Exploited Vulnerabilities**
   Address all critical severity findings and publicly known exploited CVEs, particularly on internet exposed or privileged systems.
2. **Elimination of End of Life Operating Systems and Unsupported Software**
   Upgrade or decommission legacy Windows versions and unsupported third party applications to remove systemic exposure.
3. **Network Resilience Hardening and WAN Failover Validation**
   Correct dual WAN configuration, test automatic failover, and eliminate identified single points of failure impacting persistent VPN connectivity.
4. **Deployment and Formalization of Managed VMDR**
   Establish continuous vulnerability discovery, risk prioritization, remediation tracking, and executive reporting.
5. **Centralized Patch Management Enforcement via Managed RMM**
   Implement structured patch cycles with documented SLAs and compliance reporting.
6. **Endpoint Detection and Response Optimization**
   Validate SentinelOne policy coverage, alert tuning, and incident response workflow.
7. **Monitoring and Logging Governance Activation**
   Enable Fortinet reporting, formalize log review cadence, and define documented alert escalation procedures.
8. **Access Control and Privileged Account Review**
   Validate least privilege enforcement, administrative group memberships, and role based access alignment.
9. **Policy to Technical Control Mapping and mGRC Documentation Alignment**
   Ensure documented policies are directly mapped to enforced technical controls and evidence artifacts.
10. **Quarterly Security and Minimum Standards Review Cadence**
    Establish recurring executive level risk review sessions aligned to PCI DSS and SOC 2 control expectations.

Project Scope

The scope includes a comprehensive review of infrastructure and network security, including Fortinet firewall configuration, VLAN and subnet segmentation, WAN redundancy and failover configuration, persistent VPN architecture, and static IP routing dependencies. Endpoint and asset management were assessed through deployment and validation of Lansweeper asset discovery, asset inventory classification, identification of unmanaged or unsupported systems, and evaluation of patch posture and endpoint configuration controls.

The engagement also covered vulnerability and risk management, including analysis of identified vulnerabilities, severity categorization, prioritization of exposure, review of end of life operating

systems, and evaluation of the organization's remediation lifecycle maturity. Identity and access management controls were reviewed across Microsoft 365 and Entra ID, including administrative privilege analysis, role based access validation, and alignment of HR onboarding and termination workflows with technical access enforcement.

Monitoring and incident detection capabilities were evaluated, including Fortinet logging configuration, alerting and escalation workflows, endpoint detection policies, and evidence retention practices. Governance and compliance alignment were reviewed through policy documentation analysis, policy to technical control mapping, evidence handling procedures, and overall alignment to PCI DSS and SOC 2 control principles.

This assessment does not constitute a full PCI DSS certification audit or SOC 2 Type 2 audit, nor does it include penetration testing, application source code review, forensic investigation, or formal incident response services. Deliverables include an executive summary, detailed risk findings with prioritized recommendations, asset and vulnerability overview, network segmentation commentary, compliance alignment analysis, and a structured remediation roadmap.

Area	Description
Infrastructure & Assets	Complete inventory of servers, endpoints, printers, VOIP, firewalls, and IoT devices via Lansweeper.
Business Processes	Review of critical workflows, documentation, and change-management maturity.
Backup & Recovery	Evaluation of tape-based strategy, frequency, and testing.
Disaster Recovery & Business Continuity	Review of planning, testing, and communication readiness.
Security & Vulnerability Management	Analysis of patch status, vulnerabilities, and endpoint protection.
Governance, Risk & Compliance (GRC)	Review of policies, risk register, awareness training, and frameworks.
Microsoft 365 / Azure Cloud	Licensing, configuration, MFA, Conditional Access, and Secure Score.
Vendor Management & PCI Data Handling	Review of ERP (CAPP) and payment workflows for compliance exposure.
IT Operations & Management	Evaluation of credentials, RMM absence, and staffing responsibilities.

Current Environment Overview

The Client operates within a hybrid infrastructure model combining on premise systems with cloud integrations and persistent VPN connectivity. Network segmentation is implemented through multiple VLANs, and a Fortinet firewall is deployed at the edge; however, WAN failover validation, centralized reporting, and formal log governance require strengthening. Asset visibility has improved with the deployment of Lansweeper, identifying 251 assets, but legacy operating systems and 1,390 active vulnerabilities, including critical and high severity findings, present elevated risk. Microsoft 365 and Entra ID provide identity management capabilities, and SentinelOne is in place for endpoint protection, though privilege governance, alert workflows, and policy to technical control mapping require further formalization. Overall, the environment reflects foundational to developing security maturity, with strong building blocks in place but requiring structured remediation and governance hardening to achieve a stable, audit defensible posture.

Category	Current State	Risk Observation	Maturity Level
Infrastructure Model	Hybrid environment, on premise infrastructure with cloud integrations and persistent VPN connectivity	Increased architectural complexity and dependency on WAN resilience	Foundational to Developing
Firewall & Edge Security	Fortinet appliance deployed	Reporting not enabled, logging governance requires formalization	Developing
Network Segmentation	Multiple VLANs and segmented subnets implemented	Segmentation present, documentation and validation testing recommended	Developing
WAN & Redundancy	Dual WAN configured but failover not fully validated	Potential single points of failure, prior fiber disruptions noted	Needs Improvement
Asset Inventory	Lansweeper deployed, 251 assets identified	Good visibility established, requires continuous governance	Developing
Operating Systems	Mix of supported and legacy Windows systems	End of life systems and unsupported software present	Needs Improvement
Vulnerability Posture	1,390 active vulnerabilities, including Critical and High severity	Elevated exposure requiring structured remediation lifecycle	Needs Improvement

Identity & Access Management	Microsoft 365 and Entra ID in use	Privilege governance and HR alignment require formal evidence handling	Developing
Endpoint Protection	SentinelOne deployed	Policy optimization and alert workflow validation recommended	Developing
Monitoring & Logging	Logging enabled at device level	Centralized reporting and formal review cadence not documented	Needs Improvement
Governance & Documentation	Policies exist in various forms	Policy to technical control mapping requires consolidation	Foundational

Identified Gaps

Governance & IT Operations

The organization demonstrates foundational governance structures, and operational maturity is beginning to improve with the addition of increased internal IT resources, including the involvement of Terry in a leadership capacity. This added oversight strengthens accountability and decision making; however, several control processes still require formalization to achieve audit defensibility and sustained maturity. While technical controls are partially in place, documentation alignment, ownership clarity, and recurring review mechanisms are not yet consistently structured.

Key gaps include:
- No formalized vulnerability remediation lifecycle with defined SLAs and reporting cadence
- Monitoring and log review responsibilities not documented with clear ownership
- HR to IT onboarding and termination workflows lack standardized evidence retention
- Policy to technical control mapping requires consolidation
- No recurring quarterly security or minimum standards review process

Security & Compliance

The current security posture reflects elevated exposure due to unresolved vulnerabilities and legacy system presence. Although tools are deployed, risk prioritization and centralized governance require strengthening to support PCI and SOC 2 alignment.

Key gaps include:
- High volume of critical and high severity vulnerabilities
- Known exploited CVEs not tracked under a documented risk based prioritization model

• End of life operating systems and unsupported third party software
• Centralized VMDR governance not fully implemented
• Inconsistent documentation alignment affecting audit defensibility

Microsoft 365 / Azure (Entra ID)

Identity and access controls are operational but require stronger governance oversight, formal review cadence, and documented evidence alignment. Administrative privileges and role assignments need structured validation to ensure least privilege enforcement.

Key gaps include:
• Privileged access reviews not formally documented
• Role based access control not fully mapped to policy enforcement
• Administrative access review cadence not established
• Access provisioning and deprovisioning evidence handling requires standardization

Network & Legacy Systems

The network architecture includes segmentation and perimeter security controls; however, resilience validation and centralized monitoring require improvement. Dependency on persistent VPN connectivity and legacy systems increases operational risk.

Key gaps include:
• Dual WAN failover configuration not fully validated
• Persistent VPN dependency without documented resilience testing
• Fortinet reporting not enabled for centralized visibility
• Logging not governed under a formal review cadence
• Legacy operating systems increasing systemic network exposure

PCI Data Handling

Although there is no current requirement for formal PCI DSS compliance, the Acme Rewards managed on behalf of customers represent significant stored value, functionally comparable to cash or credit in terms of financial impact and fraud exposure. Unauthorized access, manipulation, or theft of these points could result in financial loss, reputational damage, and customer trust erosion similar to a payment data breach.

Given this risk profile, PCI aligned control principles should be considered a best practice baseline, including:
• Strong access controls and least privilege enforcement
• Network segmentation protecting systems that manage point balances
• Continuous vulnerability management and patch enforcement
• Centralized logging and monitoring of transactional activity
• Formal incident response procedures for fraud or data manipulation events
Treating Acme Rewards infrastructure with controls comparable to payment environments materially reduces operational and financial risk, even in the absence of a formal PCI compliance mandate.

Risk Summary

The Client operates a hybrid infrastructure environment supporting systems that manage customer Acme Rewards with material stored value. While foundational security controls are in place, several structural, operational, and governance gaps elevate the organization's overall risk profile. The following summarizes the primary risk domains and associated business impact

Risk Category	Risk Description	Likelihood	Impact	Overall Risk	Business Impact	Recommended Mitigation
Vulnerability Management	High volume of Critical and High vulnerabilities, including known exploited CVEs	High	High	**Elevated**	Ransomware, system compromise, financial exposure	Deploy Managed VMDR, enforce remediation SLAs, eliminate known exploited CVEs
Legacy Systems	Presence of End of Life operating systems and unsupported software	High	High	**Elevated**	Increased exploitability, audit findings	Upgrade or decommission legacy systems
Network Resilience	Dual WAN failover not fully validated	Medium	High	**Elevated**	Full service outage due to ISP or hardware failure	Validate and test failover configuration
VPN Dependency	Persistent VPN reliance without documented resilience testing	Medium	High	**Elevated**	Operational disruption, transaction interruption	Document and test redundancy architecture
Monitoring & Logging	Fortinet reporting not enabled and no formal log review cadence	Medium	High	**Moderate to Elevated**	Delayed breach detection, forensic gaps	Enable reporting and formalize review cadence

Identity Governance	Privileged access reviews not formally documented	Medium	Medium	**Moderate**	Insider risk, excessive privilege exposure	Establish quarterly access recertification
HR to IT Workflow	Onboarding and termination evidence handling not standardized	Medium	Medium	**Moderate**	Orphaned accounts, access control gaps	Formalize workflow and documentation
Governance Alignment	Policy to technical control mapping incomplete	Medium	Medium	**Moderate**	Reduced audit defensibility	Map policies to enforced controls in mGRC platform
Acme Rewards Fraud Exposure	Points represent stored value similar to cash without PCI-aligned safeguards	Medium	High	**Elevated**	Financial loss, reputational damage	Apply PCI-aligned controls and monitoring
Executive Risk Visibility	No centralized executive risk dashboard or quarterly review cadence	Medium	Medium	**Moderate**	Reactive decision making	Establish recurring executive security review

Risk Definitions & Rating Methodology

This assessment applies a qualitative risk rating model based on the evaluation of **Likelihood** and **Impact**. Each identified risk was assessed using professional judgment, observed technical evidence, environmental exposure, and business context.

Likelihood

Likelihood reflects the probability that a risk event could occur within the current environment based on factors such as exploitability, exposure, historical incidents, and control maturity.

- **High** – Actively exploitable, externally exposed, or lacking effective mitigating controls
- **Medium** – Exploitable under certain conditions or partially mitigated by existing controls
- **Low** – Limited exposure with strong compensating controls in place

Impact

Impact reflects the potential business consequence if the risk were realized. Impact considerations include operational disruption, financial loss, regulatory implications, reputational damage, and customer trust impact.

- **High** – Significant operational outage, material financial loss, major reputational damage, or regulatory exposure
- **Medium** – Measurable disruption or financial impact with manageable recovery
- **Low** – Limited operational or financial consequence

Overall Risk Rating

Overall Risk is determined by combining Likelihood and Impact using professional risk evaluation principles. Risks classified as **Elevated** or **Moderate to Elevated** represent conditions requiring prioritized remediation due to either active exposure, material business impact, or both.

This model is designed to support executive decision making, remediation prioritization, and alignment with PCI DSS and SOC 2 risk evaluation expectations.

Current overall risk posture is assessed as **Moderate to Elevated**, primarily driven by vulnerability exposure, WAN resilience gaps, and incomplete monitoring governance. Foundational controls are present and the addition of increased IT leadership resources strengthens forward trajectory; however, structured remediation, centralized risk visibility, and formalized governance processes are required to materially reduce residual risk.

Recommendations

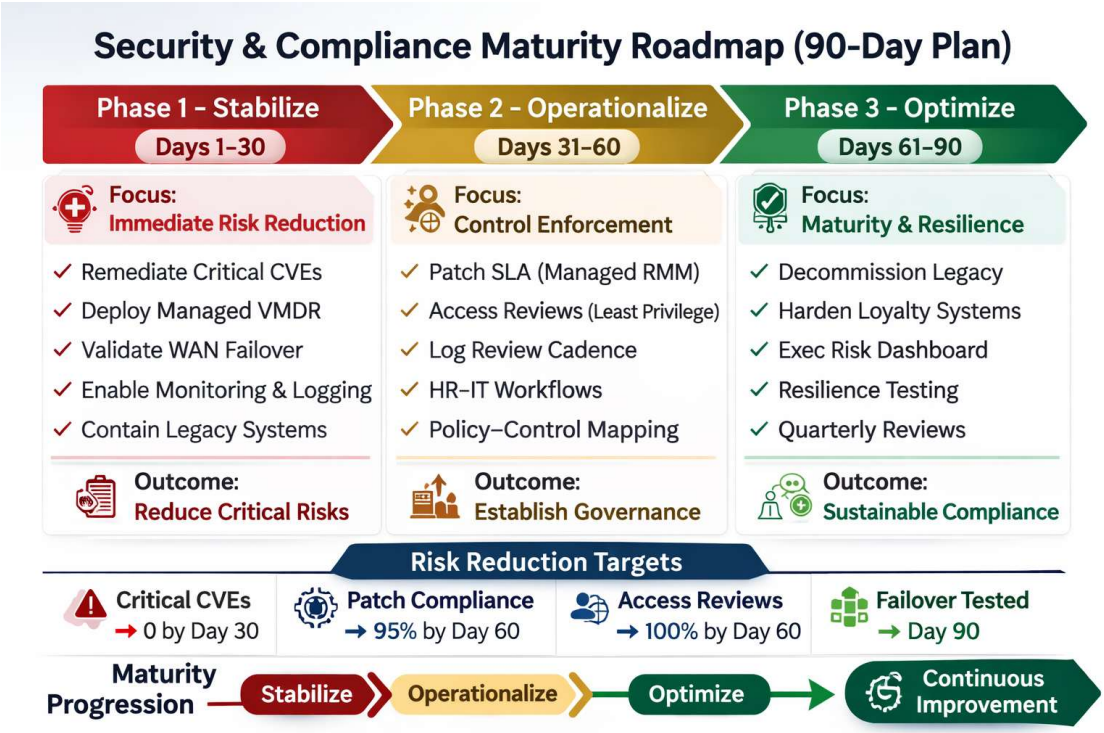
Uzado recommends prioritizing the deployment of its Managed VMDR service as the foundational control layer for risk reduction and security maturity improvement. Managed VMDR provides continuous asset discovery, vulnerability identification, risk based prioritization, remediation tracking, and executive level reporting, transforming vulnerability management from reactive patching into a structured, measurable program. By centralizing exposure visibility across servers, endpoints, and network assets, The Client can immediately identify critical and known exploited vulnerabilities, enforce defined remediation timelines, and demonstrate documented risk reduction aligned to PCI and SOC 2 principles. Managed VMDR also integrates with patch management and endpoint security controls, creating a unified feedback loop between detection, remediation, and governance reporting, thereby accelerating risk stabilization within the 90 day execution window and establishing a sustainable long term security baseline.

90-Day Security & Governance Execution Plan

Timeframe	Focus Area	Key Actions	Objective	Expected Outcome	Owner Type
Days 1–30	Critical Vulnerability Remediation	Remediate all Critical and Known Exploited CVEs	Immediate risk stabilization	Significant reduction in active exploitation exposure	IT + Managed VMDR
Days 1–30	Deploy Managed VMDR	Enable continuous scanning, prioritization, and reporting	Establish centralized vulnerability governance	Real-time risk visibility and tracking	Managed Services
Days 1–30	Legacy System Containment	Identify, isolate, or restrict unsupported systems	Reduce systemic exposure	Lower attack surface while upgrade planning begins	IT
Days 1–30	WAN & Failover Validation	Correct and test dual WAN automatic failover	Eliminate single points of failure	Validated network resilience	Network Team
Days 1–30	Enable Fortinet Reporting	Activate logging, alert dashboards, and reporting exports	Improve detection capability	Centralized monitoring visibility	Security Team
Days 31–60	Patch Governance Enforcement	Implement structured patch SLAs via Managed RMM	Formalize remediation lifecycle	Measurable patch compliance	IT + Managed RMM
Days 31–60	Privileged Access Review	Conduct documented admin and role-based access review	Enforce least privilege	Reduced insider and escalation risk	IT + Leadership

Days 31–60	Log Review Cadence	Establish weekly and monthly documented log reviews	Strengthen monitoring governance	Improved incident detection defensibility	Security Team
Days 31–60	HR–IT Workflow Standardization	Formalize onboarding and termination access controls	Close access lifecycle gaps	Reduced orphaned account risk	HR + IT
Days 31–60	Policy-to-Control Mapping	Align policies within mGRC platform to enforced technical controls	Improve audit defensibility	Documented control traceability	Compliance
Days 61–90	Legacy System Remediation	Upgrade or decommission end-of-life systems	Long-term exposure reduction	Sustainable security baseline	IT
Days 61–90	Acme Rewards System Hardening	Apply PCI-aligned safeguards to point management systems	Protect stored value assets	Reduced fraud and financial manipulation risk	Security + Dev
Days 61–90	Executive Risk Dashboard	Deploy centralized executive reporting	Improve leadership risk visibility	Data-driven decision making	Compliance
Days 61–90	Resilience Simulation	Conduct controlled WAN and VPN failover test	Validate continuity planning	Confirmed operational resilience	Network Team
Days 61–90	Launch Quarterly Governance Review	Establish recurring executive security review cadence	Institutionalize oversight	Sustainable governance maturity	Leadership

90 Day Execution Summary



By Day 90, The Client should have materially reduced critical exposure, validated network resilience, operationalized Managed VMDR governance, formalized access and monitoring controls, and established an executive-level security oversight cadence aligned to PCI and SOC 2 principles.

Maturity Beyond 90 Days

Beyond the initial 90 day stabilization period, the focus should shift from reactive risk reduction to structured operational maturity and strategic optimization. This phase emphasizes embedding governance into routine operations, strengthening control automation, and institutionalizing executive oversight. Priorities should include full legacy system remediation, advanced threat detection integration, expanded resilience testing including recovery simulations, and the establishment of measurable security KPIs tied to leadership reporting. Additionally, ongoing policy refinement, third party risk management formalization, and periodic access recertification should become standardized processes. The objective beyond 90 days is to transition from foundational control implementation to a sustainable, continuously improving security program aligned to PCI and SOC 2 expectations, ultimately achieving an optimized, audit ready posture with predictable risk governance.

Workstream Grouping

While the workstreams below are grouped by logical phases for prioritization and clarity, parallel execution may be limited due to current resource constraints. Sequencing and pacing may need to be adjusted based on available internal capacity, with some initiatives executed serially rather than concurrently.

Managed Services Alignment

Service	Function	Outcome
Managed RMM & Lansweeper Integration	Asset visibility, patch automation	Central control & accountability
Managed EDR (SentinelOne)	Endpoint protection & response	Reduced incident impact
mGRC Platform	Policy, risk & evidence management	Compliance readiness (SOC 2/PCI)
Microsoft 365 / Intune Hardening	Identity & device security	Cloud posture improvement
Security Awareness (KnowBe4)	Phishing simulations & training	Improved user behavior
vCISO Oversight	Strategic governance leadership	Continuous improvement & reporting

Uzado's managed services model is designed to align operational execution with governance maturity, ensuring that security controls are not only implemented but continuously monitored, measured, and improved. Through the integration of Managed VMDR, Managed RMM, SentinelOne Managed EDR, and the Uzado mGRC compliance platform, technical enforcement is directly connected to policy oversight and executive reporting. This alignment reduces manual effort, increases consistency in remediation and patch governance, and provides structured accountability across infrastructure, identity, and monitoring domains. By consolidating risk visibility, remediation tracking, and compliance documentation under a unified managed framework, The Client can transition from reactive issue resolution to proactive, risk based security management that supports both operational resilience and long term compliance objectives.

Condensed Report Summary

The Client operates a hybrid infrastructure environment supporting systems that manage customer Acme Rewards representing significant stored value. While foundational security controls are in place, the current posture reflects moderate to elevated risk driven by unresolved critical vulnerabilities, legacy operating systems, incomplete monitoring governance, and unvalidated WAN failover resilience. Identity and access controls within Microsoft 365 and Entra ID are operational but require stronger documentation, privilege review cadence, and formalized HR-to-IT lifecycle alignment to ensure audit defensibility.

Key priorities include immediate remediation of critical and known exploited vulnerabilities, elimination or containment of unsupported systems, validation of network failover capabilities, activation of centralized monitoring and reporting, and formal deployment of Managed VMDR to establish structured vulnerability governance. Strengthening privileged access controls, documenting log review cadence, and consolidating policy-to-technical control mapping will materially improve compliance alignment with PCI and SOC 2 principles.

Although a 90-day execution plan has been defined, workstream parallelization may be limited due to current resource constraints. As additional IT leadership resources are introduced, including strengthened oversight capacity, execution velocity and governance maturity are expected to improve. By executing the recommended actions, The Client can significantly reduce operational risk, enhance resilience, and establish a sustainable, audit-ready security framework.

AI-Assisted Content Disclosure

Portions of this report were prepared with the assistance of artificial intelligence (AI) tools to enhance clarity, consistency, and efficiency in drafting. All findings, interpretations, and recommendations were reviewed, validated, and approved by **Ken Dobson, vCISO – Uzado Inc.** to ensure technical accuracy and alignment with the **SOC2/PCI** and Uzado's professional standards.

If you have any questions regarding this report or the associated remediation plan, please contact **Ken Dobson** at your earliest convenience for clarification or next-step coordination.

Ken Dobson | vCISO

e: kdobson@uzado.com | **w:** www.uzado.com
p: 647-847-4660 ext 100 | **m:** 519-757-7291
a: 95 Mural Street, Richmond Hill | ON L4B 3G2 Canada