Risk ID	Asset ID	Risk Description
R-001	AST-001	Unauthorized Access to Active Directory
R-002	AST-002, AST-003	Data Breach / Data Loss
R-003	AST-002, AST-005	Undetected Cyber Attack
R-004	AST-001	Lack of Cybersecurity Governance
R-005	AST-014	Supply Chain Attack
R-006	AST-001, AST-008	Weak Remote Access Security
R-007	AST-006	Vulnerability Exploitation
R-008	All Systems	Ineffective Incident Response
R-009	AST-002, AST-003	Lack of Data Protection Controls
R-010	AST-010	Configuration Drift
R-011	AST-009	Insufficient Security Awareness
R-012	All Systems	Inadequate Audit Logging

Threat	Vulnerability	Impact (1-3)
Credential compromise, insider threat, external attack	No MFA implemented, shared admin passwords, no PAM	3
External attack, insider threat, ransomware	No DLP solution, no data classification, no encryption policy	3
APT, malware, lateral movement, exfiltration	No SIEM, no centralized logging, no SOC, limited monitoring	3
Strategic misalignment, compliance failures	No cybersecurity strategy, no information security policy, roles undefined	2
Third-party compromise, vendor breach	No TPRM process, no vendor security assessments, no contract security clauses	2
Compromised remote access, VPN exploitation	No MFA for VPN, contractor access not managed, no network access control	3
Exploit of known vulnerabilities, zero-day attacks	Ad-hoc vulnerability scanning, no formal VM program, high/severe vulns unresolved	3
Delayed detection, inadequate containment	No incident response plan, no IR team, no runbooks, no 24/7 coverage	2
Unauthorized data access, data leakage	No data classification, USB drives allowed, no removable media policy	2
Unauthorized changes, misconfigurations	No change management process, no configuration baselines	2
Phishing attacks, social engineering	Basic training only, no phishing simulations, no ongoing awareness	2
Undetected malicious activity, no forensics	Logs not reviewed, no centralized logging, no retention policy	2

Likelihood (1-3)	Risk Score	Risk Level	Business Impact
3	9	High	Complete system compromise, unauthorized access to all resources
3	9	High	Loss of sensitive data, regulatory fines, reputational damage
3	9	High	Prolonged breach, extensive data loss, system compromise
3	6	High	Regulatory non-compliance, ineffective security program, board liability
3	6	High	Breach via trusted vendor, data exposure, service disruption
2	6	High	Unauthorized remote access, lateral movement from compromised accounts
2	6	High	System compromise, privilege escalation, data breach
3	6	High	Extended dwell time, ineffective containment, regulatory reporting failures
2	4	Medium	Sensitive data exfiltration, USB-based malware, intellectual property theft
2	4	Medium	System instability, security vulnerabilities, compliance failures
2	4	Medium	Successful phishing, credential compromise, malware infection
2	4	Medium	Inability to investigate incidents, compliance failures, no accountability

Mitigation Strategy	NIST Controls	Status
Implement MFA, deploy PAM solution, eliminate shared accounts	IA-2, IA-2(1), AC-2, AC-6	Open
Implement DLP, classify data, deploy encryption, establish data governance	SC-28, MP-6, SC-13, SI-12	Open
Deploy SIEM, implement centralized logging, establish 24/7 monitoring	AU-2, AU-6, SI-4, IR-5	Open
Develop cybersecurity strategy, create infosec policy, define roles and responsibilities	PL-1, PL-2, PL-8, PM-1	Open
Establish TPRM program, conduct vendor assessments, update contracts	SR-2, SR-3, SA-9	Open
Implement MFA for VPN, manage contractor access, deploy NAC	AC-17, IA-2(1), AC-20	Open
Establish formal VM program, remediate critical vulns, regular scanning	RA-5, SI-2	Open
Develop IR plan, establish IR team, create runbooks, conduct tabletop exercises	IR-1, IR-4, IR-8	Open
Classify data, restrict USB usage, implement removable media controls	MP-3, MP-7, SC-28	Open
Implement change management, establish configuration baselines, automate compliance	CM-2, CM-3, CM-6	Open
Enhance training, conduct phishing simulations, quarterly awareness campaigns	AT-2, AT-3	Open
Centralize logging, implement log review process, define retention	AU-2, AU-3, AU-6, AU-12	Open

Risk Owner	Target Date
IT Manager	2026-02-15
IT Manager	2026-03-31
IT Manager	2026-04-30
CISO / IT Manager	2026-03-15
Procurement Manager	2026-06-30
Network Team Leader	2026-03-31
IT Manager	2026-02-28
IT Manager	2026-04-15
IT Manager	2026-05-31
IT Manager	2026-05-15
HR Manager	2026-03-31
IT Manager	2026-04-30