Rec ID	Risk ID	Recommendation
REC-001	R-001	Deploy Multi-Factor Authentication (MFA)
REC-002	R-004	Develop Information Security Policy Framework
REC-003	R-001	Eliminate Shared Admin Accounts and Deploy PAM
REC-004	R-007	Establish Formal Vulnerability Management Program
REC-005	R-012	Implement Centralized Logging
REC-006	R-003	Deploy SIEM and Security Monitoring
REC-007	R-008	Develop and Implement Incident Response Plan
REC-008	R-006	Enhance Remote Access Security
REC-009	R-011	Enhance Security Awareness Training
REC-010	R-012	Implement Log Review and Monitoring Procedures
REC-011	R-002	Implement Data Classification and Governance Program
REC-012	R-002	Deploy Data Loss Prevention (DLP) Solution
REC-013	R-005	Establish Third-Party Risk Management Program
REC-014	R-010	Implement Change Management Process
REC-015	R-009	Implement Removable Media Controls
REC-016	R-004	Establish Cyber Risk Assessment Program
REC-017	R-010	Extend Asset Inventory to Complete CMDB
REC-018	R-002	Implement Encryption Key Management
REC-019	R-003	Establish SOC or MSSP Partnership
REC-020	R-008	Conduct Cyber Crisis Simulation Exercise

Description	NIST Controls	Priority
Implement MFA for all users starting with privileged accounts, VPN, and cloud services (Azure AD, O365)	IA-2(1), AC-2	Critical
Create comprehensive information security policy, define cybersecurity strategy, establish governance structure	PL-1, PL-2, PL-8	Critical
Implement privileged access management solution, create individual admin accounts, establish privileged access reviews	AC-2, AC-6, IA-5	Critical
Formalize Qualys usage, define scanning schedules, create remediation SLAs, prioritize critical vulnerabilities	RA-5, SI-2	High
Deploy centralized logging solution, onboard critical systems, establish log retention policy	AU-2, AU-3, AU-12	High
Implement SIEM solution (e.g., Microsoft Sentinel), onboard critical systems, create detection use cases	SI-4, AU-6, IR-5	Critical
Create comprehensive IR plan, establish IR team, develop runbooks, conduct tabletop exercises	IR-1, IR-4, IR-8	Critical
Implement MFA for VPN (if not in Phase 1), establish contractor access management, deploy network access control	AC-17, IA-2(1), AC-20	High
Implement phishing simulation platform, create role-based training, establish quarterly awareness campaigns	AT-2, AT-3	Medium
Establish log review schedules, create monitoring dashboards, define alerting thresholds	AU-6	High
Conduct data discovery, implement classification scheme, label data, establish data governance policies	SI-12, MP-3	Critical
Implement DLP for O365, email, and endpoints, configure policies based on data classification	SC-28, MP-6	Critical
Create TPRM framework, develop vendor assessment questionnaires, update contracts with security clauses	SR-1, SR-2, SR-3	High
Develop change management procedures, implement approval workflows, establish change advisory board	CM-3, CM-6	Medium
Develop removable media policy, restrict USB usage, implement USB monitoring and DLP for removable media	MP-1, MP-7	Medium
Develop risk assessment methodology, conduct organization-wide cyber risk assessment, establish annual cadence	RA-1, RA-3	High
Inventory all software, SaaS applications, cloud resources, and third-party vendors in CMDB	CM-8	Medium
Develop encryption policy, implement key management procedures, document encryption usage	SC-12, SC-13	Medium
Evaluate build vs. buy for SOC, establish 24/7 monitoring capability, hire or partner for security operations	SI-4, IR-5, AU-6	High
Plan and execute full-scale cyber crisis simulation, test IR plan, engage executive leadership	IR-3, CP-4	Medium

Timeline	Phase	Est. Cost (USD)	Owner	Status
0-3 months	Phase 1: Quick Wins	75000	IT Manager	Not Started
0-3 months	Phase 1: Quick Wins	50000	CISO / IT Manager	Not Started
0-3 months	Phase 1: Quick Wins	100000	IT Manager	Not Started
0-3 months	Phase 1: Quick Wins	25000	IT Manager	Not Started
0-3 months	Phase 1: Quick Wins	50000	IT Manager	Not Started
3-6 months	Phase 2: Detection & Response	200000	IT Manager	Not Started
3-6 months	Phase 2: Detection & Response	75000	CISO / IT Manager	Not Started
3-6 months	Phase 2: Detection & Response	80000	Network Team Leader	Not Started
3-6 months	Phase 2: Detection & Response	40000	HR Manager / CISO	Not Started
3-6 months	Phase 2: Detection & Response	30000	IT Manager	Not Started
6-9 months	Phase 3: Data Protection	120000	Data Protection Officer	Not Started
6-9 months	Phase 3: Data Protection	150000	IT Manager	Not Started
6-9 months	Phase 3: Data Protection	60000	Procurement Manager	Not Started
6-9 months	Phase 3: Data Protection	40000	IT Manager	Not Started
6-9 months	Phase 3: Data Protection	35000	IT Manager	Not Started
9-12 months	Phase 4: Continuous Improvement	80000	CISO / Risk Manager	Not Started
9-12 months	Phase 4: Continuous Improvement	50000	IT Manager	Not Started
9-12 months	Phase 4: Continuous Improvement	60000	IT Manager	Not Started
9-12 months	Phase 4: Continuous Improvement	250000	CISO / IT Manager	Not Started
9-12 months	Phase 4: Continuous Improvement	45000	CISO	Not Started

Business Justification
Immediate risk reduction for credential compromise
Foundation for entire security program
Accountability and control over privileged access
Reduce attack surface from known vulnerabilities
Foundation for monitoring and forensics
Visibility into security events and threat detection
Effective incident handling and containment
Secure remote access controls
Reduce human error and improve security culture
Proactive threat detection and compliance
Foundation for data protection and compliance
Prevent unauthorized data exfiltration
Manage supply chain security risks
Control configuration changes and reduce risk
Prevent data exfiltration via removable media
Risk-based decision making and resource allocation
Complete visibility into organizational assets
Proper cryptographic controls and key lifecycle
24/7 threat detection and incident response
Validate readiness and improve response capability