Risk ID	NIST Family	NIST Control ID	Control Name
R-001	AC	AC-1	Access Control Policy and Procedures
R-001	AC	AC-2	Account Management
R-001	AC	AC-6	Least Privilege
R-006	AC	AC-17	Remote Access
R-005	AC	AC-20	Use of External Systems
R-001	IA	IA-1	Identification and Authentication Policy
R-001	IA	IA-2	Identification and Authentication
R-001	IA	IA-2(1)	Multi-Factor Authentication (MFA)
R-001	IA	IA-5	Authenticator Management
R-012	AU	AU-1	Audit and Accountability Policy
R-003	AU	AU-2	Event Logging
R-012	AU	AU-3	Content of Audit Records
R-003	AU	AU-6	Audit Review, Analysis, and Reporting
R-012	AU	AU-12	Audit Record Generation
R-010	CM	CM-1	Configuration Management Policy
R-010	CM	CM-2	Baseline Configuration
R-010	CM	CM-3	Configuration Change Control
R-010	CM	CM-6	Configuration Settings
R-010	CM	CM-8	System Component Inventory
R-008	CP	CP-1	Contingency Planning Policy
R-008	CP	CP-2	Contingency Plan
R-008	CP	CP-9	System Backup
R-008	IR	IR-1	Incident Response Policy and Procedures
R-008	IR	IR-4	Incident Handling
R-003	IR	IR-5	Incident Monitoring
R-008	IR	IR-8	Incident Response Plan
R-009	MP	MP-1	Media Protection Policy
R-002	MP	MP-6	Media Sanitization
R-011	PE	PE-1	Physical and Environmental Protection Policy
R-011	PE	PE-2	Physical Access Authorizations
R-011	PE	PE-3	Physical Access Control
R-011	PE	PE-6	Monitoring Physical Access
R-004	PL	PL-1	Security Planning Policy
R-004	PL	PL-2	System Security Plan
R-004	PL	PL-8	Security Architecture
R-004	RA	RA-1	Risk Assessment Policy
R-004	RA	RA-3	Risk Assessment
R-007	RA	RA-5	Vulnerability Scanning
R-002	SC	SC-7	Boundary Protection
R-002	SC	SC-8	Transmission Confidentiality and Integrity
R-002	SC	SC-12	Cryptographic Key Management

R-002	SC	SC-13	Cryptographic Protection
R-002	SC	SC-28	Protection of Information at Rest
R-007	SI	SI-2	Flaw Remediation
R-007	SI	SI-3	Malicious Code Protection
R-003	SI	SI-4	System Monitoring
R-005	SR	SR-1	Supply Chain Risk Management Policy
R-005	SR	SR-2	Supply Chain Risk Management Plan
R-005	SR	SR-3	Supply Chain Controls and Processes
R-011	AT	AT-1	Awareness and Training Policy
R-011	AT	AT-2	Security Awareness Training

Implementation Status	Current State / Evidence
Not Implemented	No formal access control policy exists
Partially Implemented	Active Directory exists but lacks RBAC, access reviews, and formal approval process
Not Implemented	Least privilege not enforced, access granted upon request
Partially Implemented	VPN exists but no MFA, contractor access not managed
Not Implemented	Third-party system access not controlled or monitored
Not Implemented	No authentication policy defined
Partially Implemented	Basic authentication via AD but weak controls
Not Implemented	MFA not implemented for any users or systems
Partially Implemented	Complex passwords required but admin passwords shared
Not Implemented	No audit policy defined
Partially Implemented	Basic logging exists but not comprehensive
Partially Implemented	Logs captured but content not standardized
Not Implemented	Logs not reviewed or analyzed
Partially Implemented	Some systems generate logs, not centralized
Not Implemented	No configuration management policy
Partially Implemented	SOE exists for laptops only
Not Implemented	No formal change management process
Partially Implemented	SOE provides baseline for Windows desktops
Partially Implemented	Hardware inventory exists, software not inventoried
Partially Implemented	DR plans exist but not comprehensive cybersecurity IR
Implemented	BC/DR plans in place and tested
Implemented	Regular backups conducted and tested
Not Implemented	No cybersecurity incident response policy
Not Implemented	No formal incident handling capability
Not Implemented	No incident monitoring or tracking
Not Implemented	No cybersecurity incident response plan
Not Implemented	No media protection or removable media policy
Not Implemented	No data disposal or sanitization procedures
Implemented	Physical security policy exists and enforced
Implemented	Extensive employee vetting and authorization
Implemented	State-of-the-art physical access controls
Implemented	24/7 CCTV monitoring for labs and facilities
Not Implemented	No information security planning policy
Not Implemented	No system security plans documented
Not Implemented	No security architecture defined
Not Implemented	No cybersecurity risk assessment policy
Not Implemented	No cyber risk assessments conducted
Partially Implemented	Qualys exists but used ad-hoc
Implemented	Palo Alto NGFWs provide boundary protection
Implemented	Data in transit encrypted by default
Not Implemented	No encryption key management program

Partially Implemented	Default encryption in O365/Azure, no policy
Partially Implemented	Encryption at rest in cloud, no DLP
Partially Implemented	No formal patch management program
Implemented	Microsoft Defender deployed
Not Implemented	No SIEM or comprehensive monitoring
Not Implemented	No TPRM policy
Not Implemented	No TPRM plan or program
Not Implemented	No vendor security assessment process
Partially Implemented	Basic training exists, needs enhancement
Partially Implemented	Induction training only, no ongoing program