Risk ID	NIST Control ID	Control Name
R-001	IA-2(1)	Multi-Factor Authentication
R-003	SI-4	System Monitoring
R-008	IR-4	Incident Handling
R-004	PL-2	System Security Plan
R-005	SR-3	Supply Chain Risk Management
R-002	SC-28	Protection of Information at Rest
R-007	RA-5	Vulnerability Scanning
R-012	AU-6	Audit Review, Analysis, and Reporting
R-001	AC-2	Account Management
R-001	AC-6	Least Privilege
R-006	AC-17	Remote Access
R-010	CM-3	Configuration Change Control
R-009	MP-6	Media Sanitization
R-011	AT-2	Security Awareness Training
N/A	CP-9	System Backup
N/A	PE-6	Monitoring Physical Access
N/A	SI-3	Malicious Code Protection
N/A	SC-7	Boundary Protection
R-010	CM-2	Baseline Configuration
R-002	SC-13	Cryptographic Protection

Current State	Implementation Status
MFA not configured for any users or systems	Not Implemented
No SIEM or centralized monitoring capability	Not Implemented
No formal incident handling capability	Not Implemented
No formal cybersecurity strategy or security plans	Not Implemented
No vendor security assessment framework	Not Implemented
No data classification or DLP	Not Implemented
Ad-hoc scanning, no formal VM program	Partially Implemented
Logs not reviewed or analyzed	Not Implemented
Weak account management practices	Partially Implemented
Least privilege not enforced	Not Implemented
VPN lacks MFA, contractor access not managed	Partially Implemented
No formal change management process	Not Implemented
No data disposal procedures	Not Implemented
Basic induction training only	Partially Implemented
Regular backups conducted and tested	Implemented
24/7 physical security monitoring	Implemented
Antivirus deployed	Implemented
Firewalls configured and maintained	Implemented
SOE for laptops only	Partially Implemented
Default encryption, no policy	Partially Implemented

Evidence / Observations
No MFA deployment observed. Users authenticate with username/password only.
No SIEM solution. Limited to antivirus alerts from Microsoft Defender.
Cybersecurity analyst responds ad-hoc. No documented procedures or runbooks.
Only generic IT policy exists. No information security strategy or system security plans.
Contracts reviewed by procurement/finance only. No cybersecurity vendor assessments.
Data encrypted by default in O365/Azure. No DLP, classification, or governance.
Qualys purchased but used ad-hoc. Large number of high/severe vulnerabilities unresolved.
Logs generated but no review process. No centralized log management.
Active Directory exists. No RBAC, no access reviews, shared admin passwords, no approval workflow.
Access granted upon request without formal approval. No least privilege enforcement or reviews.
VPN solution exists. No MFA for VPN. Contractor remote access not controlled.
No documented change management or change control procedures.
No documented data disposal or media sanitization procedures.
Induction training includes basic cybersecurity. No ongoing training or phishing simulations.
IT team takes regular backups. Backups tested periodically.
State-of-the-art CCTV, 24/7 monitoring for labs and facilities.
Microsoft Defender deployed across endpoints. IT team responds to alerts.
Palo Alto Next Gen Firewalls configured, audited annually, regularly updated.
SOE images all laptops with latest Windows. No baselines for servers or cloud resources.
Encryption by default in O365/Azure. No encryption policy or key management.

Recommendations
Deploy MFA for all users (O365, Azure AD, VPN). Start with privileged accounts.
Deploy SIEM (e.g., Sentinel, Splunk). Onboard all critical systems and applications.
Develop incident response plan, establish IR team, create runbooks and playbooks.
Develop organizational cybersecurity strategy and system-specific security plans.
Establish TPRM program with vendor assessment questionnaires and security requirements.
Implement data classification program, deploy DLP solution, establish data governance.
Establish formal vulnerability management program with regular scanning and remediation SLAs.
Implement log review procedures, deploy centralized logging, define review frequency.
Implement RBAC, conduct quarterly access reviews, eliminate shared accounts, establish approval process.
Implement least privilege model, conduct privilege reviews, remove excessive permissions.
Implement MFA for VPN, establish contractor access management procedures.
Implement change management process with approvals, documentation, and testing.
Develop and implement media sanitization and data disposal procedures.
Enhance training program with annual refreshers, phishing simulations, role-based training.
Continue current backup practices. Document backup procedures.
Maintain current physical security controls.
Consider enhanced endpoint protection (EDR). Ensure coverage on all endpoints.
Continue current firewall practices. Consider IPS/IDS capabilities.
Extend baseline configurations to all systems including cloud infrastructure.
Develop encryption policy, implement key management procedures.