Risk ID	Control Area	Required State (NIST)
R-001	Identity and Access Management	MFA enforced for all users and privileged accounts
R-003	Security Monitoring and Detection	SIEM deployed with centralized logging and 24/7 monitoring
R-008	Incident Response	Documented IR plan with defined roles, procedures, and 24/7 coverage
R-004	Governance and Strategy	Cybersecurity strategy defined, roles assigned, board oversight
R-002	Data Protection	Data classified, DLP deployed, encryption policy implemented
R-005	Third-Party Risk Management	Vendor security assessment framework with contract security clauses
R-001	Privileged Access Management	PAM solution deployed, no shared admin accounts
R-007	Vulnerability Management	Formal VM program with regular scanning and remediation SLAs
R-006	Remote Access Security	MFA for VPN, contractor access management, NAC deployed
R-012	Audit Logging and Review	Centralized logging with regular review and retention policy
R-010	Change Management	Formal change management process with approvals and documentation
R-009	Removable Media Controls	USB restrictions enforced, removable media policy implemented
R-011	Security Awareness	Ongoing training program with phishing simulations and role-based training
R-010	Asset Inventory	Complete CMDB including hardware, software, cloud resources, and vendors
R-004	Risk Assessment	Regular cyber risk assessments with documented methodology

Current State (Oscorp)	Gap Severity
No MFA implementation	Critical
No SIEM, no centralized logging, limited to AV alerts	Critical
No IR plan, ad-hoc response only	Critical
No cybersecurity strategy, roles undefined, no board visibility	Critical
No data classification, no DLP, no encryption policy	Critical
No TPRM process, no vendor assessments	High
Shared admin passwords, no PAM solution	High
Ad-hoc scanning, large number of unresolved critical vulnerabilities	High
No MFA for VPN, contractor access unmanaged	High
Logs not reviewed, no centralized logging, no retention policy	High
No change management process	Medium
USB drives allowed without restriction	Medium
Induction training only, no ongoing program	Medium
Hardware inventory exists, software and vendors not tracked	Medium
No cyber risk assessments conducted	Medium

Impact of Gap	Related NIST Controls
Complete absence of MFA creates significant risk of credential compromise	IA-2(1), AC-2
Cannot detect attacks, no visibility into security events, extended dwell time	SI-4, AU-2, AU-6, IR-5
Ineffective incident containment, regulatory reporting failures, extended impact	IR-1, IR-4, IR-8
Strategic misalignment, ineffective security program, compliance failures	PL-1, PL-2, PL-8, PM-1
Data loss risk, regulatory non-compliance, inability to protect sensitive information	SC-28, SI-12, MP-6
Supply chain attack risk, vendor-introduced vulnerabilities, no visibility into vendor security	SR-1, SR-2, SR-3
Privileged account compromise, no accountability, lateral movement risk	AC-2, AC-6, IA-5
Exploitation of known vulnerabilities, system compromise, data breach	RA-5, SI-2
Compromised remote access, unauthorized entry point, lateral movement	AC-17, IA-2(1)
Inability to detect malicious activity, forensics limitations, compliance failures	AU-2, AU-3, AU-6, AU-12
Configuration drift, unauthorized changes, system instability	CM-3, CM-6
Data exfiltration via USB, USB-based malware introduction	MP-1, MP-7
Successful phishing attacks, weak security culture, human error	AT-2, AT-3
Unknown assets, shadow IT, incomplete risk assessment	CM-8
Unknown risk landscape, inability to prioritize security investments	RA-1, RA-3

Remediation Actions
Deploy MFA for all users, starting with privileged accounts and VPN access
Deploy SIEM solution, onboard critical systems, establish SOC or MSSP partnership
Develop comprehensive IR plan, establish IR team, create runbooks, conduct tabletop exercises
Develop organizational cybersecurity strategy and roadmap, define roles and responsibilities
Implement data classification program, deploy DLP solution, establish data governance
Establish TPRM program, create vendor assessment questionnaire, update contracts
Deploy PAM solution, eliminate shared admin accounts, implement privileged access reviews
Establish formal vulnerability management program with defined SLAs and remediation workflows
Implement MFA for VPN, establish contractor access management procedures
Implement centralized logging, establish log review procedures, define retention policy
Implement change management process with approval workflows and documentation
Develop removable media policy, restrict USB usage, implement USB monitoring
Enhance training with annual refreshers, phishing simulations, role-based modules
Extend asset inventory to include all software, SaaS applications, and third-party vendors
Establish cyber risk assessment program with defined methodology and annual frequency