OSCORP INDUSTRIES

Comprehensive Cybersecurity GRC Assessment Report

Assessment Framework: NIST SP 800-53 Revision 5
Evaluation Methodology: Custom NIST Framework developed for this project
Prepared by: Nirmay Soni
Role: GRC Analyst & Cybersecurity Consultant
Date: January 30, 2026

Table of Contents

Executive Summary

Assessment Overview

This comprehensive Governance, Risk, and Compliance (GRC) assessment was conducted for Oscorp Industries using a **custom-developed NIST SP 800-53 Revision 5 framework**. The evaluation framework was specifically designed for this project to provide a structured, risk-based assessment of Oscorp's cybersecurity posture aligned with industry best practices and federal security standards.

The assessment evaluated Oscorp's current security controls, identified critical vulnerabilities, assessed governance maturity, and developed a prioritized remediation roadmap to strengthen the organization's cybersecurity resilience.

Key Findings Summary

Critical Risks Identified: 12 cybersecurity risks assessed, with 8 classified as High risk (67%) and 4 as Medium risk (33%). Primary risk areas include weak authentication mechanisms, absence of centralized security monitoring, lack of formal cybersecurity governance, inadequate data protection controls, and unmanaged third-party vendor risks.

NIST Control Implementation Status: Of the 51 NIST SP 800-53 controls evaluated across 15 control families, only 22% are fully implemented, 27% are partially implemented, and 51% are not implemented. This indicates significant security maturity gaps requiring immediate attention.

Policy and Governance Gaps: 15 of 17 critical security policies are either missing or inadequately defined. Only Business Continuity/Disaster Recovery and Physical Security policies are properly implemented.

Business Impact: The identified gaps expose Oscorp to elevated risks of unauthorized access, data breaches, operational disruptions, extended incident dwell time, regulatory non-compliance, and reputational damage. Without remediation, the organization faces potential financial losses, customer trust erosion, and regulatory penalties.

Investment Required: A 12-month phased remediation program requiring total investment of **$1,615,000** across four implementation phases will address critical gaps and achieve **75%+ NIST Cybersecurity Framework maturity**.

Strategic Recommendations

1. **Immediate Priority (0-3 months):** Deploy Multi-Factor Authentication (MFA), implement Privileged Access Management (PAM), develop comprehensive information security policy framework, and establish formal vulnerability management program.

2. **Detection & Response (3-6 months):** Deploy Security Information and Event Management (SIEM) solution, develop incident response plan, enhance remote access security, and implement security awareness training program.

3. **Data Protection (6-9 months):** Implement data classification and governance program, deploy Data Loss Prevention (DLP) solution, establish Third-Party Risk Management (TPRM) program, and implement formal change management.

4. **Continuous Improvement (9-12 months):** Establish cyber risk assessment program, extend asset inventory to complete CMDB, implement encryption key management, and establish SOC or MSSP partnership.

1. Organization Profile

1.1 About Oscorp Industries

Oscorp Industries is a pharmaceutical and biotechnology research organization specializing in advanced scientific research, product development, and laboratory operations. The organization operates state-of-the-art research facilities with highly sensitive intellectual property, proprietary research data, and regulated pharmaceutical information.

Business Model: Research and development focused organization with high-value intellectual property assets, regulatory compliance requirements (FDA, pharmaceutical industry standards), and critical operational dependencies on IT infrastructure.

Technology Environment: Oscorp operates a hybrid IT environment with on-premises Active Directory infrastructure, Microsoft Azure cloud services, Office 365 productivity suite, and various specialized research and laboratory management systems.

Employee Profile: Approximately 100-150 employees including research scientists, laboratory technicians, IT staff, administrative personnel, and executive leadership.

Critical Dependencies: Business operations are highly dependent on:

- Availability and integrity of research data and intellectual property
- Cloud infrastructure supporting collaboration and data analysis
- Identity and access management systems
- Secure remote access for researchers and contractors
- Third-party research partners and vendors

1.2 Business Context

Oscorp's operations generate and process highly sensitive information including:

- Proprietary pharmaceutical research data and formulas
- Clinical trial information and patient data
- Intellectual property and trade secrets
- Employee and contractor personal information
- Financial and business strategy information

Any cybersecurity breach, data loss, or operational disruption could result in:

- Loss of competitive advantage through IP theft
- Regulatory penalties and compliance failures
- Research timeline delays and financial losses
- Damage to scientific credibility and reputation

- Legal liability from data breaches

Therefore, establishing robust cybersecurity governance, risk management, and control implementation is critical to protecting Oscorp's research mission and business continuity.

End of Section 1: Organization Profile

2. Assessment Scope and Methodology

2.1 Scope of Assessment

This GRC assessment included comprehensive evaluation of the following organizational areas:

In-Scope Systems and Processes:

- Cloud infrastructure (Microsoft Azure, Office 365, SaaS applications)
- Identity and access management systems (Active Directory, Azure AD)
- Network infrastructure (firewalls, VPN, wireless networks)
- Data security and protection mechanisms
- Security monitoring, logging, and detection capabilities
- Endpoint protection and vulnerability management
- Business continuity and disaster recovery
- Governance framework, policies, and procedures
- Third-party vendor and contractor risk management
- Security awareness and training programs

Excluded from Scope:

- Detailed physical security systems (already well-controlled)
- Specialized laboratory equipment and operational technology
- Non-IT business processes and operational workflows
- Financial auditing and non-cybersecurity compliance

Assessment Deliverables:

1. Asset Inventory (14 critical assets catalogued)
2. Risk Register (12 risks identified and assessed)
3. NIST SP 800-53 Control Mapping (51 controls across 15 families)
4. Control Evaluation Report (20 critical controls evaluated)
5. Policy Mapping Analysis (17 policies assessed)
6. Gap Analysis (15 critical gaps identified)
7. Recommendations and Roadmap (20 initiatives across 4 phases)

2.2 Assessment Methodology

This assessment was conducted using a **custom-developed NIST SP 800-53 framework** specifically designed for this GRC project. The methodology follows industry-standard GRC practices aligned with NIST Cybersecurity Framework and NIST SP 800-53 Revision 5 control catalog.

Assessment Process Flow:

Step 1: Asset Identification
↓
Step 2: Risk Identification and Assessment
↓
Step 3: NIST Control Mapping
↓
Step 4: Control Implementation Evaluation
↓
Step 5: Policy and Governance Assessment
↓
Step 6: Gap Analysis
↓
Step 7: Recommendations and Roadmap Development

Risk Assessment Methodology

Risk Scoring Model: Quantitative risk assessment using Impact × Likelihood calculation

Risk Score = Impact Rating × Likelihood Rating

- **Impact Rating:** Scored 1-3 based on potential business consequences (1=Low, 2=Medium, 3=High)
- **Likelihood Rating:** Scored 1-3 based on threat probability and vulnerability exploitability (1=Low, 2=Medium, 3=High)
- **Risk Level Classification:**
  - Risk Score 1-3: Low Risk
  - Risk Score 4-6: Medium Risk
  - Risk Score 7-9: High Risk

Assessment Evidence Sources:

- Documentation review (policies, procedures, system configurations)
- Stakeholder interviews (IT management, cybersecurity analyst, operations)
- Current state analysis provided by Oscorp
- System and network configuration review
- Tool and technology inventory review

NIST Framework Customization

The NIST SP 800-53 framework was customized for this assessment by:

1. Selecting relevant control families applicable to Oscorp's environment
2. Prioritizing controls based on risk assessment findings
3. Mapping organizational risks to specific NIST controls
4. Evaluating implementation status using three-tier classification
5. Developing gap analysis between current state and required baseline
6. Creating phased roadmap aligned with business priorities and budget

This custom framework ensures that NIST control implementation is risk-driven, business-aligned, and prioritized for maximum security improvement with available resources.

End of Section 2: Assessment Scope and Methodology

3. Asset Inventory

3.1 Asset Identification Approach

Critical information assets were identified to establish the foundation for risk assessment by understanding what systems, data, and processes require protection. Assets were categorized by type, assigned business impact ratings, and linked to organizational risks.

3.2 Asset Inventory Summary

Asset ID	Asset Name	Asset Type	Criticality	Business Impact
AST-001	Active Directory	Infrastructure	High	Identity foundation for entire organization
AST-002	Microsoft Azure	Cloud Platform	High	Hosts critical business applications
AST-003	Office 365	SaaS Platform	High	Email, collaboration, productivity
AST-004	Research Data	Data Asset	High	Core intellectual property
AST-005	Palo Alto Firewalls	Network Security	High	Perimeter protection
AST-006	VPN Infrastructure	Remote Access	High	Remote workforce connectivity
AST-007	Windows Endpoints	Endpoints	Medium	User workstations (SOE managed)
AST-008	Microsoft Defender	Security Tool	Medium	Endpoint protection
AST-009	Qualys Scanner	Security Tool	Medium	Vulnerability management
AST-010	Salesforce CRM	SaaS Application	Medium	Customer relationship management
AST-011	DocuSign	SaaS Application	Low	Document signing
AST-012	Zoom	SaaS Application	Low	Video conferencing
AST-013	AWS Services	Cloud Platform	Medium	Development and testing
AST-014	Third-Party Vendors	External Entity	High	Research partners, service providers

Table 1: Oscorp Industries Asset Inventory

3.3 Asset Analysis

High Criticality Assets (9 assets, 64%): These assets are essential to business operations and contain sensitive data. Compromise would result in severe business impact including operational disruption, data loss, or regulatory consequences.

Medium Criticality Assets (4 assets, 29%): Important assets supporting business functions but with moderate impact if compromised. Alternative processes or redundancy exists.

Low Criticality Assets (1 asset, 7%): Supporting assets with minimal business impact if temporarily unavailable.

Key Dependencies:

- Identity systems (Active Directory, Azure AD) are foundational dependencies for all other systems
- Cloud platforms (Azure, O365) host majority of business applications and data
- Network security infrastructure provides critical boundary protection
- Research data represents the organization's core value and competitive advantage

---

End of Section 3: Asset Inventory

4. Risk Assessment

4.1 Risk Identification Process

Cybersecurity risks were identified through analysis of assets, threats, vulnerabilities, and potential business impacts. Each risk was evaluated using the quantitative risk scoring methodology to prioritize remediation efforts.

4.2 Risk Register

Risk ID	Risk Description	Impact	Likelihood	Risk Score
R-001	Credential compromise - weak authentication	3	3	9 (High)
R-002	Data breach - inadequate data protection	3	3	9 (High)
R-003	Undetected attacks - no SIEM/monitoring	3	3	9 (High)
R-004	Strategic misalignment - no governance	3	2	6 (Medium)
R-005	Vendor security breach - no TPRM	3	2	6 (Medium)
R-006	Remote access compromise - weak controls	3	3	9 (High)
R-007	Exploitation of vulnerabilities	3	3	9 (High)
R-008	Ineffective incident response	3	3	9 (High)
R-009	Data exfiltration via removable media	2	2	4 (Medium)
R-010	Configuration drift and unauthorized changes	2	2	4 (Medium)
R-011	Successful phishing attacks	3	3	9 (High)
R-012	Compliance and audit failures	3	3	9 (High)

Table 2: Risk Assessment Summary

4.3 Risk Analysis

Risk Distribution:

- High Risk: 8 risks (67%)
- Medium Risk: 4 risks (33%)
- Low Risk: 0 risks (0%)

Top 5 Critical Risks:

R-001: Credential Compromise (Risk Score 9):

- **Threat:** External attackers, malicious insiders, credential theft malware
- **Vulnerability:** No Multi-Factor Authentication, shared admin passwords, weak password policies
- **Impact:** Unauthorized access to systems and data, lateral movement, privilege escalation
- **Affected Assets:** Active Directory, Azure AD, all connected systems

R-003: Undetected Security Incidents (Risk Score 9):

- **Threat:** Advanced persistent threats, insider threats, malware
- **Vulnerability:** No SIEM, logs not centrally collected or analyzed, no SOC capability
- **Impact:** Extended attacker dwell time, inability to detect breaches, forensic limitations
- **Affected Assets:** All IT systems and data

R-002: Data Breach (Risk Score 9):

- **Threat:** Data exfiltration, ransomware, insider threat
- **Vulnerability:** No data classification, no DLP, encryption policy not defined
- **Impact:** Loss of intellectual property, regulatory fines, reputational damage
- **Affected Assets:** Research data, customer information, employee PII

R-008: Ineffective Incident Response (Risk Score 9):

- **Threat:** Cybersecurity incidents (ransomware, breach, DDoS)
- **Vulnerability:** No incident response plan, no IR team, ad-hoc response only
- **Impact:** Extended incident duration, regulatory reporting failures, increased damage
- **Affected Assets:** All organizational assets

R-007: Exploitation of Known Vulnerabilities (Risk Score 9):

- **Threat:** External attackers exploiting unpatched systems
- **Vulnerability:** Ad-hoc vulnerability scanning, no patch management program, large backlog
- **Impact:** System compromise, malware infection, data breach

- **Affected Assets:** All IT infrastructure and applications

---

End of Section 4: Risk Assessment

5. NIST SP 800-53 Control Mapping

5.1 Control Framework Overview

The NIST SP 800-53 Revision 5 framework provides a comprehensive catalog of security and privacy controls organized into 20 control families. For this assessment, 51 controls across 15 relevant families were evaluated based on risk assessment findings.

5.2 Control Family Coverage

Family Code	Control Family Name	Controls Evaluated
AC	Access Control	5
AT	Awareness and Training	2
AU	Audit and Accountability	5
CM	Configuration Management	5
CP	Contingency Planning	3
IA	Identification and Authentication	4
IR	Incident Response	4
MP	Media Protection	2
PE	Physical and Environmental Protection	4
PL	Planning	3
RA	Risk Assessment	3
SC	System and Communications Protection	5
SI	System and Information Integrity	3
SR	Supply Chain Risk Management	3
PM	Program Management	2
Total Controls Assessed		51

Table 3: NIST Control Family Coverage

5.3 Risk-to-Control Mapping Sample

Risk ID	NIST Control	Control Objective
R-001	IA-2(1)	Multi-Factor Authentication
R-001	AC-2	Account Management
R-001	AC-6	Least Privilege
R-001	IA-5	Authenticator Management
R-002	SC-28	Protection of Information at Rest
R-002	MP-6	Media Sanitization
R-002	SI-12	Information Management
R-003	SI-4	System Monitoring
R-003	AU-2	Event Logging
R-003	AU-6	Audit Review and Analysis
R-004	PL-1	Security Planning Policy
R-004	PL-2	System Security Plan
R-004	PM-1	Information Security Program Plan
R-005	SR-1	Supply Chain Risk Mgmt Policy
R-005	SR-2	Supply Chain Risk Mgmt Plan
R-005	SR-3	Supply Chain Controls

Table 4: Sample Risk-to-Control Mapping

Complete control mapping with all 51 controls is provided in the supporting Excel documentation.

End of Section 5: NIST SP 800-53 Control Mapping

6. Control Implementation Evaluation

6.1 Evaluation Methodology

Each mapped NIST control was evaluated to determine its current implementation status at Oscorp. Controls were classified into three categories:

- **Implemented:** Control is fully deployed, documented, and operating effectively
- **Partially Implemented:** Control exists but has significant gaps or weaknesses
- **Not Implemented:** Control does not exist or is insufficient to be effective

6.2 Overall Implementation Status

Implementation Status	Number of Controls	Percentage
Implemented	11	22%
Partially Implemented	14	27%
Not Implemented	26	51%
Total Controls Evaluated	51	100%

Table 5: NIST Control Implementation Summary

Analysis: Only 22% of assessed controls are fully implemented, indicating significant cybersecurity maturity gaps. The 51% of controls not implemented represent the highest priority remediation areas.

6.3 Critical Control Evaluation Details

Access Control (AC) Family

AC-2: Account Management - Partially Implemented

- **Current State:** Active Directory provides basic account management, but lacks formal RBAC model, access review process, or approval workflows. Admin passwords are shared.
- **Gap:** No least privilege enforcement, no quarterly access reviews, shared admin accounts violate accountability principle.
- **Recommendation:** Implement RBAC, establish access review process, eliminate shared accounts, deploy PAM solution.

AC-6: Least Privilege - Not Implemented

- **Current State:** Access granted upon request without formal approval or justification. No enforcement of least privilege principle.
- **Gap:** Users may have excessive permissions, no privilege reviews conducted.
- **Recommendation:** Implement least privilege model, conduct privilege audit, remove excessive permissions.

AC-17: Remote Access - Partially Implemented

- **Current State:** VPN solution exists but lacks MFA. Contractor remote access not formally managed.
- **Gap:** VPN compromise risk due to password-only authentication.
- **Recommendation:** Implement MFA for VPN, establish contractor access management procedures.

Identification and Authentication (IA) Family

IA-2(1): Multi-Factor Authentication - Not Implemented

- **Current State:** MFA not deployed for any users or systems. Authentication relies solely on username/password.
- **Gap:** High risk of credential compromise through phishing, password reuse, brute force.
- **Recommendation:** Deploy MFA for all users starting with privileged accounts, Azure AD, O365, and VPN.

IA-5: Authenticator Management - Partially Implemented

- **Current State:** Complex password policy enforced by Active Directory, but admin passwords are shared.
- **Gap:** Shared credentials violate accountability and non-repudiation principles.
- **Recommendation:** Eliminate all shared accounts, implement PAM for privileged access.

Audit and Accountability (AU) Family

AU-2: Event Logging - Partially Implemented

- **Current State:** Basic logging exists on some systems but not comprehensive or standardized.
- **Gap:** Inconsistent logging, no centralized collection, gaps in log coverage.
- **Recommendation:** Implement centralized logging solution, define logging standards, ensure comprehensive coverage.

AU-6: Audit Review, Analysis, and Reporting - Not Implemented

- **Current State:** Logs generated but not reviewed or analyzed. No monitoring procedures.
- **Gap:** Security events go undetected, no proactive threat detection.

- **Recommendation:** Implement log review procedures, deploy SIEM for correlation and analysis.

System and Information Integrity (SI) Family

SI-4: System Monitoring - Not Implemented

- **Current State:** No SIEM or comprehensive monitoring capability. Limited to antivirus alerts.
- **Gap:** Cannot detect sophisticated attacks, insider threats, or anomalous behavior.
- **Recommendation:** Deploy SIEM solution (e.g., Microsoft Sentinel), onboard critical systems, create detection use cases.

SI-2: Flaw Remediation - Partially Implemented

- **Current State:** Qualys vulnerability scanner exists but used ad-hoc. Large backlog of critical vulnerabilities.
- **Gap:** No formal vulnerability management program, no remediation SLAs.
- **Recommendation:** Establish formal VM program with scanning schedules, prioritization, and remediation SLAs.

SI-3: Malicious Code Protection - Implemented

- **Current State:** Microsoft Defender deployed across all endpoints. IT team responds to alerts.
- **Gap:** Consider enhanced endpoint detection and response (EDR) capabilities.
- **Recommendation:** Evaluate EDR solutions for advanced threat detection and response.

Incident Response (IR) Family

IR-4: Incident Handling - Not Implemented

- **Current State:** Cybersecurity analyst responds to incidents ad-hoc. No documented procedures or runbooks.
- **Gap:** Inconsistent response, no established procedures, potential for errors under pressure.
- **Recommendation:** Develop incident response plan, establish IR team, create incident handling runbooks.

IR-8: Incident Response Plan - Not Implemented

- **Current State:** No cybersecurity incident response plan exists. BC/DR plans exist but don't cover cyber incidents.
- **Gap:** No structured approach to incident management, containment, eradication, and recovery.
- **Recommendation:** Develop comprehensive IR plan aligned with NIST SP 800-61, conduct tabletop exercises.

Planning (PL) and Program Management (PM) Families

PL-2: System Security Plan - Not Implemented

- **Current State:** No system security plans documented for any IT systems.
- **Gap:** No documented security requirements, controls, or responsibilities per system.
- **Recommendation:** Develop system security plans for critical systems documenting security controls and configurations.

PM-1: Information Security Program Plan - Not Implemented

- **Current State:** No formal cybersecurity strategy or program plan. Only generic IT policy exists.
- **Gap:** No strategic direction, no defined security objectives, no governance structure.
- **Recommendation:** Develop organizational cybersecurity strategy and program plan with board oversight.

End of Section 6: Control Implementation Evaluation

7. Policy and Governance Assessment

7.1 Policy Mapping Approach

Organizational policies were evaluated against NIST SP 800-53 requirements to identify governance gaps. Policies provide the foundation for control implementation and demonstrate management commitment to cybersecurity.

7.2 Policy Status Summary

NIST Controls	Required Policy	Status
IA-2, IA-2(1), IA-5	Authentication and MFA Policy	Missing
AC-1, AC-2, AC-6	Access Control Policy	Missing
PL-1, PL-2, PM-1	Information Security Policy	Weak
IR-1, IR-4, IR-8	Incident Response Policy	Missing
AU-1, AU-2, AU-6	Logging and Monitoring Policy	Missing
SC-12, SC-13, SC-28	Data Protection and Encryption Policy	Missing
SI-12, MP-3, MP-6	Data Classification Policy	Missing
SR-1, SR-2, SR-3	Third-Party Risk Management Policy	Missing
RA-1, RA-3	Cyber Risk Assessment Policy	Missing
RA-5, SI-2	Vulnerability Management Policy	Missing
CM-1, CM-3	Change Management Policy	Missing
MP-1, MP-7	Removable Media Policy	Missing
AT-1, AT-2, AT-3	Security Awareness Policy	Partial
AC-17	Remote Access Policy	Missing
CM-2, CM-6	Configuration Management Policy	Partial
PE-1, PE-2, PE-3	Physical Security Policy	Implemented
CP-1, CP-2, CP-9	Business Continuity Policy	Implemented

Table 6: Policy Gap Analysis

Policy Status Analysis:

- **Implemented:** 2 policies (12%) - Physical Security, Business Continuity/DR

- **Partial:** 3 policies (18%) - Information Security (weak), Awareness Training, Configuration Management
- **Missing:** 12 policies (70%) - Critical security policies do not exist

7.3 Governance Structure Assessment

Current State:

- No designated Chief Information Security Officer (CISO) or equivalent role
- Cybersecurity responsibilities distributed across IT Manager and single security analyst
- No cybersecurity steering committee or governance board
- Limited board-level visibility into cybersecurity risks
- No defined security strategy or program objectives

Gaps:

- Lack of senior security leadership and accountability
- Insufficient resources dedicated to cybersecurity program
- No strategic planning or risk-based prioritization
- Limited communication of cyber risks to executive leadership
- No security metrics or KPIs tracked

Recommendations:

- Designate or hire CISO to lead cybersecurity program
- Establish cybersecurity steering committee with executive representation
- Develop 3-year cybersecurity strategy aligned with business objectives
- Implement quarterly board reporting on cybersecurity risks and metrics
- Define security program KPIs and track progress

End of Section 7: Policy and Governance Assessment

8. Gap Analysis

8.1 Gap Analysis Methodology

Gap analysis compared Oscorp's current security posture against NIST SP 800-53 baseline requirements to identify specific deficiencies requiring remediation. Gaps were prioritized by severity based on risk exposure.

8.2 Critical Gaps Summary

Gap Area	Description	Severity
Multi-Factor Authentication	No MFA implementation	Critical
Security Monitoring	No SIEM or centralized monitoring	Critical
Incident Response	No IR plan or procedures	Critical
Cybersecurity Governance	No strategy or leadership	Critical
Data Protection	No classification or DLP	Critical
Privileged Access Mgmt	Shared admin passwords	High
Third-Party Risk Mgmt	No vendor assessment process	High
Vulnerability Management	Ad-hoc scanning, large backlog	High
Remote Access Security	No MFA for VPN	High
Audit Logging	Logs not reviewed or analyzed	High
Change Management	No formal process	Medium
Removable Media Controls	USB unrestricted	Medium
Security Awareness	Induction only, no ongoing program	Medium
Asset Inventory	Software and vendors not tracked	Medium
Risk Assessment	No cyber risk assessments	Medium

Table 7: Security Gap Analysis

8.3 Detailed Gap Analysis

Gap 1: Identity and Access Management (Critical)

Required State (NIST): MFA enforced for all users and privileged accounts (IA-2(1)), role-based access control implemented (AC-2), least privilege enforced (AC-6), no shared admin accounts (IA-5).

Current State (Oscorp): No MFA implementation, access granted on request without formal approval, shared admin passwords, no RBAC model, no access reviews conducted.

Impact of Gap: High risk of credential compromise through phishing, password reuse, or brute force attacks. Shared admin accounts violate accountability principles. Excessive permissions increase lateral movement risk if account is compromised.

Related NIST Controls: IA-2(1), IA-5, AC-2, AC-6

Remediation Actions:

1. Deploy MFA for all users starting with privileged accounts, O365, Azure AD, and VPN
2. Implement PAM solution to eliminate shared admin accounts and control privileged access
3. Implement RBAC model with defined roles and access approval workflows
4. Conduct quarterly access reviews to validate permissions and remove excessive access
5. Enforce least privilege principle across all systems

Gap 2: Security Monitoring and Detection (Critical)

Required State (NIST): SIEM deployed with centralized logging (AU-2, AU-12), 24/7 monitoring capability (SI-4), log review and analysis procedures (AU-6), incident monitoring and correlation (IR-5).

Current State (Oscorp): No SIEM solution, logs not centrally collected, no log analysis or review, limited monitoring to antivirus alerts only.

Impact of Gap: Cannot detect sophisticated attacks, insider threats, or anomalous behavior. Extended attacker dwell time (industry average 200+ days). Limited forensic capability. Regulatory compliance failures for audit logging.

Related NIST Controls: SI-4, AU-2, AU-3, AU-6, AU-12, IR-5

Remediation Actions:

1. Deploy SIEM solution (e.g., Microsoft Sentinel, Splunk, or similar)
2. Onboard all critical systems and applications to centralized logging
3. Implement log retention policy (minimum 1 year recommended)
4. Create detection use cases and correlation rules for common attack patterns
5. Establish log review procedures with defined frequency and responsibilities
6. Consider SOC or MSSP partnership for 24/7 monitoring capability

Gap 3: Incident Response (Critical)

Required State (NIST): Documented incident response plan (IR-8), established IR team with defined roles (IR-4), incident handling procedures and runbooks (IR-4), regular tabletop exercises (IR-3), communication and escalation procedures.

Current State (Oscorp): No cybersecurity incident response plan, ad-hoc response by security analyst, no documented procedures, no IR team or defined roles. BC/DR plans exist but don't cover cyber incidents.

Impact of Gap: Ineffective incident containment and eradication, extended incident duration, regulatory reporting failures (GDPR, breach notification laws), increased business impact and recovery costs.

Related NIST Controls: IR-1, IR-3, IR-4, IR-5, IR-8

Remediation Actions:

1. Develop comprehensive incident response plan aligned with NIST SP 800-61
2. Establish incident response team with defined roles (IR Lead, IT, Legal, Communications, Management)
3. Create incident handling runbooks for common scenarios (ransomware, data breach, DDoS)
4. Implement incident tracking and documentation system
5. Conduct quarterly tabletop exercises to test IR plan and procedures
6. Establish communication templates and escalation procedures

Gap 4: Data Protection (Critical)

Required State (NIST): Data classification scheme implemented (SI-12, MP-3), DLP solution deployed (SC-28, MP-6), encryption policy defined (SC-12, SC-13), data handling procedures documented, media sanitization process established.

Current State (Oscorp): No data classification program, no DLP solution, encryption by default in O365/Azure but no policy, no data governance, no disposal procedures.

Impact of Gap: Cannot protect data appropriately without classification, data exfiltration risk via email/cloud/USB, regulatory non-compliance for data protection, intellectual property theft risk.

Related NIST Controls: SC-28, SI-12, MP-3, MP-6, SC-12, SC-13

Remediation Actions:

1. Conduct data discovery and implement classification scheme (Public, Internal, Confidential, Restricted)
2. Deploy DLP solution for O365, endpoints, and network
3. Implement data labeling and handling procedures
4. Develop encryption policy and key management procedures
5. Establish data governance framework with data owners and stewards
6. Implement media sanitization and data disposal procedures

Gap 5: Third-Party Risk Management (High)

Required State (NIST): TPRM policy and framework (SR-1, SR-2), vendor security assessment process (SR-3), contract security clauses, ongoing vendor risk monitoring.

Current State (Oscorp): No TPRM policy or framework, contracts reviewed by procurement/finance only with no cybersecurity assessment, vendor access not controlled or monitored.

Impact of Gap: Supply chain attack risk, vendor-introduced vulnerabilities, no visibility into vendor security posture, compliance failures for vendor management.

Related NIST Controls: SR-1, SR-2, SR-3, SA-9

Remediation Actions:

1. Develop third-party risk management policy and framework
2. Create vendor security assessment questionnaire based on criticality tiers
3. Update contract templates with security requirements and right-to-audit clauses
4. Implement vendor risk register and ongoing monitoring program
5. Conduct security assessments for all current critical vendors
6. Establish vendor access management and monitoring procedures

---

End of Section 8: Gap Analysis

9. Recommendations and Security Roadmap

9.1 Remediation Strategy

The remediation strategy follows a phased approach over 12 months, prioritizing critical gaps that pose the highest risk to the organization. Each phase builds upon previous accomplishments to achieve progressive security maturity improvement.

Phased Approach Benefits:

- Spreads investment over 12 months for budget planning
- Allows time for organizational change management and adoption
- Builds foundational capabilities before advanced controls
- Demonstrates progress and value to executive leadership
- Reduces implementation risk through incremental deployment

9.2 Implementation Roadmap

Phase 1: Foundation and Quick Wins (Months 0-3)

Objective: Establish critical foundational security controls and governance framework

Budget: $300,000

Key Initiatives:

REC-001: Deploy Multi-Factor Authentication (MFA)

- **NIST Controls:** IA-2(1), AC-2
- **Scope:** Implement MFA for all users starting with privileged accounts, Azure AD, Office 365, and VPN
- **Timeline:** Month 1-2
- **Investment:** $75,000
- **Expected Outcome:** 90% reduction in credential compromise risk

REC-002: Develop Information Security Policy Framework

- **NIST Controls:** PL-1, PL-2, PL-8, PM-1
- **Scope:** Create comprehensive information security policy, define cybersecurity strategy, establish governance structure
- **Timeline:** Month 1-3

- **Investment:** $50,000
- **Expected Outcome:** Foundation for entire security program, board-level oversight

REC-003: Implement Privileged Access Management (PAM)

- **NIST Controls:** AC-2, AC-6, IA-5
- **Scope:** Deploy PAM solution, eliminate shared admin accounts, create individual privileged accounts, implement just-in-time access
- **Timeline:** Month 2-3
- **Investment:** $100,000
- **Expected Outcome:** Complete accountability for privileged actions, reduced privilege escalation risk

REC-004: Establish Formal Vulnerability Management Program

- **NIST Controls:** RA-5, SI-2
- **Scope:** Formalize Qualys usage, define scanning schedules (weekly critical systems), create remediation SLAs (Critical: 7 days, High: 30 days), prioritize current backlog
- **Timeline:** Month 1-3
- **Investment:** $25,000
- **Expected Outcome:** Systematic vulnerability remediation, reduced attack surface

REC-005: Implement Centralized Logging

- **NIST Controls:** AU-2, AU-3, AU-12
- **Scope:** Deploy centralized logging solution, onboard critical systems, establish 1-year log retention policy
- **Timeline:** Month 2-3
- **Investment:** $50,000
- **Expected Outcome:** Foundation for security monitoring, compliance logging, forensic capability

Phase 1 Success Metrics:

- MFA adoption rate: 100% of users
- Vulnerability remediation: 80% of critical vulnerabilities resolved
- Policy completion: 5 core policies published
- Shared accounts eliminated: 100%

Phase 2: Detection and Response (Months 3-6)

Objective: Implement security monitoring, detection, and incident response capabilities

Budget: $425,000

Key Initiatives:

REC-006: Deploy SIEM and Security Monitoring

- **NIST Controls:** SI-4, AU-6, IR-5
- **Scope:** Implement SIEM solution (Microsoft Sentinel recommended for Azure/O365 integration), onboard all critical systems, create 20+ detection use cases, implement correlation rules
- **Timeline:** Month 3-5
- **Investment:** $200,000
- **Expected Outcome:** 24/7 visibility into security events, automated threat detection

REC-007: Develop and Implement Incident Response Plan

- **NIST Controls:** IR-1, IR-4, IR-8, IR-3
- **Scope:** Create comprehensive IR plan aligned with NIST SP 800-61, establish IR team (Lead, IT, Legal, Comms, Management), develop runbooks for ransomware/breach/DDoS, implement ticketing system, conduct 2 tabletop exercises
- **Timeline:** Month 3-5
- **Investment:** $75,000
- **Expected Outcome:** Structured incident response capability, reduced incident duration by 70%

REC-008: Enhance Remote Access Security

- **NIST Controls:** AC-17, IA-2(1), AC-20
- **Scope:** Verify MFA for VPN (from Phase 1), implement contractor access management procedures, deploy network access control (NAC), implement VPN access reviews
- **Timeline:** Month 4-6
- **Investment:** $80,000
- **Expected Outcome:** Secure remote access, controlled contractor access

REC-009: Enhance Security Awareness Training

- **NIST Controls:** AT-2, AT-3
- **Scope:** Implement phishing simulation platform (e.g., KnowBe4), create role-based training modules (general users, developers, admins), establish quarterly awareness campaigns, measure phishing susceptibility baseline
- **Timeline:** Month 4-6
- **Investment:** $40,000
- **Expected Outcome:** 50% reduction in phishing click rates within 6 months

REC-010: Implement Log Review and Monitoring Procedures

- **NIST Controls:** AU-6

- **Scope:** Establish log review schedules (daily for critical alerts, weekly for trends), create monitoring dashboards, define alerting thresholds, document review procedures
- **Timeline:** Month 4-6
- **Investment:** $30,000
- **Expected Outcome:** Proactive threat detection, compliance with audit logging requirements

Phase 2 Success Metrics:

- SIEM detection use cases deployed: 20+
- Incident response tabletop exercises completed: 2
- Phishing click rate reduction: 50%
- Critical security events reviewed: 100% within 24 hours

Phase 3: Data Protection and Governance (Months 6-9)

Objective: Implement data protection controls and formalize governance processes

Budget: $405,000

Key Initiatives:

REC-011: Implement Data Classification and Governance Program

- **NIST Controls:** SI-12, MP-3
- **Scope:** Conduct data discovery across file shares, databases, cloud storage; implement 4-tier classification scheme (Public, Internal, Confidential, Restricted); deploy data labeling solution; establish data governance framework with data owners; create data handling procedures
- **Timeline:** Month 6-8
- **Investment:** $120,000
- **Expected Outcome:** Visibility into sensitive data locations, foundation for data protection

REC-012: Deploy Data Loss Prevention (DLP) Solution

- **NIST Controls:** SC-28, MP-6
- **Scope:** Implement DLP for Office 365, email, and endpoints; configure policies based on data classification; implement blocking for high-risk scenarios; deploy monitoring for other scenarios; integrate with SIEM
- **Timeline:** Month 7-9
- **Investment:** $150,000
- **Expected Outcome:** Prevention of unauthorized data exfiltration, compliance with data protection regulations

REC-013: Establish Third-Party Risk Management Program

- **NIST Controls:** SR-1, SR-2, SR-3, SA-9
- **Scope:** Develop TPRM framework with 3-tier vendor criticality model; create security assessment questionnaire; update contract templates with security clauses; assess all current critical vendors; implement vendor risk register and monitoring program
- **Timeline:** Month 6-9
- **Investment:** $60,000
- **Expected Outcome:** Visibility into vendor security posture, reduced supply chain risk

REC-014: Implement Change Management Process

- **NIST Controls:** CM-3, CM-6
- **Scope:** Develop change management procedures with approval workflows; implement change request system; establish Change Advisory Board (CAB) with weekly meetings; create change documentation templates; define emergency change procedures
- **Timeline:** Month 7-9
- **Investment:** $40,000
- **Expected Outcome:** Controlled configuration changes, reduced risk of unauthorized modifications

REC-015: Implement Removable Media Controls

- **NIST Controls:** MP-1, MP-7
- **Scope:** Develop removable media policy; implement USB restrictions via Group Policy; whitelist approved devices; deploy USB monitoring and logging; extend DLP to removable media
- **Timeline:** Month 8-9
- **Investment:** $35,000
- **Expected Outcome:** Prevention of data exfiltration via USB drives

Phase 3 Success Metrics:

- Data classified: 100% of file shares and databases
- DLP policies deployed: 15+ covering all data classifications
- Vendor assessments completed: 100% of critical vendors
- USB restrictions implemented: 100% of endpoints

Phase 4: Continuous Improvement and Maturity (Months 9-12)

Objective: Achieve advanced security maturity and establish continuous improvement

Budget: $485,000

Key Initiatives:

REC-016: Establish Cyber Risk Assessment Program

- **NIST Controls:** RA-1, RA-3, PM-9
- **Scope:** Develop risk assessment methodology aligned with NIST SP 800-30; conduct organization-wide cyber risk assessment; create risk register with treatment plans; establish annual risk assessment cadence; implement risk reporting to board
- **Timeline:** Month 9-11
- **Investment:** $80,000
- **Expected Outcome:** Risk-based decision making, risk-informed budgeting

REC-017: Extend Asset Inventory to Complete CMDB

- **NIST Controls:** CM-8
- **Scope:** Deploy automated asset discovery tool; inventory all software, SaaS applications, cloud resources; track third-party vendors and data flows; implement ongoing asset tracking and reconciliation; integrate with vulnerability management
- **Timeline:** Month 9-11
- **Investment:** $50,000
- **Expected Outcome:** Complete visibility into organizational assets, foundation for risk assessment

REC-018: Implement Encryption Key Management

- **NIST Controls:** SC-12, SC-13
- **Scope:** Develop encryption policy defining encryption requirements; implement key management procedures and lifecycle; document encryption usage across organization; consider Azure Key Vault for cloud key management
- **Timeline:** Month 10-12
- **Investment:** $60,000
- **Expected Outcome:** Proper cryptographic controls and key lifecycle management

REC-019: Establish SOC or MSSP Partnership

- **NIST Controls:** SI-4, IR-5, AU-6
- **Scope:** Evaluate build internal SOC vs. Managed Security Service Provider (MSSP) partnership; establish 24/7 monitoring capability; define service level agreements for detection and response; implement escalation procedures; conduct monthly service reviews
- **Timeline:** Month 10-12
- **Investment:** $250,000 (annual)
- **Expected Outcome:** 24/7 threat detection and response capability, reduced mean time to detect (MTTD)

REC-020: Conduct Cyber Crisis Simulation Exercise

- **NIST Controls:** IR-3, CP-4
- **Scope:** Plan and execute full-scale cyber crisis simulation (ransomware or data breach scenario); engage executive leadership and board; test IR plan and BC/DR procedures; document lessons learned; update plans based on findings
- **Timeline:** Month 11-12
- **Investment:** $45,000
- **Expected Outcome:** Validated incident response readiness, executive engagement in cybersecurity

Phase 4 Success Metrics:

- Risk assessment completed: Organization-wide
- Asset inventory completeness: 100% (hardware, software, cloud, vendors)
- SOC/MSSP operational: 24/7 monitoring coverage
- Crisis simulation executed: 1 full-scale exercise

9.3 Investment Summary

Phase	Timeline	Investment
Phase 1: Foundation & Quick Wins	0-3 months	$300,000
Phase 2: Detection & Response	3-6 months	$425,000
Phase 3: Data Protection	6-9 months	$405,000
Phase 4: Continuous Improvement	9-12 months	$485,000
Total 12-Month Investment		$1,615,000

Table 8: Phased Implementation Investment

9.4 Expected Outcomes and Benefits

Risk Reduction:

- 70% reduction in likelihood of successful cyberattack
- 80% reduction in credential compromise risk (MFA + PAM)
- 90% reduction in mean time to detect security incidents (SIEM + SOC)
- 60% reduction in data breach risk (DLP + data classification)
- 50% reduction in phishing susceptibility (awareness training)

Compliance and Governance:

- NIST Cybersecurity Framework maturity: 28% → 75%+

- NIST SP 800-53 control implementation: 22% → 75%+
- Board-level cybersecurity visibility and reporting established
- 15 critical security policies developed and implemented
- Regulatory compliance improved for GDPR, industry standards

Operational Improvements:

- 24/7 security monitoring and incident response capability
- Incident response time reduced from ad-hoc to defined SLAs
- Vulnerability remediation: Critical within 7 days, High within 30 days
- Complete visibility into organizational assets and data
- Systematic third-party risk management

Business Value:

- Protection of intellectual property and research data (primary business asset)
- Reduced insurance premiums through improved security posture
- Competitive advantage through demonstrated security commitment
- Customer and partner trust through security maturity
- Reduced likelihood of business disruption from security incidents

---

End of Section 9: Recommendations and Security Roadmap

10. Conclusion and Next Steps

10.1 Assessment Summary

This comprehensive GRC assessment of Oscorp Industries identified significant cybersecurity maturity gaps requiring immediate attention. The evaluation, conducted using a **custom-developed NIST SP 800-53 framework**, revealed that only 22% of assessed controls are fully implemented, with 51% not implemented at all.

Critical findings include:

- 8 high-risk cybersecurity risks (67% of total risks)
- Absence of Multi-Factor Authentication across all systems
- No Security Information and Event Management (SIEM) capability
- No formal incident response plan or procedures
- Inadequate data protection and governance
- Missing or weak cybersecurity policies (70% gap)
- Limited cybersecurity governance and strategic direction

These gaps expose Oscorp to significant risks of data breach, operational disruption, regulatory non-compliance, and intellectual property theft. However, the organization has strong foundations in Business Continuity/Disaster Recovery and physical security that can be built upon.

10.2 Strategic Recommendations

The 12-month phased remediation roadmap provides a risk-based, structured approach to achieving cybersecurity maturity:

1. **Phase 1 (0-3 months):** Establish critical foundation controls (MFA, PAM, policies, vulnerability management)
2. **Phase 2 (3-6 months):** Implement detection and response capabilities (SIEM, IR plan, monitoring)
3. **Phase 3 (6-9 months):** Deploy data protection and governance (DLP, data classification, TPRM)
4. **Phase 4 (9-12 months):** Achieve continuous improvement maturity (risk assessment, SOC/MSSP, advanced controls)

Total investment of **$1,615,000** over 12 months will achieve **75%+ NIST CSF maturity** and **70% risk reduction**.

10.3 Immediate Next Steps

Week 1-2: Executive Engagement

1. Present findings to executive leadership and board of directors
2. Secure commitment and budget approval for Phase 1 initiatives
3. Establish cybersecurity steering committee with executive representation
4. Designate or hire Chief Information Security Officer (CISO)

Month 1: Quick Start Initiatives

1. Begin MFA deployment (Azure AD, O365, privileged accounts)
2. Initiate information security policy development
3. Conduct assessment of PAM solution vendors
4. Formalize vulnerability management procedures
5. Deploy centralized logging solution

Month 2-3: Foundation Building

1. Complete MFA rollout to all users
2. Implement PAM solution and eliminate shared admin accounts
3. Publish first wave of security policies (Access Control, Authentication, Information Security)
4. Establish formal vulnerability remediation process with SLAs
5. Begin SIEM vendor evaluation and procurement

10.4 Success Factors

Critical success factors for this remediation program:

1. **Executive Sponsorship:** Board and C-suite commitment to cybersecurity investment and cultural change
2. **Dedicated Leadership:** CISO or equivalent role to drive program execution and accountability
3. **Resource Allocation:** Budget, personnel, and time allocated to security initiatives
4. **Change Management:** Communication, training, and user adoption strategies for new controls
5. **Vendor Partnerships:** Selection of qualified vendors and service providers for tool implementation
6. **Measurement and Reporting:** Regular progress tracking against roadmap milestones and KPIs
7. **Continuous Improvement:** Commitment to ongoing security maturity beyond initial 12 months

10.5 Long-Term Vision

Beyond the 12-month roadmap, Oscorp should establish continuous improvement mechanisms:

- **Annual risk assessments** to identify emerging threats and evolving business risks
- **Quarterly security metrics reporting** to board and executive leadership
- **Continuous control monitoring** and maturity assessment against NIST CSF
- **Security program budget** as percentage of IT budget (industry benchmark: 10-15%)
- **Security awareness culture** embedded in organizational values
- **Threat intelligence program** to stay informed of industry-specific threats
- **Advanced capabilities** such as threat hunting, penetration testing, red team exercises

By implementing the recommendations in this assessment, Oscorp Industries will transform its cybersecurity posture from reactive and fragmented to proactive, comprehensive, and risk-driven - positioning the organization for secure innovation and sustainable business growth.

End of Section 10: Conclusion and Next Steps

11. Appendices

Appendix A: Assessment Framework and Methodology

This assessment was conducted using a **custom-developed NIST SP 800-53 Revision 5 framework** specifically designed for this GRC project. The framework adapts NIST guidelines to Oscorp's organizational context, risk profile, and business requirements.

Framework Development Process

1. **NIST SP 800-53 Control Selection:** From the complete NIST SP 800-53 Rev 5 catalog containing 1,000+ controls, 51 controls across 15 families were selected based on relevance to identified organizational risks and industry best practices.
2. **Risk-Based Prioritization:** Controls were prioritized based on risk assessment findings, focusing on high-impact, high-likelihood risk scenarios affecting Oscorp's critical assets.
3. **Maturity Assessment Model:** Three-tier implementation status model (Implemented, Partially Implemented, Not Implemented) provides clear evaluation criteria and gap identification.
4. **Roadmap Alignment:** Recommendations are sequenced based on dependency relationships, resource constraints, and progressive capability building.

Assessment Evidence Sources

- Oscorp current state documentation and self-assessment
- Stakeholder interviews (IT management, security analyst, operations teams)
- System and network configuration reviews
- Policy and procedure documentation analysis
- Technology inventory and architecture diagrams
- Industry benchmarking and best practices research

Quality Assurance

This assessment followed professional GRC standards and methodologies:

- NIST Cybersecurity Framework (CSF)
- NIST SP 800-53 Rev 5: Security and Privacy Controls
- NIST SP 800-30: Guide for Conducting Risk Assessments
- NIST SP 800-61: Computer Security Incident Handling Guide
- ISO 27001/27002 principles for governance and control implementation

- Industry-standard risk assessment methodologies

Appendix B: Risk Scoring Methodology

Risk Calculation Formula

Risk Score = Impact Rating × Likelihood Rating

Impact Rating Scale (1-3)

Rating	Level	Criteria
3	High	Severe business impact: operational shutdown, significant financial loss ($1M+), major data breach, regulatory penalties, severe reputational damage
2	Medium	Moderate business impact: partial service disruption, moderate financial loss ($100K-$1M), limited data exposure, customer complaints
1	Low	Minor business impact: minimal disruption, low financial loss (<$100K), no data exposure, internal impact only

Table 9: Impact Rating Criteria

Likelihood Rating Scale (1-3)

Rating	Level	Criteria
3	High	Very likely to occur: known active threats, easily exploitable vulnerabilities, historical incidents, inadequate controls
2	Medium	Moderately likely: possible threats, vulnerabilities exist but require some effort, partial controls in place
1	Low	Unlikely to occur: theoretical threats, difficult to exploit vulnerabilities, strong controls in place

Table 10: Likelihood Rating Criteria

Risk Level Classification

Score	Risk Level	Response Priority
7-9	High	Immediate action required, executive attention, highest priority remediation
4-6	Medium	Action required within defined timeline, management attention, planned remediation
1-3	Low	Accept or mitigate as resources allow, periodic review

Table 11: Risk Classification

Appendix C: Supporting Documentation

The following supporting Excel documentation provides detailed assessment data:

1. **Asset-Inventory.xlsx** - Complete asset catalog with 14 organizational assets including business impact ratings, asset owners, and locations

2. **Risk-Register.xlsx** - Comprehensive risk assessment with 12 identified risks including threat sources, vulnerabilities, impact analysis, likelihood assessment, risk scores, and mitigation strategies

3. **NIST-Control-Mapping.xlsx** - Detailed mapping of 51 NIST SP 800-53 controls to identified risks across 15 control families with implementation status and current state evidence

4. **Control-Evaluation.xlsx** - In-depth evaluation of 20 critical controls with implementation status, evidence, observations, and specific recommendations

5. **Policy-Mapping.xlsx** - Analysis of 17 required security policies mapped to NIST controls with policy status, priority ratings, target timelines, and policy ownership assignments

6. **Gap-Analysis.xlsx** - Identification of 15 critical security gaps with required state vs. current state comparison, gap severity ratings, impact analysis, and remediation actions

7. **Recommendations-Roadmap.xlsx** - Comprehensive 12-month implementation roadmap with 20 prioritized recommendations across 4 phases including cost estimates, owners, timelines, and business justification

Appendix D: NIST Control Family Reference

Family Code	Control Family Name
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Assessment, Authorization, and Monitoring
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management
PS	Personnel Security
PT	PII Processing and Transparency
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
SR	Supply Chain Risk Management

Table 12: NIST SP 800-53 Rev 5 Control Families

Appendix E: Glossary of Terms

Active Directory (AD): Microsoft directory service providing identity and access management for Windows environments

Azure AD: Microsoft's cloud-based identity and access management service

CMDB: Configuration Management Database - repository of IT assets and their relationships

CISO: Chief Information Security Officer - executive role responsible for cybersecurity program

DLP: Data Loss Prevention - technology preventing unauthorized data exfiltration

EDR: Endpoint Detection and Response - advanced endpoint security solution

GRC: Governance, Risk, and Compliance - integrated approach to managing organizational risks

IAM: Identity and Access Management - processes and technologies for managing digital identities

IR: Incident Response - organized approach to addressing and managing security incidents

MFA: Multi-Factor Authentication - security mechanism requiring two or more verification factors

MSSP: Managed Security Service Provider - outsourced security operations provider

NIST: National Institute of Standards and Technology - US federal agency developing cybersecurity standards

NIST CSF: NIST Cybersecurity Framework - voluntary framework for managing cybersecurity risk

NIST SP 800-53: NIST Special Publication 800-53 - catalog of security and privacy controls

PAM: Privileged Access Management - solution for securing and monitoring privileged accounts

RBAC: Role-Based Access Control - access control model based on user roles

SIEM: Security Information and Event Management - centralized security monitoring and analysis platform

SOC: Security Operations Center - dedicated facility for security monitoring and response

SoA: Statement of Applicability - document defining which controls apply to organization (ISO 27001 term)

SOE: Standard Operating Environment - standardized configuration for endpoints

TPRM: Third-Party Risk Management - process for assessing and managing vendor cybersecurity risks

VPN: Virtual Private Network - encrypted connection for remote access

End of Section 11: Appendices

Document Control

Document Version: 1.0
Document Classification: Internal Use - Management Circulation
Document Owner: GRC Analyst - Nirmay Soni
Review Date: January 30, 2026
Next Review: July 2026 (6-month progress review)

Distribution List:

- Board of Directors
- Chief Executive Officer
- Chief Financial Officer
- IT Manager
- Cybersecurity Analyst
- Legal Counsel
- Risk Management Team

Confidentiality Notice: This document contains confidential information about Oscorp Industries' cybersecurity posture and should be handled according to organizational information classification and handling procedures. Distribution should be limited to individuals with legitimate business need.

End of Report