OSCORP Cyber Security GRC Assessment Report

Aligned with NIST CSF & NIST SP 800-53

---

1. Executive Summary

1.1 Overview

This report presents the results of a Cyber Security Governance, Risk, and Compliance (GRC) assessment conducted for Oscorp, a Small and Medium Enterprise (SME). The assessment evaluates Oscorp's current cyber security posture, identifies key risks and gaps, and provides a structured roadmap to improve security maturity in alignment with the NIST Cybersecurity Framework (CSF) and NIST SP 800-53 controls.

The assessment reveals that while Oscorp has implemented certain technical controls such as firewalls, backups, and cloud services, significant gaps exist in identity management, monitoring, governance, incident response, and data protection. These gaps expose the organization to high cyber risk.

This report provides a practical and prioritized security improvement plan tailored to Oscorp's business context and risk profile.

1.2 Key Findings

Strengths Identified

- Use of Microsoft Azure and Office 365 cloud platforms
- Next-generation firewalls and network segmentation
- Regular backups and disaster recovery testing
- Physical security controls (CCTV and facility monitoring)
- Complex password policies

Critical Weaknesses Identified

- No Multi-Factor Authentication (MFA)
- Shared privileged accounts and lack of PAM
- No centralized monitoring or SIEM
- No formal incident response process
- Weak governance and absence of cyber security strategy
- No data classification or DLP controls

- No third-party risk management framework

1.3 Overall Security Maturity Assessment

Domain	Maturity Level
Governance & Strategy	Low
Identity & Access Management	Low
Monitoring & Detection	Low
Incident Response	Low
Data Security	Low
Vulnerability Management	Medium-Low
Network Security	Medium
Business Continuity & Recovery	Medium
Overall Security Posture	**Low to Medium**

Table 1: Security Maturity Assessment Summary

---

2. Scope and Methodology

2.1 Scope of Assessment

The assessment covered the following areas:

- Governance and security strategy
- Asset management
- Risk management
- Identity and access management (IAM)
- Network and cloud security
- Vulnerability management
- Data security
- Third-party risk management
- Incident detection and response
- Policies and procedures
- Business continuity and disaster recovery

In-Scope Systems

- Microsoft Azure Cloud
- Microsoft Office 365
- Active Directory
- Endpoint devices (laptops)
- Network infrastructure (firewalls, VLANs)
- Horizon Labs SaaS application
- Security tools (Qualys, Microsoft Defender)
- Backup systems

2.2 Assessment Framework

The assessment was conducted using:

- NIST Cybersecurity Framework (CSF)
- NIST SP 800-53 Rev. 5 control catalog
- Risk-based GRC methodology

2.3 Assessment Approach

The assessment followed a structured GRC lifecycle:

1. Asset Identification and Classification
2. Risk Assessment

3. Current State Control Assessment (NIST-based)
4. Gap Analysis
5. NIST Control Mapping
6. Control Effectiveness Evaluation
7. Policy and Procedure Mapping
8. Target State Definition (IST)
9. Recommendations and Roadmap

---

3. Asset Inventory and Classification

3.1 Objective

The objective of asset identification was to determine critical business, information, and technology assets that support Oscorp's operations and to evaluate their business impact.

3.2 Key Assets Identified

Critical Assets

Asset	Category	Criticality
Microsoft Azure Cloud	Cloud Infrastructure	Critical
Active Directory	Identity System	Critical
Horizon Labs SaaS	Third-Party Application	Critical
Microsoft Office 365	SaaS Platform	High
Network Infrastructure	IT Infrastructure	High
Backup Systems	Data Protection	High

Table 2: Critical Assets

Supporting Assets

Asset	Category	Criticality
Employee Laptops	Endpoints	Medium
Palo Alto Firewalls	Network Security	High
Qualys Scanner	Security Tool	Medium
Microsoft Defender	Security Tool	Medium
VPN Solution	Remote Access	High

Table 3: Supporting Assets

3.3 Asset Classification Summary

Assets were classified based on Confidentiality, Integrity, and Availability (CIA).

Classification	Description
Critical	Severe business impact if compromised
High	Major operational impact
Medium	Moderate impact
Low	Minimal impact

Table 4: Asset Classification Criteria

---

4. Risk Assessment

4.1 Risk Assessment Approach

Risks were identified by analyzing threats and vulnerabilities associated with Oscorp's assets. Each risk was evaluated based on likelihood and impact.

4.2 Key Risks Identified

Risk Area	Description	Risk Level
Unauthorized Access	No MFA and shared admin accounts	Critical
Data Breach	No DLP or data classification	Critical
Undetected Attacks	No SIEM or monitoring	Critical
Weak Governance	No cyber strategy or roles	High
Vulnerability Exploitation	Ad-hoc vulnerability management	High
Third-Party Risk	No vendor risk assessment	High
Weak Incident Response	No IR plan or playbooks	High

Table 5: Key Risk Register

---

5. Current State Control Assessment (NIST)

5.1 Overview

Oscorp's current controls were assessed against the NIST Cybersecurity Framework across five functions:

- Identify
- Protect
- Detect
- Respond
- Recover

5.2 Current State Summary

NIST Function	Status
Identify	Weak
Protect	Partially Implemented
Detect	Weak
Respond	Weak
Recover	Moderate

Table 6: NIST CSF Function Assessment

Example Findings

- Identity controls are weak due to absence of MFA and PAM.
- Monitoring controls are insufficient due to lack of SIEM.
- Recovery controls are relatively mature due to backups and DR testing.

---

6. Gap Analysis

6.1 Overview

Gap analysis identifies differences between Oscorp's current security posture and NIST-required controls.

6.2 Key Gaps Identified

Domain	Current State	Required State	Gap Severity
Identity Management	No MFA	MFA enforced	Critical
Monitoring	No SIEM	Centralized SIEM	Critical
Incident Response	No IR plan	Formal IR process	High
Governance	No cyber strategy	Defined strategy	High
Data Security	No DLP	Data classification & DLP	Critical
Third-Party Risk	No TPRM	Vendor risk program	High

Table 7: Gap Analysis Summary

---

7. NIST Control Mapping

7.1 Purpose

NIST control mapping identifies specific controls required to address identified gaps and risks.

7.2 Example Control Mapping

Risk	NIST Controls
Unauthorized Access	IA-2, AC-2, AC-6, IA-5
Data Breach	SC-28, MP-6, SI-12
Lack of Monitoring	AU-2, AU-6, SI-4
Weak Governance	PL-1, PL-2, PM-1
Third-Party Risk	SR-2, SR-3, SA-9

Table 8: Risk to NIST Control Mapping

---

8. Control Effectiveness Evaluation

8.1 Overview

Existing controls were evaluated based on implementation status and effectiveness.

8.2 Control Effectiveness Summary

Control	Status	Effectiveness
Firewall	Implemented	Medium
Backup & DR	Implemented	High
VPN	Implemented	Medium
MFA	Not Implemented	Low
SIEM	Not Implemented	Low
Incident Response	Not Implemented	Low

Table 9: Control Effectiveness Evaluation

---

9. Policy and Procedure Mapping

9.1 Overview

Policies were mapped against NIST control requirements.

9.2 Policy Status Summary

Policy Area	Status
Information Security Policy	Weak
Access Control Policy	Missing
Authentication Policy	Missing
Incident Response Policy	Missing
Logging Policy	Missing
Third-Party Risk Policy	Missing
Backup & DR Policy	Exists

Table 10: Policy Status Assessment

---

10. Information Security Target State (IST)

10.1 Objective

The IST defines Oscorp's desired future security posture aligned with NIST standards.

10.2 Target State Vision

Domain	Current State	Target State
IAM	No MFA	MFA + PAM + RBAC
Monitoring	No SIEM	Centralized SIEM
Governance	No strategy	Formal cyber strategy
Data Security	No DLP	Data classification + DLP
Incident Response	Ad-hoc	Formal IR framework
Third-Party Risk	None	Structured TPRM program

Table 11: Current State vs Target State

---

11. Recommendations and Roadmap

11.1 Phase-Based Roadmap

Phase 1: Quick Wins (0–3 Months)

- Deploy MFA across Azure AD and VPN
- Eliminate shared admin accounts
- Develop core security policies
- Formalize vulnerability management process

Phase 2: Core Security Controls (3–6 Months)

- Implement SIEM and centralized logging
- Develop incident response framework
- Implement data classification and DLP
- Establish third-party risk assessment process

Phase 3: Security Maturity & Optimization (6–12 Months)

- Deploy PAM solution
- Enhance SOC capabilities
- Conduct regular security audits and risk assessments
- Implement security awareness programs

11.2 Prioritization Rationale

Recommendations were prioritized based on:

- Risk severity
- Asset criticality
- Business impact
- Regulatory exposure
- Implementation feasibility

---

12. Business Impact and Value

Implementing the recommended controls will:

- Reduce risk of account compromise and data breaches
- Improve detection and response capability
- Strengthen governance and accountability
- Enhance resilience against cyber incidents
- Improve stakeholder and customer trust

---

13. Conclusion

This GRC assessment demonstrates that Oscorp's current cyber security posture is at a low to medium maturity level. However, by implementing the recommended controls and roadmap, Oscorp can significantly improve its security posture and align with NIST standards in a structured and realistic manner.

The proposed roadmap provides Oscorp with a practical path to achieve its target security state while balancing security requirements with business constraints typical of an SME environment.

---

14. Appendix

A. Mapping Between Deliverables

Deliverable	Purpose
Asset Inventory	Identify critical assets
Risk Register	Identify key risks
NIST Assessment	Evaluate current controls
Gap Analysis	Identify missing controls
Control Mapping	Map risks to NIST controls
IST	Define future state
Roadmap	Plan implementation

Table 12: Deliverable Mapping

Document Control

Version	1.0
Date	January 30, 2026
Classification	Confidential
Distribution	Internal Use Only