NIST CYBERSECURITY FRAMEWORK

Cybersecurity Maturity Assessment and Three-Year Remediation Roadmap

Oscorp (a fictional organization used for capstone assessment training)

Prepared by J Damien Scott, SRMP GRCP ITGRC

GRC Analyst, Portfolio Demonstration

July 2026

Portfolio note: Oscorp is a fictional organization used in a capstone cybersecurity program design exercise. This document applies the NIST Cybersecurity Framework (CSF) Core to a full set of stakeholder interview notes and produces a complete, per-control maturity assessment and a three-year remediation roadmap. It is presented as a work sample demonstrating applied gap-assessment and program-design capability, not as output from an engagement with a real client or employer.

Document Control

Field	Detail
Document title	NIST Cybersecurity Framework Maturity Assessment and Three-Year Remediation Roadmap
Organization (fictional)	Oscorp
Assessment framework	NIST Cybersecurity Framework (CSF) Core, Version 1.0/1.1 structure: 5 functions, 98 subcategories
Assessment method	Structured stakeholder interviews mapped to CSF subcategories; Pass/Fail determination per control
Document owner	GRC Analyst
Reviewed by	Chief Information Security Officer (pending review)
Approved by	Chief Executive Officer / Board Risk Committee (pending approval)
Version	1.0
Status	Draft, prepared for portfolio demonstration
Classification	Internal use only

Table of Contents

1. Executive Summary

This report presents a cybersecurity maturity assessment of Oscorp, a fictional organization, conducted against the NIST Cybersecurity Framework (CSF) Core. The assessment evaluated all 98 subcategories across the five CSF functions: Identify, Protect, Detect, Respond, and Recover. Oscorp passed 26 of 98 controls, an overall compliance rate of 27 percent.

Performance is uneven across functions. Protect and Recover are the strongest areas, driven by real investments Oscorp has already made: next-generation firewalls, network segmentation, physical security, and tested disaster recovery and backup procedures. Identify and Detect are weak because the organization lacks asset classification, a functioning cyber risk process, and any monitoring capability. Respond is the most urgent gap in the entire assessment: Oscorp passed zero of fifteen Respond subcategories, meaning it has no structured way to execute, communicate, or learn from a security incident.

Third-party risk management does not appear as a native category in this version of the CSF Core, so it is treated as a supplementary finding rather than a scored subcategory. Oscorp has no third-party risk process at all, and its most critical SaaS supplier, Horizon Labs, has never been assessed.

The report closes with a three-year roadmap that sequences remediation by urgency and dependency: foundational governance and access control fixes in Year 1, detection and response capability plus third-party risk management in Year 2, and quantified risk management and continuous improvement in Year 3.

2. Purpose, Scope, and Framework Note

2.1 Purpose

The purpose of this assessment is to establish Oscorp's current cybersecurity maturity against a recognized, structured framework, to identify and prioritize gaps, and to propose a realistic, sequenced roadmap for remediation. The assessment is based entirely on structured interviews with Oscorp stakeholders across IT, cybersecurity, risk, and procurement functions.

2.2 Scope

The assessment covers Oscorp's cybersecurity program in full: asset management, governance, risk management, access control, data security, vulnerability management, third-party risk, detection, incident response, and disaster recovery. It does not include a technical penetration test or vulnerability scan; findings are based on interview evidence and the existence or absence of documented processes.

2.3 Framework Note: Version and Scope of the CSF Core Used

This assessment applies the NIST Cybersecurity Framework Core exactly as structured in CSF Version 1.0/1.1: five functions (Identify, Protect, Detect, Respond, Recover) comprising 98 subcategories. NIST released CSF 2.0 in February 2024, which adds a sixth function, Govern, and elevates supply chain risk management to its own category (GV.SC) rather than treating it as a footnote. This assessment predates that restructuring and follows the five-function, 98-subcategory Core. As a result, findings related to third-party and supply chain risk are presented in Section 6.3 as a supplementary finding rather than as a native, scored CSF

subcategory. This distinction matters for anyone comparing this assessment against a CSF 2.0-based report: the compliance percentages here are not directly comparable to a CSF 2.0 assessment, since the denominators and category structure differ.

3. Current State: Stakeholder Interview Findings

The findings below summarize what Oscorp stakeholders reported during the assessment interviews, organized by domain. These findings are the raw evidence base from which the per-control determinations in Section 5 were made.

Domain	Current state, as reported by stakeholders
Team structure	A generalist cybersecurity analyst and a network engineer report through IT and network management lines respectively; a new cybersecurity consultant role reports to the IT Manager. There is no independent security function.
Asset management	IT maintains a spreadsheet of laptop serial numbers, models, and warranty data only. No CMDB or comprehensive asset inventory exists. All applications are SaaS (Microsoft 365), and all data resides in Microsoft Azure. A Secure Operating Environment (SOE) image is used for laptop builds.
Business continuity and disaster recovery	Disaster recovery testing is conducted regularly, business continuity plans are documented, and backups are taken and periodically tested.
Vulnerability management	A Qualys vulnerability scanner has been purchased but is used only on an ad hoc basis. No formal program exists, and Qualys reports a large number of high and severe findings.
Risk management	A risk team exists but performs financial risk activities only. No technology or cyber risk process exists.
Third-party risk management	No TPRM process exists. Contracts are reviewed by procurement and finance only; IT is not involved. The key critical application is a SaaS service from Horizon Labs, which has never been assessed.
Identity and access management	Microsoft Active Directory manages users and groups. No privileged access management (PAM) solution exists. An administrator account password is shared among a few senior IT staff. Access is granted on request with no formal process or periodic access reviews. No multi-factor authentication (MFA) is in place, though password complexity requirements exist. A VPN is available for remote access.
Network security	Palo Alto next-generation firewalls are configured, audited annually, and regularly updated. Network diagrams, including the cloud environment, are current. The network is segmented using VLANs.
Physical security	State-of-the-art CCTV covers the facility, employee vetting is extensive, and research labs and physical facilities are monitored 24/7.
Data security	No Data Loss Prevention (DLP) solution exists. All data resides in Microsoft Azure and Microsoft 365.
Policy	A single generic IT policy exists. There is no formal information security policy and no data governance or information classification framework.
Detection and response	No detection or response capability exists. The IT team reacts only to Microsoft Defender antivirus alerts. No Security Information and Event Management (SIEM) platform is in place.
Security awareness	All employees complete a basic cybersecurity module during induction. No ongoing or periodic training program exists.

4. Assessment Results Summary

Each of the 98 CSF subcategories was assessed as Pass or Fail based on the interview findings in Section 3. Results are summarized by function below; full per-control results appear in Section 5.

NIST function	Controls	Pass	Fail	Compliance
Identify	24	4	20	17%
Protect	35	16	19	46%
Detect	18	3	15	17%
Respond	15	0	15	0%
Recover	6	3	3	50%
Total	98	26	72	27%

Protect (46 percent) and Recover (50 percent) are the strongest functions, reflecting genuine investment in firewalls, network segmentation, physical security, backups, and disaster recovery testing. Identify (17 percent) and Detect (17 percent) are weak because Oscorp lacks asset classification, a cyber risk process, and any monitoring capability. Respond (0 percent) is the single most urgent finding: with no incident response plan, no defined roles, and no forensic capability, Oscorp cannot currently manage a security incident in a structured way.

Note on controls marked Pass despite limited program maturity: several Protect subcategories, including the separation of development and production environments, the System Development Life Cycle control, and hardware maintenance controls, were rated Pass because Oscorp is SaaS-only and does not perform in-house development or maintain physical servers. These represent an absence of the associated risk rather than a demonstrated control. One control, PR.DS-6 (integrity checking), reflects a control type that has been de-emphasized in more recent NIST guidance; it is retained here as Pass, consistent with the source assessment, but should not be read as a modern best-practice benchmark.

5. Detailed Per-Control Assessment

The following tables record the Pass or Fail result for every one of the 98 CSF subcategories assessed, organized by function.

5.1 Identify (24 subcategories)

Ref.	Subcategory	Result
ID.AM-1	Physical devices and systems within the organization are inventoried.	Pass
ID.AM-2	Software platforms and applications within the organization are inventoried.	Fail
ID.AM-3	Organizational communication and data flows are mapped.	Pass
ID.AM-4	External information systems are catalogued.	Fail
ID.AM-5	Resources (hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value.	Fail
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (suppliers, customers, partners) are established.	Fail
ID.BE-1	The organization's role in the supply chain is identified and communicated.	Fail
ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated.	Fail
ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated.	Pass

Ref.	Subcategory	Result
ID.BE-4	Dependencies and critical functions for delivery of critical services are established.	Pass
ID.BE-5	Resilience requirements to support delivery of critical services are established.	Fail
ID.GV-1	Organizational information security policy is established.	Fail
ID.GV-2	Information security roles and responsibilities are coordinated and aligned with internal roles and external partners.	Fail
ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	Fail
ID.GV-4	Governance and risk management processes address cybersecurity risk.	Fail
ID.RA-1	Asset vulnerabilities are identified and documented.	Fail
ID.RA-2	Threat and vulnerability information is received from information sharing forums and sources.	Fail
ID.RA-3	Threats, both internal and external, are identified and documented.	Fail
ID.RA-4	Potential business impacts and likelihoods are identified.	Fail
ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	Fail
ID.RA-6	Risk responses are identified and prioritized.	Fail
ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders.	Fail
ID.RM-2	Organizational risk tolerance is determined and clearly expressed.	Fail
ID.RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis.	Fail

5.2 Protect (35 subcategories)

Ref.	Subcategory	Result
PR.AC-1	Identities and credentials are managed for authorized devices and users.	Fail
PR.AC-2	Physical access to assets is managed and protected.	Pass
PR.AC-3	Remote access is managed.	Fail
PR.AC-4	Access permissions are managed, incorporating the principles of least privilege and separation of duties.	Fail
PR.AC-5	Network integrity is protected, incorporating network segregation where appropriate.	Pass
PR.AT-1	All users are informed and trained.	Fail
PR.AT-2	Privileged users understand roles and responsibilities.	Fail
PR.AT-3	Third-party stakeholders (suppliers, customers, partners) understand roles and responsibilities.	Fail
PR.AT-4	Senior executives understand roles and responsibilities.	Fail
PR.AT-5	Physical and information security personnel understand roles and responsibilities.	Fail
PR.DS-1	Data-at-rest is protected.	Fail
PR.DS-2	Data-in-transit is protected.	Fail
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition.	Fail
PR.DS-4	Adequate capacity to ensure availability is maintained.	Pass
PR.DS-5	Protections against data leaks are implemented.	Fail

Ref.	Subcategory	Result
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity.	Pass
PR.DS-7	The development and testing environment(s) are separate from the production environment.	Pass
PR.IP-1	A baseline configuration of information technology and industrial control systems is created and maintained, incorporating security principles.	Pass
PR.IP-2	A System Development Life Cycle to manage systems is implemented.	Pass
PR.IP-3	Configuration change control processes are in place.	Fail
PR.IP-4	Backups of information are conducted, maintained, and tested periodically.	Pass
PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met.	Pass
PR.IP-6	Data is destroyed according to policy.	Fail
PR.IP-7	Protection processes are continuously improved.	Fail
PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties.	Fail
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	Pass
PR.IP-10	Response and recovery plans are tested.	Pass
PR.IP-11	Cybersecurity is included in human resources practices (deprovisioning, personnel screening).	Pass
PR.IP-12	A vulnerability management plan is developed and implemented.	Fail
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	Pass
PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	Pass
PR.PT-1	Audit and log records are determined, documented, implemented, and reviewed in accordance with policy.	Fail
PR.PT-2	Removable media is protected and its use restricted according to policy.	Fail
PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality.	Pass
PR.PT-4	Communications and control networks are protected.	Pass

5.3 Detect (18 subcategories)

Ref.	Subcategory	Result
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed.	Fail
DE.AE-2	Detected events are analyzed to understand attack targets and methods.	Fail
DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors.	Fail
DE.AE-4	Impact of events is determined.	Fail
DE.AE-5	Incident alert thresholds are established.	Fail
DE.CM-1	The network is monitored to detect potential cybersecurity events.	Fail
DE.CM-2	The physical environment is monitored to detect potential cybersecurity events.	Pass
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events.	Fail
DE.CM-4	Malicious code is detected.	Pass

Ref.	Subcategory	Result
DE.CM-5	Unauthorized mobile code is detected.	Pass
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events.	Fail
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.	Fail
DE.CM-8	Vulnerability scans are performed.	Fail
DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability.	Fail
DE.DP-2	Detection activities comply with all applicable requirements.	Fail
DE.DP-3	Detection processes are tested.	Fail
DE.DP-4	Event detection information is communicated to appropriate parties.	Fail
DE.DP-5	Detection processes are continuously improved.	Fail

5.4 Respond (15 subcategories)

Ref.	Subcategory	Result
RS.RP-1	Response plan is executed during or after an event.	Fail
RS.CO-1	Personnel know their roles and order of operations when a response is needed.	Fail
RS.CO-2	Events are reported consistent with established criteria.	Fail
RS.CO-3	Information is shared consistent with response plans.	Fail
RS.CO-4	Coordination with stakeholders occurs consistent with response plans.	Fail
RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	Fail
RS.AN-1	Notifications from detection systems are investigated.	Fail
RS.AN-2	The impact of the incident is understood.	Fail
RS.AN-3	Forensics are performed.	Fail
RS.AN-4	Incidents are categorized consistent with response plans.	Fail
RS.MI-1	Incidents are contained.	Fail
RS.MI-2	Incidents are mitigated.	Fail
RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks.	Fail
RS.IM-1	Response plans incorporate lessons learned.	Fail
RS.IM-2	Response strategies are updated.	Fail

5.5 Recover (6 subcategories)

Ref.	Subcategory	Result
RC.RP-1	Recovery plan is executed during or after an event.	Pass
RC.IM-1	Recovery plans incorporate lessons learned.	Fail
RC.IM-2	Recovery strategies are updated.	Pass
RC.CO-1	Public relations are managed.	Fail
RC.CO-2	Reputation after an event is repaired.	Fail
RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams.	Pass

6. Key Findings

6.1 Existing Strengths to Preserve

Oscorp should preserve and build on several genuine strengths identified in this assessment: strong physical security (CCTV, 24/7 monitoring, employee vetting); solid network infrastructure (Palo Alto next-generation firewalls, VLAN segmentation, annual firewall audits); current network documentation, including the cloud environment; tested business continuity and disaster recovery with regularly tested backups; and a Secure Operating Environment image for laptop builds. Any remediation roadmap should treat these as a foundation, not as areas requiring rework.

6.2 Current Deficiencies by Function

Governance and Identify (17 percent compliance): no information security policy, no asset classification, no cyber risk process, no risk appetite statement, no defined security roles, and unmanaged regulatory obligations.

Protect (46 percent compliance): no multi-factor authentication; a shared administrator password; no privileged access management; no formal access reviews or least-privilege enforcement; no Data Loss Prevention; onboarding-only awareness training; no supplier security requirements; and no change management or secure data disposal process.

Detect (17 percent compliance): no SIEM; no monitoring of network, systems, or personnel activity; no alert thresholds or escalation procedures; and no monitoring of external service provider activity.

Respond (0 percent compliance): no incident response plan, no defined roles, no forensic capability, no communication protocols, and no lessons-learned cycle. This is the most urgent gap in the assessment.

Recover (50 percent compliance): disaster recovery and backups are tested, but there is no crisis communications or reputation-repair capability and no lessons-learned step feeding back into recovery planning.

6.3 Supplementary Finding: Third-Party Risk

Third-party and supply chain risk management does not exist as a scored category in the version of the CSF Core applied in this assessment (see Section 2.3), so this finding is reported separately rather than folded into the compliance percentages above. Oscorp has no third-party risk management process. Contracts are reviewed only by procurement and finance, with no cybersecurity input. Horizon Labs, the supplier of Oscorp's key critical SaaS application, has never been assessed for security posture and carries no contractual security clauses. Under the classification model used elsewhere in this candidate's portfolio work, Horizon Labs would be tiered as a Tier 1 supplier: it holds a service so critical that its disruption would stop core business operations, which places it in the highest-priority category for immediate assessment.

7. Three-Year Remediation Roadmap

The roadmap below sequences remediation by urgency and dependency. Foundational work in Year 1 is a prerequisite for the detection and response capability built in Year 2, which in turn supports the quantified, continuously improving program targeted for Year 3.

7.1 Year One: Foundations and Quick Wins

Theme: establish governance, close the most dangerous gaps, and build the asset and policy foundations everything else depends on.

Priority quick wins (first 90 days):

1. Deploy multi-factor authentication across all logins, including VPN access.
2. Eliminate the shared administrator password and move to individual, attributable privileged accounts.
3. Stand up a basic incident response plan using an established template, such as the SANS incident handling process.
4. Activate the existing Qualys scanner on a fixed schedule and begin clearing the high and severe vulnerability backlog.

Foundational work (full year):

1. Define cybersecurity roles and responsibilities across the organization.
2. Develop and approve an information security policy with data governance and classification.
3. Establish a cyber risk process, including a risk register and a management-endorsed risk appetite statement.
4. Build and classify a complete asset inventory spanning hardware, SaaS applications, and data.
5. Document legal and regulatory obligations relevant to cybersecurity.
6. Formalize the vulnerability management program beyond ad hoc scanning.
7. Launch recurring security awareness training with phishing simulations.

Target by end of Year 1: governance is established and critical access gaps are closed. Posture moves from Tier 1 toward Tier 2 on the NIST CSF implementation tier scale.

7.2 Year Two: Detection, Response, and Third-Party Risk

Theme: gain visibility, build the ability to respond, and manage supplier risk.

1. Implement a SIEM and onboard logs from cloud services, endpoints, firewalls, and identity systems.
2. Establish a monitoring and detection capability, whether internal, outsourced to a managed security service provider, or hybrid, with defined alert thresholds and escalation paths.
3. Mature incident response with a full plan, communication protocols, tabletop exercises, and forensic support.
4. Build a third-party risk management program: supplier inventory, tiering, assessments, and contractual security clauses including breach notification and ongoing monitoring, prioritizing Horizon Labs as a Tier 1 supplier.
5. Deploy Data Loss Prevention and restrict removable media.
6. Complete the privileged access management implementation begun in Year 1.
7. Introduce change management and secure data disposal procedures.
8. Conduct the first independent network penetration test, with tracked remediation of findings.

Target by end of Year 2: Oscorp can detect, respond to, and recover from incidents, and it actively manages supplier risk. Posture reaches Tier 2, approaching Tier 3.

7.3 Year Three: Maturity and Continuous Improvement

Theme: optimize, measure, and embed continuous improvement.

1. Introduce cyber risk quantification, using a model such as FAIR (Factor Analysis of Information Risk), for the highest-priority risks so investment decisions are expressed in financial terms.
2. Establish regular penetration testing and at least one annual red team exercise, rotating providers between cycles.
3. Mature detection through continuous tuning and the incorporation of threat intelligence.
4. Embed lessons-learned cycles across incident response and disaster recovery, including crisis communications.
5. Formalize continuous-improvement reviews with metrics reported to leadership and the board.
6. Pursue an external assurance milestone, such as ISO/IEC 27001 alignment or certification.
7. Review the cybersecurity team structure with a view toward a dedicated security function independent of IT operations.

Target by end of Year 3: a repeatable, risk-informed, continuously improving program. Posture reaches Tier 3, with elements of Tier 4.

7.4 Roadmap at a Glance

Year	Focus	Key outcomes
Year 1	Foundations and quick wins	MFA; remove shared admin password; basic incident response plan; governance and policy; asset classification; cyber risk process; formal vulnerability management; awareness training
Year 2	Detection, response, third-party risk	SIEM and monitoring; mature incident response with exercises; third-party risk program; DLP; PAM completion; change management; first penetration test
Year 3	Maturity and continuous improvement	Cyber risk quantification (FAIR); regular penetration testing and red teaming; detection tuning; lessons-learned cycles; ISO/IEC 27001 alignment; security team structure review

8. Conclusion and Recommendation

Oscorp's cybersecurity program is at an early stage of maturity, passing 27 percent of the NIST CSF Core subcategories assessed. The organization has made real, defensible investments in physical security, network infrastructure, and disaster recovery, and this roadmap deliberately builds on those investments rather than discarding them. The most urgent priority is Respond: an organization with no incident response capability cannot manage a security event in a structured way regardless of how strong its preventive controls are, and a single unmanaged incident could erase the value of every other control in place today.

The recommended sequence, governance and access control first, then detection and response and third-party risk, then quantified and continuously improving management, reflects genuine

dependency rather than an arbitrary schedule: an organization cannot detect what it has not inventoried, and it cannot respond to what it cannot detect. Following this roadmap would move Oscorp from an ad hoc, reactive security posture today to a managed, risk-informed program within three years.

Appendix A: Glossary of Key Terms

Term	Definition
CSF Core	The set of Functions, Categories, and Subcategories in the NIST Cybersecurity Framework that describe desired cybersecurity outcomes, independent of any specific implementation tier.
DLP	Data Loss Prevention: technology and process controls that detect and prevent unauthorized transmission of sensitive data outside the organization.
Implementation Tier	A NIST CSF construct (Tier 1 Partial through Tier 4 Adaptive) describing how well an organization's cyber risk management practices exhibit the characteristics defined in the framework, distinct from a maturity model but often used similarly in practice.
MFA	Multi-Factor Authentication: an authentication method requiring more than one independent credential to verify identity.
PAM	Privileged Access Management: controls governing access by users with elevated system permissions, such as administrators.
SIEM	Security Information and Event Management: a platform that aggregates and analyzes security log data from across the environment to support detection.
Subcategory	The most granular element of the CSF Core; a specific outcome statement (for example, ID.AM-1) against which an organization's practice is assessed.
TPRM	Third-Party Risk Management: the process of managing cybersecurity risk posed by suppliers, vendors, and external service providers.

References

Factor Analysis of Information Risk (FAIR) Institute. (2023). FAIR risk taxonomy and standard.

International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection: Information security management systems: Requirements (ISO/IEC 27001:2022).

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, Version 1.1.

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0.

SANS Institute. (2023). Incident handler's handbook.

Verizon. (2023). Data breach investigations report.