ITMS 478-578

University Cybersecurity Program Audit

Title: Audit Report for Illinois Institute of Technology

Institution: Illinois Institute of Technology

Date: 11/20/2024

Documents Audited by:

Pierre Lopez	**:**	**Media Protection Plan**
Radha Prabhakaran	**:**	**System and Communications Protection Plan**
Mahesh Nutheti	**:**	**Vulnerability Management Plan**
Bhargavi Punnam	**:**	**Vulnerability Management Policy**
Avery Huerta	**:**	**Vulnerability Management Standard**

Table of contents

1.Executive summary

Purpose: The audit of the document *Vulnerability Management Standards* was conducted to evaluate and ensure that the documentation complied with *NIST Special Publication 800-171A* for the organization of Illinois Institute of Technology. Specifically in compliance with risk and vulnerability assessment procedures. Processes such as identifying, evaluating, mitigating, and reporting vulnerabilities.

Scope: The scope of this audit is to ensure the compliance of the documents of the Illinois Institute of Technology with *NIST Special Publication 800-171A Rev.3*.

This audit covers the following areas:

- Media Protection Plan
- System and Communications Protection Plan
- Vulnerability Management Plan
- Vulnerability Management Policy
- Vulnerability Management Standard

Key findings

- **Media Protection Plan**: Media labeling and marketing procedures may fail to ensure proper identification without revealing data.
- **System and Communications Protection Plan:** It lacks comprehensive enforcement and monitoring for secure boundary protection, cryptographic key management, and sessions controls.
- **Vulnerability Management Plan:** Unscheduled network-based scanning produces inconsistent results and exposes the vulnerability at a later point of time than it should.
- **Vulnerability Management Policy :** There is the need to enhance risk update procedures, protection against malicious code and structured assessments.
- **Vulnerability Management Standard**: They need to state when vulnerability tools are updated regularly to ensure new vulnerabilities can be identified.

Recommendations

1. Enhance Sanitization Procedures.
2. Include automated boundary monitoring, FIPS compliant cryptographic storage, session timeout policies and full control over mobile code and collaborative devices.

3. Develop comprehensive network profiling to then properly schedule a regular, automated network scanning schedule to identify and address vulnerabilities as they rapidly appear.
4. Update of these baseline configurations. Limit which ports, protocols, and services an organization's systems can use to slash exposure to malicious attacks , and by improving the external and internal security.
5. **Tools to add:** Security Information and Event Management (SIEM) systems, Intrusion Detection/Prevention Systems (IDS/IPS), and log analyzers.

2. Introduction

Purpose:

This audit evaluated the effectiveness and compliance of the *Illinois Institute of Technology's* vulnerability management and associated security policies with *NIST Special Publication 800-171A Rev. 3.* The objective of this audit is to determine areas in which the institute could improve for risk assessments and adherence to security controls and standards to protect *Controlled Unclassified Information (CUI).*

Scope:

This audit scope has been defined as the review of the Media Protection Plan, System and Communications Protection Plan, Vulnerability Management Plan, Vulnerability Management Policy, and Vulnerability Management Standard. These documents will be examined for alignment with *NIST SP 800-171A Rev. 3* and will be assessed those vulnerabilities and that remediation and risk management processes.

3. Scope and Objectives

Scope:

The audit will assess policies and practices relative to media protection, system and communications protection, and vulnerability management as they relate to the *Illinois Institute of Technology.* It means reviewing the vulnerability scanning processes, risk assessments, asset tracking, vulnerability remediation strategies in place in the institution's security planning and security policy.

Objectives:

To evaluate management of vulnerabilities and protection of CUI to determine the institution's compliance with *NIST SP 800-171A Rev. 3*. To identify weakness and insertion of vulnerability management practices such as asset tracking, vulnerability scanning, and remediation timelines.

Actionable recommendations for improving alignment between the institution's policies and NIST standards are provided that will improve overall cybersecurity posture.

4. Summary of Findings

Media Protection Plan

- Access to physical media is restricted to authorized personnel (MP-2).
- Media storage is secure and on-site (MP-4).
- Media transport follows encryption guidelines (MP-5).
- Media protection is documented with defined roles and a review process.
- Weaknesses include gaps in documentation for external contractor transport and lack of logging/review of media storage access (MP-2).
- Limited staff training increases the risk of human error.
- Media labeling and marketing procedures may fail to ensure proper identification without revealing data.

System and Communications Protection Plan

- System and user functionalities are logically and physically separated as per NIST requirements but do not provide any testing metrics for isolation boundaries.
- Resource prioritization and monitoring is included to manage denial-of service attacks, but automated response thresholds are undefined.
- Proxy servers and extrusion detection for boundary protection align with standards, however split tunneling exceptions require stricter documentation.
- Cryptographic key lifecycle management is established but auditing third party operations and fallback mechanisms are not specified.
- Enhancing session authenticity with unique session identifiers is not enough; logout enforcement or termination audits are not enough.

Vulnerability Management Plan

- Delay due to network-based scan scheduling.

- Lack of consistent documentation for real time Remediation Tracking.
- Limited benchmarks for trailing remediation timings.
- Uncertain update inconsistencies in the tracking of assets.
- Lacking the documentation for secure decommissioning of assets.
- Lack of standardization of documenting compensating controls.

- Acceptable risk defined in terms of undefined criteria and approval process.
- Lack of verification of those high-risk asset categories.

Vulnerability Management Policy

- The policy lacks a structured approach for risk acceptance, with no clearly defined criteria for evaluating and approving residual risks. This gap in guidance can lead to inconsistent decision-making regarding acceptable risks across different systems and assets.
- Risk mitigation processes are inconsistently applied and do not account for new and evolving threats.
- The absence of a regular review or update mechanism for these processes poses a risk to maintaining effective defenses against current vulnerabilities.
- Documentation of compensating controls is not standardized, leading to variability in how compensatory measures are recorded and applied across assets. This inconsistency may result in some assets having insufficient protective controls, increasing their vulnerability to threats.

Vulnerability Management Standard

- The document has a timeline of when systems should be scanned regularly and has a policy to scan the system when new vulnerabilities are found.
- Document gives a thorough description of who should handle the vulnerability if one is found.
- The document states that all vulnerabilities should be overseen by the Asset Owner if they are identified anywhere in the organization as regulated in *Risk Response 03.11.04.*
- The document does discuss when systems should be scanned for vulnerabilities in the system configurations. Found in Systems to Scan and Scanning Tool Requirements as regulated in *Baseline Configuration 03.04.01.*
- The document does not specifically address the process in which CUI information is managed through the organization.

- The document does not go into detail about monitoring, updating, and configurations of systems, and applications, such as vulnerability scanning tools.

5.Detailed findings

Media Protection Plan:

Observations:

- **A.03.08.02.ODP[01]:** Access to physical media and storage facility is defined per the media access requirement to authorized personnel only.
- **A.03.08.04.ODP[02]:** Storage is also secure at media storage locations, including storage on site as it is in data centers that meet secure storage standards.
- **A.03.08.05.ODP[01]:** For media transport, in particular encryption, there are guidelines for security transport.
- **A.03.08.04.a[03]:** High quality media protection documentation exists, including roles, responsibilities, and defined review process.
- **A.03.08.02.ODP[02]:** The documentation gaps that may have risks associated with external contractor's media transportation.
- **A.03.08.02.a[04]:** A lack of clear logging or audit of access to media storage areas may result in unauthorized access and therefore undermine compliance with an access control requirement.
- **A.03.08.03.a[01]:** Inability of a large number of personnel to be appropriately trained and aware, potentially increasing errors by people.
- **A.03.08.03.ODP[01]:** The procedures for labeling and marking media may not result in identification of the media without disclosing sensitive data.

Shortfalls:

- **A.03.08.05.b[01]:** Specific insufficient incident response procedure specifically for media protection, which may prolong containment in the event of a breach.
- **A.03.08.04.c[02]:** Unclear oversight of these off-site vendors of potentially sensitive data to risks.

System and Communications Protection Plan

Observations:

- **A.03.13.05.a[01]:** Layered architectures are used to logically isolate system management functions from user functionalities, modular cohesion is applied to improve cohesion, and hardware-based segmentation is used to help avoid vulnerabilities.
- **A.03.13.05.b[01]:** Resource allocation by quotas, bandwidth management and monitoring tools to detect potential attack indicators are measures to protect denial of service.
- **A.03.13.07.a[02]:** Secure routing is enforced through boundary protection 'proxy servers', 'managed interfaces and intrusion detection'. That is to prevent data exfiltration or unauthorized access on outgoing traffic.
- **A.03.13.11.b[02], A.03.13.12.c[01]:** Cryptographic key lifecycle management combines secure key generation, storage, distribution, and destruction. Physical security measures and symmetric key controls are put in place that govern keys externally stored.
- **A.03.13.23.a[01]:** Session authenticity is implemented using system generated, unique session identifiers, and trusted certificate authorities. On termination, session identifiers are invalidated.

Shortfalls:

- **A.03.13.05.a[01]:** There are no established performance metrics or testing procedures to verify isolation boundaries against performance under operational conditions.
- **A.03.13.05.b[01]:** Thresholds define denial of service response automation and no simulation testing for large scale attacks exists.
- **A.03.13.07.a[02]:** Split tunneling in SSL VPNs is not comprehensively due. Periodic reviews are not built into boundary access policies.
- **A.03.13.11.b[02], A.03.13.12.c[01]:** The audits are not mandated for third party cryptographic operation. No such defined fallback strategy is used in case of compromised or corrupted keys.
- **A.03.13.23.a[01]:** The mechanism of enforcement of session termination does not get defined, nor does the audit trail for the tasks to be validated if logout were complete.

Vulnerability Management Plan

Observations:

- **A.03.11.02.ODP[01]:** The inconsistency in scheduling the scanning process based on the network leads to late vulnerabilities identification, therefore may lead to an increase of the exposure risk of the system.
- **A.03.11.02.ODP[02]:** Documentation of remediation tracking is too incomplete and too unclear. The progress of remediation actions, as well as the corresponding timelines, are not defined and are not tracked using benchmarks or processes.

- **A.03.11.02.ODP[03]:** Because of inconsistent asset tracking updates, part of vulnerability assessments often falls through the gaps, leaving room for unmonitored or untracked vulnerabilities.
- **A.03.04.04.a[01]:** The procedure of asset decommissioning is not sufficiently documented. There is not as clear a definition of secure decommissioning practices as should be the case, which puts at risk that important systems will remain exposed post decommissioning.

- **A.03.14.01.ODP[01]:** Compensating controls are not systematically formalized or consistently documented across systems, thereby severely lacking in a contingent manner, causing inconsistency in security measures where there is a vulnerability that cannot be immediately remedied.
- **A.03.11.02.a[01]:** Without clearly defined criteria and relative approval processes for acceptable risks, the plan is ambiguous on the risk management side, and it is not noticeably clear how one can be certain to take the same risk mitigation approach.
- **A.03.11.02.a[02]:** Such high risk asset category potential vulnerabilities are not properly verified, resulting in higher likelihood of undetected vulnerabilities in critical systems.

Shortfalls:

- **A.03.11.02.ODP[01]:** Network scans are inappropriately scheduled, with no consistent record of what it scans for, hence the delay in vulnerability detection.
- **A.03.11.02.ODP[02]:** Gaps within the vulnerability management process remain due to the lack of documentation regarding real time remediation tracking, preventing effective and complete vulnerability resolution.
- **A.03.11.02.ODP[03]:** There are no set benchmarks or timelines that would say when remediation should occur, and that means vulnerabilities are not addressed as quickly and those systems are left vulnerable for long stretches.
- **A.03.04.04.a[02]:** Asset tracking updates are missing or outdated essential information for a meaningful vulnerability assessment.
- **A.03.11.02.ODP[04]:** The decommissioning of assets involves no standardized process, and current practices do not fully address the requirement for the secure removal and data protection during the decommissioning of assets.
- **A.03.14.01.ODP[02]:** Compensating controls are not formally defined or approved, and as a result, inconsistent security practice exists where some vulnerabilities simply cannot be remediated.
- **A.03.11.02.a[03]:** The definition of what constitutes acceptable risk is not made explicit in the document, and there is no formal approval procedure for approval of active and passive methods for risk acceptance and mitigation.
- **A.03.11.02.a[04]:** Missing vulnerabilities in critical systems can arise from a lack of the process for verifying vulnerabilities in high risk asset categories.

Vulnerability Management Policy

Observations :

- **A.03.11.02.ODP[02]:** The policy does not specify clear criteria for risk acceptance, leaving room for subjective judgment. This lack of structured guidance hinders consistency in risk treatment, as asset owners and managers may apply different standards when deciding which risks to accept.
- **A.03.01.ODP[03]:** Existing risk mitigation procedures are outdated and lack a defined schedule for review or updates. As a result, the policy may not adequately address the latest vulnerabilities, leaving systems exposed to newly identified threats.
- **A.03.01.ODP[01]:** The documentation and implementation of compensating controls vary across assets. This inconsistency reduces the effectiveness of the vulnerability management strategy, as not all assets benefit equally from alternative protective measures.

Shortfalls :

- **A.04.03.01:** A lack of well-defined and documented criteria and an organized process to accept risk decision making, therefore could result in inconsistent or unstructured risk management practices.
- **A.04.03.02:** There is no schedule to which regular updates to risk mitigation processes are committed until the defenses become outdated without being able to fight off evolving security threats effectively.
- **A.04.03.03:** Compensating controls are documented inconsistently across assets, potentially leaving critical holes in important assets protection, and placing a strain on the overall security measures.

Vulnerability Management Standard

Observations:

- **A.03.11.02.ODP[02]:** The document provides the description of the type of system that is being scanned, when it needs to be scanned, and the justification for why a system may

need to be scanned for vulnerabilities. Found *Systems to Scan and Scanning Tool Requirements.*

- **A.03.11.02.ODP[03]:** Prioritizes vulnerabilities based on CVE score, location of vulnerability, and how critical it is to the organization. Found in *Vulnerability Remediation.*
- **A.03.11.02.a[04]:** Although this documents states timelines for when systems should be scanned for vulnerabilities in *Systems to Scan and Scanning Tool Requirements* it also discusses scanning process when new vulnerabilities are discovered in *Vulnerability Remediation* but keep in mind it does not go into too much detail.
- **A.03.04.04.a:** For new systems, applications, and when systems are being changed for a different role, they are scanned and analyzed for potential security impacts as regulated in *Impact Analyses 03.04.04.*

Shortfalls:

- **A.03.11.01.ODP[01]:** Does not specify the timeframe of when risk assessments are updated.
- **A.03.11.01.a:** Does not provide supply chain risk assessments for third party sources such as private vendors or outside organizations.
- **A.03.11.01.b:** Does not provide information that will ensure the update process is implemented.
- **A.03.11.02.ODP[01]:** This document does not address the frequency at which the system is monitored for vulnerabilities.
- **A.03.11.02.ODP[04]:** Does not state when vulnerability scanning tools will be regularly updated.
- **A.03.11.02.c[02]:** The document does not state that vulnerability tools will be updated when new vulnerabilities are found.
- **A.03.14.01.ODP[01]:** Does not specify the period in which to install security-relevant software updates after the release of the updates is defined.
- **A.03.14.01.ODP[02]:** Does not specify the period within which to install security-relevant firmware updates after the release of the updates is defined.
- **A.03.14.02.ODP[01]:** Although this document discusses the frequency of scans for vulnerabilities it does not expand into malicious code protection mechanisms. Found *Systems to Scan and Scanning Tool Requirements.*
- **A.03.14.02.a[01]:** Does not specify any implementation for malicious code protection mechanisms at system entry and exit points for detection processes.
- **A.03.14.02.a[02]:** Does not specify any implementation for malicious code protection mechanisms at system entry and exit points for eradicating malicious code.
- **A.03.14.02.b:** Does not have any specifications of when the malicious code protection mechanism should be updated.
- **A.03.14.02.c.01[01]:** Does not have any malicious code protection system mentioned

- **A.03.14.02.c.01[02]:** Does not have any protection mechanism for files that are downloaded, opened, or executed.
- **A.03.14.02.c.02:** Does not specify any malicious code protection mechanism that blocks, quarantines, or takes other actions to malicious code.
- **A.03.14.03.a:** Does not discuss any system security alerts, advisories, and directives from outside organizations.
- **A.03.14.03.b[01]:** Does not discuss generating internal security alerts, advisories, and directives.
- **A.03.14.03.b[02]:** Does not discuss disseminating internal security alerts, advisories, and directives.
- **A.03.14.06.a.01[01]:** Does not mention any monitoring system to detect attacks.
- **A.03.14.06.a.01[02]:** Does not mention any monitoring system to detect indicators of potential attacks.
- **A.03.14.06.a.02:** Does not mention any monitoring system to detect unauthorized connections.

6.Recommendations

Media Protection Plan

- Have better sanitation procedures and have regular audits about it.
- Training should be given to staff in secure media handling and transport.
- Enhance Sanitization Procedures.

System and Communications Protection Plan

- Establish performance metrics and validate isolation boundaries for performance under diverse operating conditions using these testing procedures.
- Set thresholds for auto denial of service response activation and run regular simulations of the large scale attacks to be ready.
- Reviewing the split-tunneling exception documentation related to SSL VPNs and to periodic reviews of boundary access policies to ensure that boundary access policies are up to date.
- Regular audits of third party cryptographic operations to formalize and validate key management practices.
- Identify fallback strategies for situations in which key compromise or corruption will compromise continuity of operations and data security.
- Enforcement mechanisms for automatic termination of sessions should be specified to be guaranteed to close sessions after predetermined conditions.

- Use detailed audit trails to verify logout processes and to record session terminations; this will improve compliance verification.
- Defining usage restrictions and control on mobile code execution to only run with authorized and security protocol enforced access and protection of the system from unauthorized execution.

Vulnerability Management Plan

- Set up regular and thorough vulnerability identifications over all assets through consistent network based and application-level scan schedules to avoid delay times.
- Develop and implement effective documentation of remediation tracking for real time, to ensure vulnerabilities can be tracked as identified to complete.
- Establish remediation timeline benchmarks so that time is specified to deal with vulnerability and to prioritize elevated risk vulnerabilities.
- Consistently and accurately tracking assets, meaning all assets should appear on vulnerability assessments and that critical assets are always accounted for.
- Procedures for asset decommissioning must be fully documented and should include that their assets are removed from the network in a secure manner before disposal and vulnerabilities are addressed.
- Setting compensating controls and documenting them to have consistent practices be followed when viable vulnerabilities cannot be remediated immediately.
- Make criteria and an approval process for acceptable risk around vulnerabilities intensely clear, and sensibly related to overall risk management policies on the institution.
- Regular elevated risk asset verification and validation to ensure exposure of any vulnerabilities related to such critical areas are discovered and corrected quickly.

Vulnerability Management Policy

- Establish Formal Risk Acceptance Criteria and Approval Process : Define clear criteria for acceptable risks and implement a standardized approval process. This will ensure that risk acceptance decisions are consistently evaluated and documented across all assets and systems.
- Implement Regular Review and Updates for Risk Mitigation Procedures : Schedule annual or semi-annual reviews of risk mitigation strategies to ensure they reflect current threat

landscapes and industry best practices. Updating these procedures proactively will help maintain effective defenses against emerging vulnerabilities.

- Standardize Compensating Control Documentation and Application : Develop a consistent format and process for documenting compensating controls across all assets. This standardization will ensure uniform application of alternative measures, reinforcing security across the institution's entire asset inventory.
- Enhance Accountability for Asset Owners and Management : Require asset owners to provide periodic updates on vulnerability status, including risk acceptance and remediation efforts. This measure will improve oversight, ensuring that all assets remain adequately protected according to the policy.

Vulnerability Management Standard

- Make an authorized software list.
- Tools to add: Security Information and Event Management (SIEM) systems, Intrusion Detection/Prevention Systems (IDS/IPS), and log analyzers.
- Specify standards for implementing malicious code protection mechanisms.
- Set update schedules for vulnerability tools, recommended before regular scan schedule.
- Make standards for how CUI is handled throughout the school infrastructure.
- Define the period of when software needs to be updated when new security-level firmware and software are released.
- Define the monitoring systems used and the procedures put in place for this system.
- Define when the risk assessment document should be updated.
- Add supply chain risk assessment.
- Go into detail of how malicious code software is handled such as blocked, quarantine, or other actions.
- Add standards for when malicious files are downloaded, opened, or executed.

---

7. Conclusion

The Media Protection Plan, System and Communications Protection Plan, Vulnerability Management Plan, Vulnerability Management Policy, and Vulnerability Management Standard audit exposes the Illinois Institute of Technology to adequately protecting sensitive information, communications and managing vulnerabilities. Although the foundation for these plans is established, the audit revealed several areas that will need enhancement to meet industry best practices and NIST SP 800-171A standards.

Some of the research results pointed out that there are weaknesses in aspects like asset tracking and management of the dynamic update triggers in vulnerability management and the certainty of

compensating control. The plans also show a lack of adequate integration with the rest of the organizational risk management structure to provide a coherent, strategic approach to security across institutions. Specifically, there is a potential for enhancing the existing documentation of the procedures and for refining the treatment of the vulnerabilities, as well as for clarifying the recovery objectives and conditions of the incidents.

These recommendations are aimed at eliminating such gaps, with a tactical stress on enhancing courses of action throughout a strategic scope regarding security policies, standards, and procedures. By improving the alignment of these plans, increasing the IIT's collaboration between departments, and having clearer procedures for detecting and preventing vulnerabilities, the Illinois Institute of Technology can much better prepare itself for defending the data and systems which it holds and for preventing new types of threats from arising.

8. Appendices

Appendix A: Scope Document

This audit will evaluate the Illinois Institute of Technology's Media Protection Plan; System and Communications Protection Plan; Vulnerability Management Plan; Vulnerability Management Policy; and Vulnerability Management Standard based on the criteria referenced in *NIST Special Publication 800-171A Rev. 3.*

The audit is to provide the following:

1. a review of these policies and plans in compliance with the conditions for safeguarding *Controlled Unclassified Information (CUI)* in non-federal systems and institutions.
2. an assessment of the level of compliance with compliance of these policies and plans.

The primary focus areas include:

- Media Protection Plan
- System and Communications Protection Plan
- Vulnerability Management Plan
- Vulnerability Management Policy
- Vulnerability Management Standard

Objectives:

1 . Evaluate the effectiveness, compliance, and implementation of the Media Protection Policy against the requirements outlined in *NIST SP 800-171.*

2. Evaluate enforcement of boundary protection, cryptographic controls, session management and mobile code execution policies in accord with standards.

3. Ensure timely identification and remediation of vulnerabilities across all systems by implementing a consistent, automated vulnerability scanning schedule and establishing clear remediation timelines.

4. The main goal is to focus on risk assessment, system integrity and periodic assessment of the security.

5. Establish timelines for the areas of risk assessments, updates, scanning, malicious code protection mechanisms and threat monitoring.

Methodology:

Document Review: Review the Structure, Content, and alignment of *NIST SP 800-171A* to existing Media Protection Plan, System and Communications Protection Plan, Vulnerability Management Plan, Vulnerability Management Policy, and Vulnerability Management Standard.

Checklist Evaluation: Detailed checklists are used to rate the details of each policy and plan against established criteria in *NIST SP 800-171A Rev. 3*. The documents were consistent with required security controls and this evaluation was done to verify that.

Interviews and Discussions: Over the course of these discussions, we talked with key personnel that do the work of developing and implementing such policies and plans. Insights into the operational effectiveness and any challenges to meeting the *NIST SP 800-171A* standards were obtained from this.

Gap Analysis: Determine and analyze where the documents do not fulfill all NIST SP 800-171A requirements. It allowed us to unveil weaknesses or gaps among the policies and procedures.

Recommendations: Offer actionable recommendations to working with identified gaps, enhance compliance and improve the entire effectiveness for the CUI safeguarding and institutional system's security.

Appendix B: Checklists

Checklist for Media Protection Plan

Access Control to Media:

- To check the identity of people who can be accessed to media storage areas, accept only the authorized person access cards, or use biometrics.

Secure Media Storage:

- Ensure the proper storage, so that sensitive media is kept secure from physical access without access to the unauthorized person.

Media Transport Security:

- Check that all sensitive media, either transported between departments or outside the institute, is protected by means of secure transport methods, like encryption.

Media Destruction and Disposal:

- Check out review procedures for secure destruction or sanitization of sensitive media before disposal, with no sensitive data able to be edited after media is decommissioned.

Training and Awareness:

- Only personnel that have been trained in appropriate policies, procedures and best practices for handling sensitive media should be handling, storing and disposing of said media.

Checklist for System and Communications Protection Plan

Boundary Protection

- Log and alert on all boundary activity, monitor internal and external traffic. Reduce external connection by using managed interfaces. Audit, and update regularly, firewalls.

Information Sharing

- Prevent unauthorized and unintended information transfers. Monitor data transfers over shared resources logs.

Denial of Service Protection

- Automated DoS detection using redundancy. Test traffic management and failover systems.

Cryptographic Key Management

- Use FIPS 140-2 compliant hardware for key storage. Automate key rotation schedules as well as key life cycle procedures.

Session Authenticity

- Session timeouts and MFA are to be enforced. Maintain the logs of the audit session management.

Mobile Code Execution

- Limit and monitor mobile code using ‘sandboxing.’ Whitelist the acceptable applications for mobile code running on the system.

Network Monitoring and Disconnects

- Enforce deny-by-default policies and monitor all network communications. Test networks disconnect mechanism and terminate idle connection.

Transmission and Storage Confidentiality

- Enable measures to encrypt the data at rest (e.g., TLS and IPSec) and in transit using approved methods. Comply with the standards by testing encryption.

Trusted Path

- Ensure the security of the communication paths for authentication and sensitive data. Run tests to the trusted path mechanisms frequently.

Training and Documentation

- Provide training for personnel on policies and maintain records of sessions. Define a policy owner, write a protocol, and review them annually for compliance.

Checklist for Vulnerability Management Plan

Scanning

- Scanning Frequency and Coverage based on Agent Based and Network Based.
- Adaptive scanning frequency according to risk documentation.

Remediation

- Real time remediation track and transparency.
- Remediation timelines benchmarking.

Asset Tracking and Decommissioning

- Update protocols for asset records.
- Documentation on securing asset decommissioning.

Acceptable Risk and Compensating Control

- Developed criteria for what was acceptable risk approval.
- Standardized documentation format for compensating controls.

New Asset Acceptance

- Considerable risk assets enhanced verification process.

Checklist for Vulnerability Management Policy

Training and Awareness

- Implement mandatory training programs for security teams and employees managing critical systems.

Documentation of Vulnerability Management Processes

- Maintain detailed records of scanning, risk assessments, remediation actions, and policy updates.

Governance and Ownership :

- Assign a policy owner (e.g., Security Officer) to oversee its implementation and maintenance.

Defined Roles and Responsibilities:

- Document specific roles such as vulnerability managers, system owners, and response teams.

Checklist for Vulnerability Management Standard

Risk Assessment 03.11.01:

- Make an authorized software list.

Vulnerability Monitoring and Scanning 03.11.02

Flaw Remediation 03.14.01:

- Define the period of when software needs to be updated when new security-level firmware and software are released.

Malicious Code Protection 3.14.02:

- Specify standards for implementing malicious code protection mechanisms.
- Add standards for when malicious files are downloaded, opened, or executed.

Security Alerts, Advisories, and Directives 03.14.03

- Set update schedules for vulnerability tools, recommended before regular scan schedule.

System Monitoring 03.14.06

- Define the monitoring systems used and the procedures put in place for this system.

Appendix C: Additional Documents

Compliance Matrices:

Matrices for mapping policies and plans against *NIST SP 800-171A* with highlighted compliant and non-compliant areas.

Audit Logs:

Interviews, document review, and evidence supporting findings, all of which are records of audit activities.

Gap Analysis Reports:

Reports of compliance gaps in policies and plans and analysis of their potential impact on security posture.

Risk Assessment Findings:

A documentation of hazard assessments with vulnerability and risks found during the audit.

Remediation Tracking Documentation:

Tracked efforts against remediation efforts including timelines, actions taken to fill any gaps, weaknesses.

Appendix D: References

1. *NIST Special Publication 800-171A Rev. 3* – Full text and sections relevant to the audit that define criteria and conditions for safeguarding *Controlled Unclassified Information (CUI).*
2. Collection of the Institution's current policies and plans as reviewed during the audit.
3. Illinois Institute of Technology. *System and Communications Protection Plan, Vulnerability Management Plan, Vulnerability Management Policy, Vulnerability Management Standard and the Media Protection Plan.* Once audited by these documents, these documents were used to assess the approach the institution took to protecting sensitive media, producing secure systems, identifying, and mitigating vulnerabilities and creating security management objectives and guidelines.