Cyan Group
Final Project

Avery Huerta, Bhargavi Punnam, Mahesh Nutheti, Pierre Lopez, Radha Prabhakaran

ITMS–478-578

Executive Summary

Purpose: The cyan group audits were conducted to evaluate and ensure that all documentation for policies, standards, and plans complied with NIST Special Publication 800-171A for the organization of Illinois Institute of Technology.

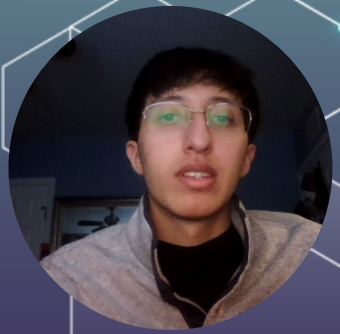
Audited Documents:

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

Vulnerability Management Standards (VMS)

01	02
Risk Assessment	System and Information Integrity

VMS Risk Assessment and Monitoring



Risk Assessment

- No defined timeframe for updating risk assessments.
- Missing supply chain risk evaluations for third-party vendors.
- Inadequate implementation of risk update processes.

Vulnerability Monitoring

- No schedule for scanning tool updates.
- Missing frequency details for system monitoring.

VMS System Integrity Gaps

Critical Issues:

1. **Malicious Code Protection**
   - No mechanisms for detection, eradication, or quarantine.
   - Lacks update processes for protection tools.
2. **System Monitoring**
   - No tools or procedures for detecting attacks or unauthorized access.
3. **Flaw Remediation**
   - Undefined timelines for applying software and firmware updates.

VMS Recommendations

- Set schedules for updating risk assessments and vulnerability tools
- Introduce malicious code protection mechanisms
- Define CUI handling procedures and policies
- Strengthen system monitoring for attack detection and prevention

Media Protection Policy

I. Scope of the audit

I. Key findings & Recommendations

I. Scope of the audit

- Media Access Control-03.08.02
- Media marking - 03.08.04
- Media Storage - 03.08.01
- Media transport-03.08.05
- Media Sanitization- 03.08.03
- Media use -03.08.07

2. Key findings

Key Strengths

- The policy is well-documented, with clear processes for storage and transport.
- Compliance with encryption for transported media reduces exposure to unauthorized access
- An annual review process

Compliances Issues

Sanitization is mentioned but not consistently implemented or logged.
No explicit procedures for media-related incidents.
Training is not regularly updated or mandatory for all personnel.

Recommendations

Improve sanitization procedures.

- Adopt automated or certified sanitization tools and processes.
- Maintain a detailed sanitization log for audit purposes.

Conduct mandatory annual training for all personnel

- Update training materials to include recent incidents and best practices.

System and Communications Protection Plan Audit

Enhance security and ensure CUI compliance.

Scope of the Audit

01

Boundary Protection

03.13.01

02

Shared System Resources

03.13.04

03

Mobile Code

03.13.13

04

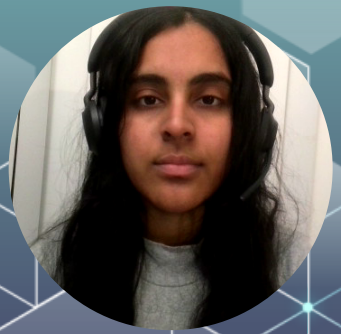
Session Authenticity

03.13.15

Purpose:

The goal is to identify strengths, address gaps, and recommend improvements to enhance security and ensure compliance with federal standards for protecting CUI.

Boundary Protection & Shared Resources



Securing Network Boundaries and Shared Systems

Boundary Protection:

- **Strengths**: Proxy servers, deny-by-default access control, subnetwork isolation.
- **Weaknesses**: Limited **internal interface monitoring** and lack of boundary protection device details.

Shared System Resources:

- **Strengths**: Isolates security functions from non-security functions.
- **Weaknesses**: Missing mechanisms for preventing **unintended data transfers**.

Data and Session Security

Access Controls, Data Integrity, and Session Management

Deny by Default:
- Fully implemented; no weaknesses identified.

Cryptographic Protection:
- **Strengths**: TLS and IPSec for secure data transmission.
- **Weaknesses**: No encryption policies for data at rest.

Network Disconnect:
- **Strengths**: Sessions terminate after inactivity.
- **Weaknesses**: Inactivity timeout period not defined.

Session Authenticity & Missing Areas

Managing Session Security and Emerging Gaps

Session Authenticity:

- **Strengths**: Unique session identifiers ensure secure communication.
- **Weaknesses**: No procedure to invalidate session IDs after termination.

Missing Areas:

- **Collaborative Computing Devices (03.13.12)**: Not addressed.
- **Mobile Code (03.13.13)**: Not included, despite relevance to modern university systems.

Addressing Emerging Threats

Mobile Code and Collaborative Devices in University Systems

Mobile Code:

- Risks from **web-based applications** and BYOD policies.
- Missing policies for acceptable use, monitoring, and control.

Collaborative Computing Devices:

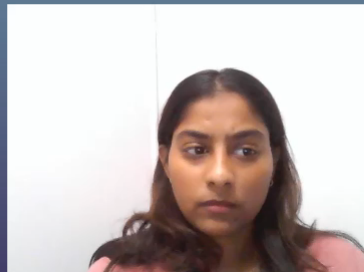
- No policy for managing remote activation or user indication during use.

Conclusion

Strengths:
•Strong foundation in **boundary protection**, **cryptographic security**, and **DoS mitigation**.

Weaknesses:
•Gaps in **internal monitoring**, **mobile code**, and **collaborative devices**.

Moving Forward:
Enhance policies to address these gaps and ensure comprehensive compliance with **NIST SP 800-171A**.



Vulnerability Management Plan

Objective:

Evaluate VMP implementation to minimize cybersecurity threats.

Focus Areas:

- Risk Assessment
- System and Information Integrity
- Configuration Management
- Security Assessment

Risk Assessment

Strengths:

- Clear scanning and remediation processes
- Assigned responsibilities for risk detection

Weaknesses:

- Specified frequency for risk assessments
- Procedures to evaluate mitigation strategy effectiveness

Recommendations:

- Schedule periodic updates
- Evaluate mitigation strategy effectiveness

System and information integrity

Strengths:

- Regular scans
- Detailed remediation processes

Weaknesses:

- Timelines for critical updates and patches
- Real-time monitoring for continuous evaluation

Recommendations:

- Establish timelines for updates
- Implement real-time monitoring

Configuration Management

Strengths:

- Scanning timelines for unused functions

Weaknesses:

- Standardized configuration management processes
- Documentation for restricting ports, protocols, and services
- Detailed process for managing changes to systems

Recommendations:

- Standardize configuration management
- Document security settings
- Manage system changes

Security Assessment

Strengths:

- Regular vulnerability scanning

Weaknesses:

- Specific procedures for periodic security assessments
- Ongoing monitoring mechanisms

Recommendations:

- Standardize security evaluations
- Monitor security controls

Conclusion

- The audit of the current VMP unveiled the key enablers and risks associated with that method with extra attention to the importance of compliance with the requirements set through NIST SP 800-171A.

- Implementation of these improvements will create enhanced risk management environments that will reduce cyber threats and general compliance with federal cybersecurity standards.

THANK YOU