Audit Report

- **Title:** Audit Report for Illinois Institute of Technology
- **Institution:** Illinois Institute of Technology
- **Date:** July 15, 2024
- **Prepared by:** Vijayamurugan Saravanan

  Darren Tan

  Kimberly Dominguez

  Nidhi Jitendra Patni

  Navya Singari

Table of Contents

1. Executive Summary

Purpose: This comprehensive audit was conducted to evaluate and ensure the compliance and effectiveness of various policies, plans, and standards at the Illinois Institute of Technology, specifically focusing on their alignment with NIST Special Publication 800-171A Rev. 3.

Scope: The audit covered the following areas:

- Incident Response Plan
- Incident Response Standard
- Incident Response Policy
- Mobile Device Policy
- System and Data Integrity Plan

Key Findings:

- **Incident Response Plan:** Needs more frequent updates and comprehensive testing.
- **Incident Response Standard:** Requires better-defined corrective action timeframes and regular testing.
- **Incident Response Policy:** Lacks clear definitions for reportable incidents and response capabilities.
- **Mobile Device Policy:** Needs improved configuration standards and better update mechanisms.
- **System and Data Integrity Plan:** Lacks benchmarks for flaw remediation and integrated situational awareness.

Recommendations:

- Establish triggers for updates and enhance testing protocols.
- Define clear corrective action timeframes and improve false positive management.
- Specify reportable incidents and improve response capabilities.
- Enhance authentication methods and monitoring procedures.
- Integrate situational awareness and optimize network traffic analysis.

2. Introduction

Purpose: This report consolidates the findings from audits conducted on key policies, plans, and standards at the Illinois Institute of Technology. The objective is to ensure compliance with NIST Special Publication 800-171A Rev. 3 and enhance the overall cybersecurity posture of the institution.

Scope: The audit focused on:

- Incident Response Plan
- Incident Response Standard
- Incident Response Policy
- Mobile Device Policy
- System and Data Integrity Plan

Objectives:

- Assess compliance with relevant regulations.
- Evaluate the effectiveness of policy implementation.
- Identify areas for improvement.

3. Scope and Objectives

Scope: The audit examined the content, implementation, and enforcement of the specified policies, plans, and standards within the Illinois Institute of Technology.

Objectives:

- Determine if the policies, plans, and standards are compliant with applicable laws and regulations.
- Assess how effectively they are being implemented and enforced.
- Identify gaps and provide recommendations for improvement.

4. Summary of Findings

Incident Response Plan:

- Plan lacks measures for intermediate updates and detailed testing scenarios.
- Communication protocols with law enforcement are not defined.
- Recovery strategies do not specify recovery time and point objectives.
- Integration with overall risk management is insufficient.

Incident Response Standard:

- Lacks benchmarks for corrective actions and regular testing procedures.
- Does not address false positives and lacks integrated situational awareness.
- Monitoring activities are not adaptable to risk changes.

Incident Response Policy:

- Incident response capability and reportable incidents are not clearly defined.
- Lacks procedures for handling system and organizational changes.
- Inconsistent enforcement of incident reporting protocols.

Mobile Device Policy:

- Lacks detailed configuration standards and update mechanisms.
- Insufficient sanitization procedures and monitoring capabilities.
- Inconsistent implementation of software updates.

System and Data Integrity Plan:

- Does not provide benchmarks for flaw remediation.
- Lacks procedures for testing software updates and managing false positives.
- Insufficient integration of monitoring data for situational awareness.
- Monitoring activities are not adjusted based on risk levels.

5. Detailed Findings

Incident Response Plan

Observations:

- Annual reviews and updates are included, but intermediate updates are not.
- Incident response testing is limited to annual testing without detailed scenarios.
- Communication with law enforcement is not addressed.
- Recovery time objectives (RTOs) and recovery point objectives (RPOs) are not specified.
- Integration with risk management is not clear.

Shortfalls:

- Lack of dynamic update triggers.
- Limited incident response testing scenarios.
- Inadequate external communication protocols.
- Undefined recovery objectives.
- Poor integration with risk management.

Incident Response Standard

Observations:

- Roles and responsibilities are well-defined.
- Comprehensive internal notification requirements are included.
- Incident handling procedures are detailed.
- Documentation and reporting processes are established.

Shortfalls:

- No benchmarks for corrective actions.
- Lack of regular testing of response procedures.
- No strategies for managing false positives.
- Inadequate integration of situational awareness.
- Monitoring activities are not adaptable to risk levels.
- Legal considerations for monitoring activities are not addressed.

Incident Response Policy

Observations:

- Clear purpose, scope, and definitions are provided.
- Procedures for reporting and responding to incidents are included.

Shortfalls:

- Incident response capability is not clearly defined.
- Definition of reportable incidents is too broad.
- No procedures for handling failures in the response chain.

Mobile Device Policy

Observations:

- Access control measures are well-defined.
- Network protection measures are in place.

Shortfalls:

- No detailed configuration standards.
- Limited specifications for OTS-managed equipment.
- Insufficient sanitization procedures.
- Inconsistent updates and lack of new technology considerations.

System and Data Integrity Plan

Observations:

- Flaw remediation and malicious code protection mechanisms are included.
- System monitoring and spam protection measures are in place.
- Information management and retention guidelines are provided.

Shortfalls:

- No benchmarks for flaw remediation.
- No testing procedures for software and firmware updates.
- False positives in malicious code detection are not addressed.
- Malicious code protection mechanisms are not regularly tested.
- Integrated situational awareness is lacking.
- Network traffic analysis is not optimized.
- Monitoring activities are not adjusted based on risk levels.
- System monitoring information is not regularly transferred to personnel.
- Legal considerations for monitoring activities are not addressed.
- Internal monitoring capabilities are not strategically invoked.

---

6. Recommendations

Incident Response Plan:

- Establish triggers for updates based on changes in technology or major incidents.
- Expand testing protocols to include diverse and realistic scenarios, particularly social engineering attacks.
- Develop procedures for coordinating with external organizations during security incidents.
- Define RTOs and RPOs for critical services and data systems.
- Strengthen the integration of incident response data into the risk management strategy.

Incident Response Standard:

- Set specific benchmarks for corrective actions.
- Conduct regular testing and evaluation of incident response procedures.
- Develop strategies to manage false positives during incident detection.
- Integrate physical, cyber, and supply chain information for enhanced situational awareness.
- Adjust monitoring activities based on risk levels and high-risk individuals.
- Obtain legal opinions for monitoring activities to ensure compliance.

Incident Response Policy:

- Define the capability and scope of incidents that can be reported.
- Clearly specify what constitutes a reportable incident.
- Establish procedures for handling failures in the incident response chain.

Mobile Device Policy:

- Enhance authentication methods, including multi-factor authentication.
- Create detailed configuration standards for secure device setup.
- Establish procedures for regular policy reviews and updates.
- Strengthen monitoring capabilities and procedures for handling lost or compromised credentials.

System and Data Integrity Plan:

- Set benchmarks for flaw remediation and corrective actions.
- Test software and firmware updates for efficacy and adverse effects before installation.
- Address false positives in malicious code detection to ensure system availability.
- Regularly test and verify malicious code protection mechanisms.
- Integrate monitoring data for comprehensive situational awareness.
- Optimize network traffic analysis and adjust monitoring activities based on risk levels.
- Transfer system monitoring information to personnel at appropriate intervals.
- Obtain legal opinions on system monitoring activities.
- Deploy internal monitoring devices strategically to track specific transactions.

---

7. Conclusion

The comprehensive audit of the Illinois Institute of Technology's policies, plans, and standards has identified several areas for improvement to ensure compliance with NIST Special Publication 800-171A Rev. 3. Addressing the identified gaps and implementing the recommended actions will significantly enhance the institution's cybersecurity posture and ensure the protection of its information systems and data.

8. Appendices

Appendix A: Scope Document

The scope of this audit encompasses the evaluation of the Illinois Institute of Technology's Incident Response Plan, Incident Response Standard, Incident Response Policy, Mobile Device Policy, and System and Data Integrity Plan against the criteria outlined in NIST Special Publication 800-171A Rev. 3. The audit aims to assess the compliance of these policies and plans with the requirements for safeguarding Controlled Unclassified Information (CUI) in non-federal systems and institutions. The primary focus areas include:

- Incident Response Plan
- Incident Response Standard
- Incident Response Policy
- Mobile Device Policy
- System and Data Integrity Plan

The audit examines the effectiveness of these documents in meeting the security controls specified by NIST SP 800-171A, identifies any gaps or deficiencies, and provides recommendations for improvement.

Objectives:

- To ensure that the Incident Response Plan, Standard, and Policy are robust and capable of managing security incidents effectively.
- To evaluate the Mobile Device Policy in safeguarding data and technology resources.
- To assess the System and Data Integrity Plan in maintaining the integrity of systems and data.
- To identify gaps and provide actionable recommendations for compliance and enhancement.

Methodology:

Document Review: Examination of the current policies and plans to understand their structure, content, and alignment with NIST SP 800-171A.

Checklist Evaluation: Use of detailed checklists to assess each document against specific NIST SP 800-171A requirements.

Interviews and Discussions: Conducting discussions with key personnel involved in the development and implementation of these policies and plans.

Gap Analysis: Identifying areas where the documents fall short of NIST requirements.

Recommendations: Providing practical recommendations to address identified gaps and enhance compliance.

Appendix B: Checklists

1. Checklist for Incident Response Plan:

Plan Updates:

- Includes measures for intermediate updates in case of significant changes.
- Annual reviews and updates during plan implementation, execution, or testing.

Incident Response Testing:

- Frequency of testing.
- Details of test cases and scenarios, including social engineering attacks.

Incident Response Communication:

- Coordination with law enforcement or regulatory agencies.

Detailed Recovery Plans:

- Recovery Time Objectives (RTOs).
- Recovery Point Objectives (RPOs).

Integration with Risk Management:

- Impact of incident response data on overall risk management strategy.

2. Checklist for Incident Response Standard:

Roles and Responsibilities:

- Identification of Incident Manager, Privacy Officer, Security Engineer, SIRT, and ESIRT.

Notification and Communication:

- Internal notification requirements and breach notification templates.

Incident Handling Procedures:

- Steps involved in preparation, detection, analysis, containment, recovery, and follow-up.

Documentation and Reporting:

- Processes for tracking, documenting, and reporting incidents.

Corrective Action Time Frames:

- Benchmarks or time frames for addressing incidents.

Checklist for Incident Response Policy:

Purpose:

- Clear definition of policies and responsibilities.

Scope:

- Coverage of all electronic data and systems within Illinois Tech.

Definitions:

- Definitions of key terms and roles.

Procedures:

- Steps for reporting, responding to, and documenting security events.

Incident Response Capability:

- Structure and capability of the incident response team.

Checklist for Mobile Device Policy:

Portable Computing Devices:

- Restrictions on remote system or application administration access.

Access Control:

- Requirement for passcodes and permissions for remote access.

Network Protection:

- Use of firewalls, screen timeouts, frequent updates, and anti-virus/malware software.

Configuration Standards:

- Requirements for secure baseline setup.

Sanitization Procedures:

- Procedures for sanitizing devices.

Checklist for System and Data Integrity Plan:

Flaw Remediation:

- Implementation of security software updates.

Malicious Code Protection:

- Detection, blocking, quarantine, and eradication of malicious code.

System Monitoring:

- Monitoring critical systems and networks.

Security Alerts, Advisories, and Directives:

- Enabling services for security alerts and advisories.

Spam Protection:

- Enabling spam protection with automatic updates.

Appendix C: Additional Documents

1. Compliance Matrices:

- Detailed matrices mapping each policy and plan against NIST SP 800-171A requirements.
- Identification of compliant and non-compliant areas.

2. Audit Logs:

- Records of all activities conducted during the audit.
- Documentation of evidence collected to support findings and recommendations.

3. Gap Analysis Reports:

- Detailed reports highlighting specific gaps in each policy and plan.
- Analysis of the potential impact of these gaps on overall security posture.

Appendix D: References

1. NIST Special Publication 800-171A Rev. 3 - Full text and relevant sections used for the audit. Guidelines and requirements for safeguarding Controlled Unclassified Information (CUI).
2. Illinois Institute of Technology Policies and Plans
3. Copies of the Incident Response Plan, Incident Response Standard, Incident Response Policy, Mobile Device Policy, and System and Data Integrity Plan.