NIST SP 800-171 Security Control Audit Report

Assessment of Controlled Unclassified Information (CUI) Security Controls

Assessment Date: July 28th, 2025

1. Executive Summary

Overall Compliance Score: 82/110

Target Compliance Score: 110/110

74.5% Compliance Rate with 28 Points in Penalties

This audit report presents the findings of a comprehensive assessment of the organization's implementation of NIST SP 800-171 security controls for protecting Controlled Unclassified Information (CUI).

The assessment evaluated 110 security controls across 14 control families, resulting in an overall compliance score of 82 out of 110 possible points.

The organization demonstrates a good foundation in cybersecurity with a 74.5% compliance rate.

Key strengths include **robust access controls**, **comprehensive audit logging**, **strong configuration management**, and **effective incident response capabilities**. However, critical gaps exist in areas such as **authentication mechanisms**, **system maintenance procedures**, and **communications protection** that require immediate attention.

CONTROLS IMPLEMENTED	CONTROLS NOT IMPLEMENTED	CONTROL FAMILIES ASSESSED
96	14	14

TOTAL PENALTY POINTS

28

2. Objective and Scope

Audit Objective

The primary objective of this audit was to assess the organization's implementation and effectiveness of NIST SP 800-171 security controls for protecting Controlled Unclassified Information (CUI).

This assessment aimed to:

- Evaluate compliance with federal requirements for CUI protection
- Identify security control gaps and vulnerabilities
- Assess the maturity of the organization's cybersecurity program
- Provide actionable recommendations for improving security posture
- Support preparation for official CMMC (Cybersecurity Maturity Model Certification) assessments

Scope of Assessment

The assessment encompassed all 14 NIST SP 800-171 control families and their associated 110 security requirements:

- **Access Control (AC)** - 22 controls
- **Awareness and Training (AT)** - 3 controls
- **Audit and Accountability (AU)** - 9 controls
- **Configuration Management (CM)** - 9 controls
- **Identification and Authentication (IA)** - 11 controls
- **Incident Response (IR)** - 3 controls
- **Maintenance (MA)** - 6 controls
- **Media Protection (MP)** - 9 controls
- **Personnel Security (PS)** - 2 controls
- **Physical Protection (PE)** - 6 controls
- **Risk Assessment (RA)** - 3 controls
- **Security Assessment (CA)** - 4 controls
- **System and Communications Protection (SC)** - 16 controls
- **System and Information Integrity (SI)** - 7 controls

3. Methodology

The assessment methodology followed the NIST SP 800-171A guidelines for assessing security controls. The evaluation process included:

Assessment Approach

- **Document Review:** Analysis of security policies, procedures, and technical documentation
- **Technical Testing:** Hands-on evaluation of security control implementation
- **Personnel Interviews:** Discussions with key stakeholders and system administrators
- **System Observation:** Direct observation of security controls in operation

Scoring Methodology

Each security control was assigned a point value based on its relative importance and impact on CUI protection:

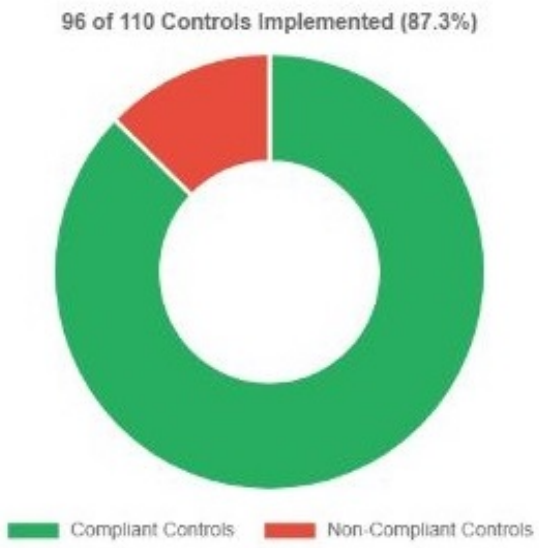
- **5 Points:** High-impact controls critical for CUI protection
- **3 Points:** Medium-impact controls important for overall security
- **1 Point:** Lower-impact controls supporting defense-in-depth

Controls were evaluated as either "Implemented" (full points awarded) or "Not Implemented" (penalty points assigned equal to control value).

The final score represents the total possible points (110) minus penalty points (28), resulting in a score of 82.

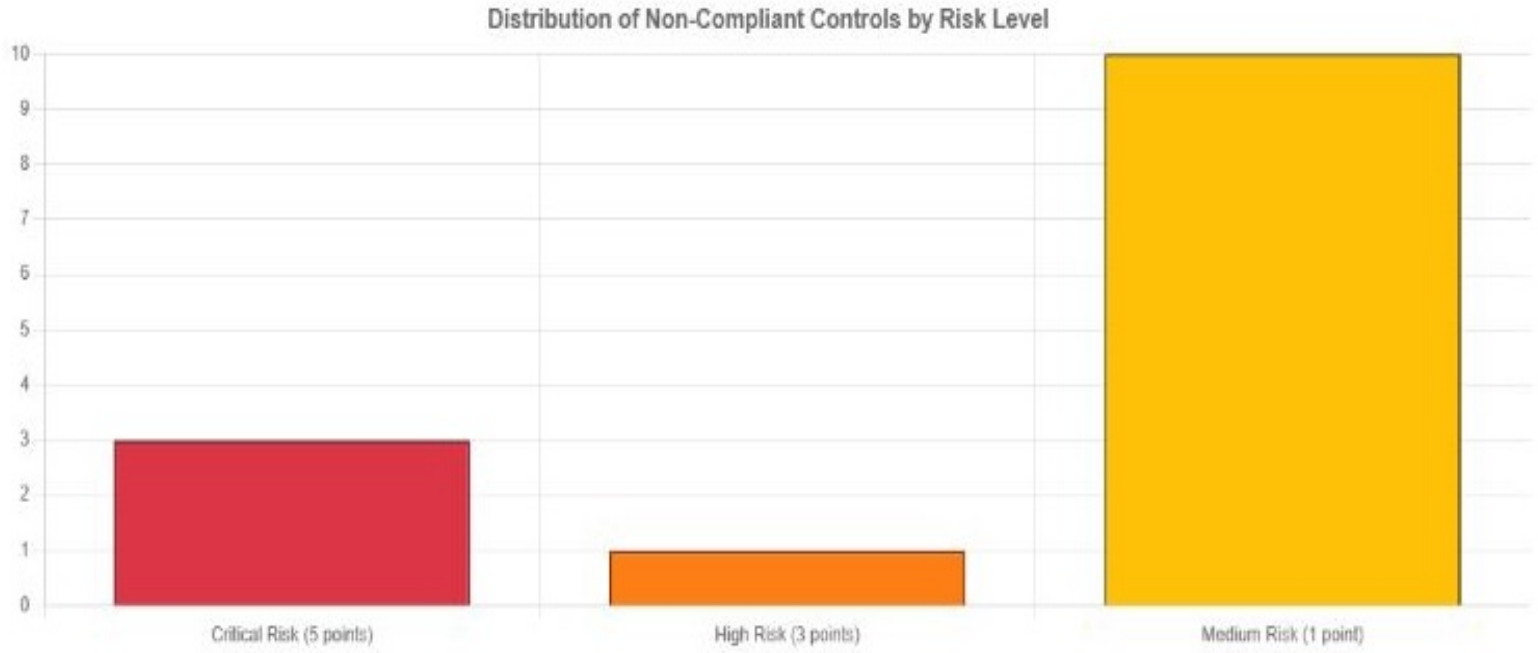
4. Compliance Analysis Charts

Overall Compliance Status



Control Family Compliance Breakdown

Risk Distribution by Control Value



5. Audit Results

Key Findings Summary

The assessment identified 14 security controls that are not currently implemented, resulting in 28 penalty points.

The following pages summarize the non-compliant controls.

Control ID	Control Family	Description	Risk Level	Points
3.5.10	Identification and Authentication	Store and transmit only cryptographically-protected passwords	**Critical**	5
3.13.15	System and Communications Protection	Protect the authenticity of communications sessions	**Critical**	5
3.14.6	System and Information Integrity	Monitor organizational systems for attacks and indicators	**Critical**	5
3.7.4	Maintenance	Check media for malicious code before use	**High**	3
3.1.14	Access Control	Route remote access via managed access control points	**Medium**	1
3.1.15	Access Control	Authorize remote execution of privileged commands	**Medium**	1
3.5.4	Identification and Authentication	Employ replay-resistant authentication mechanisms	**Medium**	1
3.5.6	Identification and Authentication	Disable identifiers after defined period of inactivity	**Medium**	1

Control ID	Control Family	Description	Risk Level	Points
3.5.9	Identification and Authentication	Allow temporary password use with immediate change	**Medium**	1
3.5.11	Identification and Authentication	Obscure feedback of authentication information	**Medium**	1
3.7.3	Maintenance	Ensure equipment removed for off-site maintenance is sanitized	**Medium**	1
3.13.9	System and Communications Protection	Terminate network connections after defined inactivity	**Medium**	1
3.13.13	System and Communications Protection	Control and monitor the use of mobile code	**Medium**	1
3.13.14	System and Communications Protection	Control and monitor the use of VoIP technologies	**Medium**	1

Organizational Strengths

Access Control Excellence

Strong implementation of access controls with multi-factor authentication, proper privilege management, and comprehensive remote access security. Account lockout after failed attempts and session management are properly configured.

Robust Audit Capabilities

Comprehensive logging infrastructure captures user activities, file access, and system changes. Monthly log reviews ensure suspicious activities are detected and investigated promptly.

Mature Configuration Management

Well-established baseline configurations, change control processes, and software inventory management. Standard configurations are enforced across all systems with proper approval workflows.

Effective Incident Response

Clear incident response procedures with defined roles, regular testing through mock incidents, and established communication channels for both internal and external reporting.

6. Recommendations

Critical Priority Actions (Immediate Implementation Required)

1. Apply Cryptographic Password Protection (3.5.10) Identification and Authentication

Current Gap: Passwords may not be stored and transmitted with proper cryptographic protection.

Recommendation: Apply password hashing using approved algorithms (SHA-256 or stronger) for storage and ensure encrypted transmission protocols (TLS 1.2+) for password communication.

Timeline: 30 days

2. Deploy Network Security Monitoring (3.14.6) System and Information Integrity

Current Gap: Lack of comprehensive monitoring for attack detection and threat indicators.

Recommendation: Implement a Security Information and Event Management (SIEM) solution or network monitoring tools to detect and analyze potential security threats in real-time.

Timeline: 60 days

3. Establish Communications Session Authentication (3.13.15) System and Communications Protection

Current Gap: Communications sessions lack proper authenticity protection.

Recommendation: Implement digital certificates, message authentication codes (MAC), or digital signatures to protect the authenticity of communications sessions.

Timeline: 45 days

High Priority Actions (Implementation within 90 days)

4. Malware Scanning for Maintenance Media (3.7.4) Maintenance

Recommendation: Establish procedures to scan all diagnostic and test media for malicious code before use in organizational systems. Deploy isolated scanning stations for this purpose.

5. Implement Managed Remote Access Points (3.1.14) Access Control

Recommendation: Configure all remote access to route through managed access control points such as VPN concentrators or jump servers with centralized monitoring and control.

Medium Priority Actions (Implementation within 6 months)

6. Enhanced Authentication Mechanisms Identification and Authentication

Implement replay-resistant authentication (3.5.4), automatic account disabling (3.5.6), temporary password management (3.5.9), and authentication feedback obscuring (3.5.11).

7. Network Security Enhancements System and Communications Protection

Implement automatic session termination (3.13.9), mobile code controls (3.13.13), and VoIP security monitoring (3.13.14).

8. Maintenance Security Procedures Maintenance and Access Control

Establish procedures for sanitizing equipment before off-site maintenance (3.7.3) and implement controls for remote privileged command execution (3.1.15).

Long-term Security Posture Improvements

- **Security Awareness Enhancement:** Expand cybersecurity training to include specific CUI handling procedures and emerging threat awareness
- **Continuous Monitoring:** Implement automated compliance monitoring to track control effectiveness over time
- **Regular Assessments:** Establish quarterly internal assessments to maintain and improve compliance posture
- **Vendor Management:** Enhance third-party risk management for vendors handling CUI
- **Business Continuity:** Strengthen backup and recovery procedures specifically for CUI systems

Estimated Implementation Costs

Based on the identified gaps, the estimated investment for achieving full compliance ranges from $75,000 to $125,000, including:

- **Network monitoring and SIEM solution:** $30,000 - $50,000
- **Enhanced authentication systems:** $15,000 - $25,000
- **Cryptographic implementation:** $10,000 - $15,000
- **Additional security tools and software:** $10,000 - $20,000
- **Professional services and training:** $10,000 - $15,000

7. Conclusion

The organization demonstrates a strong commitment to cybersecurity with a solid foundation of implemented controls achieving a 74.5% compliance rate.

The existing security program shows maturity in key areas such as **access control**, **audit capabilities**, and **incident response**.

However, to achieve full NIST SP 800-171 compliance and strengthen protection of CUI, immediate attention must be given to the 14 identified control gaps, particularly the three critical-risk items.

The recommended implementation plan provides a phased approach to address these gaps while maintaining operational efficiency.

With proper implementation of the recommended improvements, the organization can achieve full compliance within 6-9 months and significantly enhance its overall security posture for protecting Controlled Unclassified Information.

Jeremy Fluker, Compliance Analyst
Email: jfluker.pro@gmail.com