NIST-800-171 v3 Compliance

Compliance Summary Report

Total Score: -185

Total Number of Controls: 101

Total Compliant Checks: 40

Total Non-Compliant Checks: 19

Total Not Applicable Checks: 31

Total To Be Implemented Checks: 9

Control: 03.01.01 - Account Management

Check: CheckUsersPolicies

Description: Define and manage allowed and prohibited system account types, including creation, modification, and removal according to policies.

Result: COMPLIANT

Impact: 5

Control: 03.01.02 - Access Enforcement

Check: CheckAcceptedPolicies

Description: Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.

Result: COMPLIANT

Impact: 5

Control: 03.01.03 - Information Flow Enforcement

Check: CheckCUIFlow

Description: Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.

Result: NOT COMPLIANT

Impact: 5

Control: 03.01.04 - Separation of Duties

Check: CheckSeparateDuties

Description: Identify the duties of individuals requiring separation. Define system access authorizations to support separation of duties.

Result: COMPLIANT

Impact: 5

Control: 03.01.05 - Least Privilege

Check: CheckLeastPrivilege

Description: Instance uses least privilege for IAM roles

Result: COMPLIANT

Impact: 5

Control: 03.01.06 - Least Privilege Privileged Accounts

Check: CheckPrivilegedAccounts

Description: Instance uses least privilege for privileged accounts

Result: COMPLIANT

Impact: 5

Control: 03.01.07 - Least Privilege Privileged Functions

Check: CheckPreventPrivilegedFunctions

Description: Prevent non-privileged users from executing privileged functions.

Result: COMPLIANT

Impact: 5

Control: 03.01.08 - Limit Unsuccessful Logon Attempts

Check: CheckLogonAttempts

Description: Instance limits unsuccessful logon attempts

Result: COMPLIANT

Impact: 5

Control: 03.01.09 - System Use Notification

Check: //

Description: Display a system use notification message with privacy and security notices consistent with applicable CUI rules before granting access to the system.

Result: NOT APPLICABLE

Impact: 5

Control: 03.01.10 - Device Lock

Check: CheckSessionLock

Description: Prevent system access by locking the device after a defined period of inactivity or requiring the user to lock it before leaving. Keep the device locked until the user reestablishes access with proper authentication.

Result: COMPLIANT

Impact: 5

Control: 03.01.11 - Session Termination

Check: CheckSessionTermination

Description: Instance automatically terminates user sessions after a defined condition

Result: NOT COMPLIANT

Impact: 5

Control: 03.01.12 - Remote Access Control

Check: CheckRemoteAccessControl

Description: Instance monitors and controls remote access sessions

Result: NOT COMPLIANT

Impact: 5

Control: 03.01.16 - Wirless Access

Check: //

Description: Establish usage, configuration, and connection requirements for wireless access to the system. Authorize wireless access before establishing connections. Disable wireless capabilities when not in use and protect access with authentication and encryption.

Result: NOT APPLICABLE

Impact: 5

Control: 03.01.18 - Access Control for Mobile Devices

Check: //

Description: Establish usage, configuration, and connection requirements for mobile devices. Authorize mobile device connections and implement encryption to protect the confidentiality of CUI.

Result: NOT APPLICABLE

Impact: 5

Control: 03.01.20 - Use of External Systems

Check: CheckExternalSystemConnections

Description: Instance controls connections to external systems

Result: COMPLIANT

Impact: 5

Control: 03.01.22 - Publicly Accessible Content

Check: //

Description: Train authorized individuals to ensure publicly accessible information does not contain CUI. Regularly review public content for CUI and remove it if found.

Result: NOT APPLICABLE

Impact: 5

Control: 03.02.01 - Publicly Accessible Content

Check: //

Description: Provide security literacy training to system users during initial onboarding and at defined intervals. Offer additional training after system changes or specific events, focusing on recognizing and reporting insider threats, social engineering, and social mining.

Result: NOT APPLICABLE

Impact: 5

Control: 03.02.02 - Publicly Accessible Content

Check: //

Description: Provide role-based security training to personnel before authorizing access to the system or CUI, before performing duties, and at organization-defined intervals. Update training content regularly and after system changes or specific events.

Result: NOT APPLICABLE

Impact: 5

Control: 03.03.01 - Event Logging

Check: CheckAuditLogs

Description: Instance creates and retains system audit logs

Result: NOT COMPLIANT

Impact: 5

Control: 03.03.02 - Audit Record Content

Check: CheckUserTraceability

Description: Instance traces actions of individual system users

Result: NOT COMPLIANT

Impact: 5

Control: 03.03.03 - Audit Record Generation

Check: CheckLoggedEventsRetention

Description: Retain audit records for a time period consistent with the records retention policy.

Result: COMPLIANT

Impact: 5

Control: 03.03.04 - Audit Logging Failure

Check: CheckAuditLoggingFailure

Description: Instance alerts in the event of audit logging process failure

Result: NO ASSET

Impact: 5

Control: 03.03.05 - Audit Record Review, Analysis, and Reporting

Check: CheckAuditLogAnalysis

Description: Instance correlates audit records for investigation

Result: COMPLIANT

Impact: 5

Control: 03.03.06 - Audit Record Reduction and Report Generation

Check: CheckAuditRecordReduction

Description: Instance provides audit reduction and report generation

Result: COMPLIANT

Impact: 5

Control: 03.03.07 - Time Synchronization

Check: TBI

Description: Instance synchronizes system clocks with an authoritative source

Result: TO BE IMPLEMENTED

Impact: 5

Control: 03.03.08 - Protection of Audit Information

Check: CheckAuditSecurity

Description: Ensure audit information is protected from unauthorized access

Result: NOT COMPLIANT

Impact: 5

Control: 03.04.01 - Baseline Configuration

Check: CheckBaselineConfigurations

Description: Develop and maintain under configuration control, a current baseline configuration of the system.

Result: NOT COMPLIANT

Impact: 5

Control: 03.04.02 - Configuration Settings

Check: TBI

Description: Establish, document, and implement the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements: [Assignment: organization-defined configuration settings].

Result: TO BE IMPLEMENTED

Impact: 5

Control: 03.04.03 - Configuration Change Control

Check: TBI

Description: Define the types of changes to the system that are configuration-controlled. Review and approve or disapprove proposed changes with explicit consideration for security impacts. Implement and document approved changes, and monitor activities related to configuration-controlled changes to the system.

Result: TO BE IMPLEMENTED

Impact: 5

Control: 03.04.04 - Impact Analyses

Check: TBI

Description: Analyze changes to the system to determine potential security impacts before implementation. Verify that security requirements continue to be met after changes are implemented.

Result: TO BE IMPLEMENTED

Impact: 5

Control: 03.04.05 - Access Restrictions for Change

Check: TBI

Description: Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system..

Result: TO BE IMPLEMENTED

Impact: 5

Control: 03.04.06 - Least Functionality

Check: CheckEssentialCapabilities

Description: Configure the system to provide only mission-essential capabilities.

Result: NOT COMPLIANT

Impact: 5

Control: 03.04.08 - Authorized Software â€” Allow by Exception

Check: CheckAuthorizedSoftware

Description: Identify software programs authorized to execute on the system.

Result: NOT COMPLIANT

Impact: 5

Control: 03.04.10 - System Component Inventory

Check: CheckInformationLocation

Description: Develop and document an inventory of system components. Review and update the inventory at organization-defined intervals, and update it during installations, removals, and system updates.

Result: COMPLIANT

Impact: 5

Control: 03.04.11 - Information Location

Check: CheckInformationLocation

Description: Identify and document the location of CUI and the system components on which the information is processed and stored.

Result: COMPLIANT

Impact: 5

Control: 03.04.12 - System and Component Configuration for High-Risk Areas

Check: CheckHighRiskTravel

Description: Issue systems or components with organization-defined configurations to individuals traveling to high-risk locations. Apply organization-defined security requirements to systems or components upon return from travel.

Result: NOT COMPLIANT

Impact: 5

Control: 03.05.01 - User Identification and Authentication

Check: CheckUserIdentification

Description: Uniquely identify and authenticate system users, associating their identification with processes acting on their behalf. Re-authenticate users under organization-defined circumstances or situations.

Result: NOT COMPLIANT

Impact: 5

Control: 03.05.02 - Device Identification and Authentication

Check: CheckDeviceIdentification

Description: Uniquely identify and authenticate [Assignment: organization-defined devices or types of devices] before establishing a system connection.

Result: NOT COMPLIANT

Impact: 5

Control: 03.05.03 - Multi-Factor Authentication

Check: CheckMFA

Description: Use multi-factor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Result:

Impact: 5

Control: 03.05.04 - Replay-Resistant Authentication

Check: CheckRRA

Description: Implement Replay-Resistant Authentication.

Result: COMPLIANT

Impact: 5

Control: 03.05.05 - Identifier Management

Check: CheckIAM

Description: Receive authorization from organizational personnel or roles to assign an individual, group, role, service, or device identifier.

Result: COMPLIANT

Impact: 5

Control: 03.05.07 - Password Management

Check: CheckPasswordComplexity

Description: Enforce a minimum password complexity and change of characters when new passwords are created.

Result: COMPLIANT

Impact: 5

Control: 03.05.11 - Authentication Feedback

Check: TBI

Description: Authentication Feedback.

Result: TO BE IMPLEMENTED

Impact: 5

Control: 03.05.12 - Authenticator Management

Check: TBI

Description: Authenticator Management.

Result: TO BE IMPLEMENTED

Impact: 5

Control: 03.06.01 - Incident Handling

Check: CheckRA

Description: Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.

Result: COMPLIANT

Impact: 5

Control: 03.06.02 - Incident Monitoring, Reporting, and Response Assistance

Check: CheckRA

Description: Track and document system security incidents. Report suspected incidents to the organizational incident response team within the organization-defined time period and to designated authorities. Provide an incident response support resource for user assistance in handling and reporting incidents.

Result: COMPLIANT

Impact: 5

Control: 03.06.03 - Incident Response Testing

Check: CheckRA

Description: Test the effectiveness of the incident response capability [Assignment: organization-defined frequency].

Result: COMPLIANT

Impact: 5

Control: 03.06.04 - Incident Response Training

Check: CheckRA

Description: Provide incident response training to users based on roles within organization-defined timeframes, system changes, and at regular intervals. Review and update training after major events.

Result: COMPLIANT

Impact: 5

Control: 03.06.05 - Incident Response Plan

Check: CheckRA

Description: Develop an incident response plan that: Provides the organization with a roadmap for implementing its incident response capability.

Result: COMPLIANT

Impact: 5

Control: 03.07.04 - Maintenance Tools

Check: CheckMaintainanceTools

Description: Approve, control, and monitor the use of system maintenance tools. Check media with diagnostic and test programs for malicious code before use. Prevent the removal of maintenance equipment containing CUI by verifying, sanitizing, destroying, or retaining the equipment within the facility.

Result: NOT COMPLIANT

Impact: 5

Control: 03.07.05 - Nonlocal Maintenance

Check: CheckNonLocalMaintainance

Description: Approve and monitor nonlocal maintenance and diagnostic activities. Implement multi-factor authentication and replay resistance for nonlocal sessions. Terminate sessions and network connections upon completion of nonlocal maintenance.

Result: COMPLIANT

Impact: 5

Control: 03.07.06 - Maintenance Personnel

Check: CheckMaintainancePersonnel

Description: Establish a process for maintenance personnel authorization. Maintain a list of authorized maintenance personnel or organizations. Verify that non-escorted maintenance personnel have the necessary access authorizations. Assign authorized personnel with technical competence to supervise maintenance activities when required.

Result: COMPLIANT

Impact: 5

Control: 03.08.01 - Media Storage

Check: //

Description: Ensure physical control and secure storage of system media containing CUI.

Result: NOT APPLICABLE

Impact: 5

Control: 03.08.02 - Media Access

Check: //

Description: Verify that only authorized personnel or roles can access CUI on system media.

Result: NOT APPLICABLE

Impact: 5

Control: 03.08.03 - Media Sanitization

Check: //

Description: Ensure system media containing CUI are sanitized before disposal or reuse.

Result: NOT APPLICABLE

Impact: 5

Control: 03.08.04 - Media Marking

Check: //

Description: Verify system media containing CUI are properly marked with handling and distribution information.

Result: NOT APPLICABLE

Impact: 5

Control: 03.08.05 - Media Transport

Check: //

Description: Ensure protection and accountability of CUI media during transport, and document transport activities.

Result: NOT APPLICABLE

Impact: 5

Control: 03.08.07 - Media Use

Check: //

Description: Enforce restrictions on system media usage, including removable media without identifiable ownership.

Result: NOT APPLICABLE

Impact: 5

Control: 03.08.09 - System Backup â€” Cryptographic Protection

Check: //

Description: Ensure backups containing CUI are protected with cryptographic mechanisms to prevent unauthorized access.

Result: NOT APPLICABLE

Impact: 5

Control: 03.09.01 - Personnel Screening

Check: //

Description: Verify that individuals are screened before being granted system access, and that rescreening is conducted as per defined conditions.

Result: NOT APPLICABLE

Impact: 5

Control: 03.09.02 - Personnel Termination and Transfer

Check: //

Description: When employment is terminated, disable system access within the organization-defined time period, revoke credentials, and retrieve security-related property.

Result: NOT APPLICABLE

Impact: 5

Control: 03.10.01 - Physical Access Authorizations

Check: //

Description: Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides. Issue authorization credentials and review the access list at an organization-defined frequency. Remove individuals from the list when access is no longer required.

Result: NOT APPLICABLE

Impact: 5

Control: 03.10.02 - Monitoring Physical Access

Check: //

Description: Verify that physical access to the facility is monitored, and access logs are regularly reviewed and analyzed for incidents.

Result: NOT APPLICABLE

Impact: 5

Control: 03.10.06 - Alternate Work Site

Check: //

Description: Ensure that alternate work sites are defined and meet specific security requirements set by the organization.

Result: NOT APPLICABLE

Impact: 5

Control: 03.10.07 - Physical Access Control

Check: //

Description: Check that physical access control measures are in place, including verification of authorizations, use of control systems, and maintenance of audit logs.

Result: NOT APPLICABLE

Impact: 5

Control: 03.10.08 - Access Control for Transmission

Check: //

Description: Verify that access to system distribution and transmission lines is controlled to prevent unauthorized physical access.

Result: NOT APPLICABLE

Impact: 5

Control: 03.11.01 - Risk Assessment

Check: CheckRA

Description: Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.

Update risk assessments [Assignment: organization-defined frequency].

Result: COMPLIANT

Impact: 5

Control: 03.11.02 - Vulnerability Monitoring and Scanning

Check: CheckMonitorAndScanning

Description: Monitor and scan the system for vulnerabilities at organization-defined intervals and when new vulnerabilities are identified. Remediate vulnerabilities within organization-defined response times. Update vulnerability scans at defined intervals and when new vulnerabilities are reported.

Result: NOT COMPLIANT

Impact: 5

Control: 03.11.04 - Risk Response

Check: CheckRiskRensponse

Description: Respond to findings from security assessments, monitoring, and audits.

Result: NOT COMPLIANT

Impact: 5

Control: 03.12.01 - Security Assessment

Check: CheckSA

Description: Assess the security requirements for the system and its environment of operation [Assignment: organization-defined frequency] to determine if the requirements have been satisfied.

Result: COMPLIANT

Impact: 5

Control: 03.12.02 - Plan of Action and Milestones

Check: TBI

Description: Develop and update a plan of action to remediate weaknesses and reduce vulnerabilities based on security assessments, audits, and monitoring.

Result: TO BE IMPLEMENTED

Impact: 5

Control: 03.12.03 - Continuous Monitoring

Check: CheckCM

Description: Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.

Result: COMPLIANT

Impact: 5

Control: 03.12.05 - Information Exchange

Check: CheckIE

Description: Approve and manage CUI exchanges between systems using agreements like security or information exchange agreements, MOUs, SLAs, or NDAs. Document interface details, security requirements, and responsibilities, and review agreements regularly.

Result: COMPLIANT

Impact: 5

Control: 03.13.01 - Boundary Protection

Check: CheckBP

Description: Ensure communications at external and key internal interfaces are monitored and controlled, and that publicly accessible components are segregated from internal networks.

Result: COMPLIANT

Impact: 5

Control: 03.13.04 - Information in Shared System Resources

Check: CheckISR

Description: Check for controls that prevent unauthorized information transfer through shared resources.

Result: COMPLIANT

Impact: 5

Control: 03.13.06 - Network Communications â€” Deny by Default â€” Allow by Exception

Check: CheckNetworkTraffic

Description: Verify that network traffic is denied by default and only allowed by explicit exceptions.

Result: NOT COMPLIANT

Impact: 5

Control: 03.13.08 - Transmission and Storage Confidentiality

Check: CheckTSC

Description: Ensure that cryptographic methods are in place to protect CUI during both transmission and storage.

Result: NOT COMPLIANT

Impact: 5

Control: 03.13.09 - Network Disconnect

Check: CheckNetworkDisconnect

Description: Check for automatic termination of network connections after sessions end or periods of inactivity.

Result: COMPLIANT

Impact: 5

Control: 03.13.10 - Cryptographic Key Establishment and Management

Check: CheckCKEM

Description: Verify that cryptographic keys are managed according to defined policies for generation, storage, and destruction.

Result: COMPLIANT

Impact: 5

Control: 03.13.11 - Cryptographic Protection

Check: CheckCP

Description: Ensure appropriate cryptographic methods are used to safeguard CUI.

Result: NOT COMPLIANT

Impact: 5

Control: 03.13.12 - Collaborative Computing Devices and Applications

Check: CheckCCDA

Description: Check for controls that prohibit remote activation of devices, with clear indicators of use for physically present users.

Result: COMPLIANT

Impact: 5

Control: 03.13.13 - Mobile Code

Check: CheckMC

Description: Ensure the organization has policies in place for acceptable use of mobile code and monitors its implementation.

Result: COMPLIANT

Impact: 5

Control: 03.13.15 - Session Authenticity

Check: CheckSessionAuthenticity

Description: Verify measures that ensure the authenticity and integrity of communications sessions.

Result: COMPLIANT

Impact: 5

Control: 03.14.01 - Flaw Remediation

Check: CheckFlawRemediation

Description: Ensure system flaws are identified, reported, and corrected. Verify that security updates are installed within the defined time frame.

Result: COMPLIANT

Impact: 5

Control: 03.14.02 - Malicious Code Protection

Check: CheckMalwareProtection

Description: Check that malicious code protection mechanisms are in place, updated regularly, and configured to scan the system at defined intervals.

Result: COMPLIANT

Impact: 5

Control: 03.14.03 - Security Alerts, Advisories, and Directives

Check: CheckSecurityAlerts

Description: Verify that the organization receives external security alerts and disseminates internal alerts as needed.

Result: COMPLIANT

Impact: 5

Control: 03.14.06 - System Monitoring

Check: CheckSystemMonitoring

Description: Ensure that system monitoring is in place to detect attacks, unauthorized connections, and unusual activities.

Result: COMPLIANT

Impact: 5

Control: 03.14.08 - Information Management and Retention

Check: TBI

Description: Verify that CUI is managed and retained in compliance with legal and operational requirements.

Result: TO BE IMPLEMENTED

Impact: 5

Control: 03.15.01 - Policy and Procedures

Check: //

Description: Ensure that security policies and procedures are developed, documented, disseminated, and regularly reviewed and updated.

Result: NOT APPLICABLE

Impact: 5

Control: 03.15.02 - System Security Plan

Check: //

Description: Verify that a comprehensive system security plan is developed, maintained, and addresses system components, threats, and security requirements.

Result: NOT APPLICABLE

Impact: 5

Control: 03.15.03 - Rules of Behavior

Check: //

Description: Check that rules of behavior are established, disseminated, acknowledged by users, and regularly reviewed.

Result: NOT APPLICABLE

Impact: 5

Control: 03.16.01 - Security Engineering Principles

Check: CheckSEP

Description: Ensure that security engineering principles are applied to system development and modifications.

Result: NOT COMPLIANT

Impact: 5

Control: 03.16.02 - Unsupported System Components

Check: //

Description: Verify that unsupported system components are replaced or that risk mitigation measures are implemented when replacement is not possible.

Result: NOT APPLICABLE

Impact: 5

Control: 03.16.03 - External System Services

Check: //

Description: Ensure that external service providers comply with defined security requirements, and that roles and monitoring processes are in place.

Result: NOT APPLICABLE

Impact: 5

Control: 03.17.01 - Supply Chain Risk Management Plan

Check: //

Description: Ensure a supply chain risk management plan is developed, maintained, regularly reviewed, and protected from unauthorized access.

Result: NOT APPLICABLE

Impact: 5

Control: 03.17.02 - Acquisition Strategies, Tools, and Methods

Check: //

Description: Verify that acquisition strategies, tools, and methods are in place to mitigate supply chain risks.

Result: NOT APPLICABLE

Impact: 5

Control: 03.17.03 - Supply Chain Requirements and Processes

Check: //

Description: Ensure processes are in place to address supply chain risks and that security requirements are enforced to protect the system and its components.

Result: NOT APPLICABLE

Impact: 5

Control: 03.17.01 - Supply Chain Risk Management Plan

Check: //

Description: Ensure a supply chain risk management plan is developed, maintained, regularly reviewed, and protected from unauthorized access.

Result: NOT APPLICABLE

Impact: 5

Control: 03.17.02 - Acquisition Strategies, Tools, and Methods

Check: //

Description: Verify that acquisition strategies, tools, and methods are in place to mitigate supply chain risks.

Result: NOT APPLICABLE

Impact: 5

Control: 03.17.03 - Supply Chain Requirements and Processes

Check: //

Description: Ensure processes are in place to address supply chain risks and that security requirements are enforced to protect the system and its components.

Result: NOT APPLICABLE

Impact: 5

Control: 03.06.01 - 1

Check: ch3k

Description: 1

Result: COMPLIANT

Impact: 5