

REPORT DOCUMENTATION PAGE					Form Approved OMB No. 0704-0188	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.						
1. REPORT DATE (DD-MM-YYYY) 09/01/2015		2. REPORT TYPE Technical Report			3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE Security Control Assessment Guides				5a. CONTRACT NUMBER FA8702-14-C-0001		
				5b. GRANT NUMBER		
				5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) Adams, Nathan; Hahn, Adam; Koch, Chriss G.; Rubinovitz, Harvey H.; Bielski, James J.; Thompson, Carmella; Shomo, Milton; Finegan, James A.; Brown, Christine; Cintron, Jose J.;				5d. PROJECT NUMBER		
				5e. TASK NUMBER		
				5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) The MITRE Corporation 202 Burlington Road Bedford, MA 01730-1420					8. PERFORMING ORGANIZATION REPORT NUMBER PRS-19-3536	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) AFLCMC/HN Hanscom AFB, MA					10. SPONSOR/MONITOR'S ACRONYM(S)	
					11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.						
13. SUPPLEMENTARY NOTES						
14. ABSTRACT Practical guidance for information security (IS) engineers who conduct security control assessments for systems that must meet federal guidance. This guide focuses on controls required by NIST SP 800-53. Included are: 1-Application Security Control Assessment Guide; 2-Database Security Control Assessment Guide; 3-Management and Operations Security Control Assessment Guide; 4-Network Security Control Assessment Guide; 5-Unix Security Control Assessment Guide; 6-Windows Security Control Assessment Guide.						
15. SUBJECT TERMS Software Engineering (General); Network Security; Information Systems Security; Database Management, application security; control assessment; access control; database security; Windows; risk assessment; UNIX; network security						
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 206	19a. NAME OF RESPONSIBLE PERSON Susan Carpenito	
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include area code) 781-271-7646	

Application Security Control Assessment Guide

The views, opinions and/or findings contained in this guide are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Approved for Public Release: 19-3536.
Distribution Unlimited.

©2019 The MITRE Corporation. All rights reserved.

Author(s): Nathan Adams
Adam Hahn
Chriss Koch

September 2015

Colorado Springs, CO

MITRE

This page intentionally left blank.

Table of Contents

1. Overview	1
1.1 Caveats	1
1.2 Assessment Methodology	1
1.2.1 Phase 1: Planning	1
1.2.2 Phase 2: Assessment	1
1.2.3 Phase 3: Reporting	2
2. Assessment Activities	3
2.1 Phase 1: Planning	3
2.2 Phase 2: Assessment	3
2.2.1 Application Testing	3
2.2.2 Tools	4
2.2.3 Interviews	5
2.3 Phase 3: Reporting	5
3. Assessing Security Controls	6
3.1 Access Control (AC)	6
3.2 Awareness and Training (AT)	10
3.3 Audit and Accountability (AU)	10
3.4 Certification, Accreditation, and Security Assessments (CA)	12
3.5 Configuration Management (CM)	12
3.6 Contingency Planning (CP)	13
3.7 Identification and Authentication (IA)	13
3.8 Incident Response (IR)	15
3.9 Maintenance (MA)	15
3.10 Media Protection (MP)	15
3.11 Physical and Environmental Protection (PE)	15
3.12 Planning (PL)	15
3.13 Personnel Security (PS)	16
3.14 Risk Assessment (RA)	16
3.15 System and Services Acquisition (SA)	16
3.16 System and Communications Protection (SC)	16
3.17 System and Information Integrity (SI)	21
3.18 Program Management (PM)	23
4. References	24

5. Acronyms.....	25
------------------	----

List of Tables

Table 1. Access Control Requirement Evaluation	6
Table 2. Audit and Accountability Requirement Evaluation	10
Table 3. Configuration Management Requirement Evaluation.....	12
Table 4. Identification and Authentication Requirement Evaluation.....	13
Table 5. System and Communications Protection Requirement Evaluation	16
Table 6. System and Information Integrity Requirement Evaluation	21

This page intentionally left blank.

1. Overview

This *Application Security Assessment Guide* is intended to serve as practical guidance for information security (IS) engineers who conduct application security control assessments for systems that must meet federal guidance. This guide focuses on testing and evaluation techniques for technical controls required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*. Parameters defined in this guide are considered industry best practice but may be modified by the organization as required.

1.1 Caveats

The controls presented here are for a Federal Information Processing Standard (FIPS) 199 Moderate Impact rated system. Thus, controls for Low and High Impact rated systems may differ.

This guide focuses on technical testing for Web applications, Web services, and thick-client applications. Testing the security of such systems requires experienced evaluators familiar with a multitude of application languages, technologies, components and testing tools. It is assumed the evaluators have the requisite understanding and experience in these areas.

In many cases, performing an application security assessment has the potential to modify data, system configurations, and system availability. Care should be taken to understand how specific tests impact the system. It is highly recommended to perform tests in a validation / test environment where the application mimics the production instance rather than testing the production application itself. However, efforts must be made to understand all environmental differences between the production and validation / test environments and how these differences affect the test results.

1.2 Assessment Methodology

1.2.1 Phase 1: Planning

The first phase, Planning, defines the assessment's scope, establishes goals, sets boundaries, and identifies assessment activities. During the planning phase, the Evaluation Team reviews all security policies and procedures in accordance with the defined security requirements. Requests for information / artifacts are made that allow for a detailed understanding of the tested environment. The team then creates assessment scenarios and defines agreeable terms as approved by the organization. This phase, as well as all subsequent phases, requires the coordination of all involved parties.

1.2.2 Phase 2: Assessment

Phase 2, Assessment, may have several steps depending on the assessment's objectives, scope, and goals as set forth in the Planning Phase. These steps can be grouped, as follows, by the nature of the activities involved:

- **Information Collection**—activities that provide information about the system/application. This information must be collected before any meaningful assessment can be conducted. The data collected is analyzed as the assessment proceeds.
- **Enumeration**—activities that provide specific information about each system component. This information is often collected using appropriate software tools.
- **Testing and Review**—activities that involve both the automated testing of security vulnerabilities via software tools as well as the evaluation of particular aspects of the organization's security policies and practices by Evaluation Team members.

1.2.3 Phase 3: Reporting

Phase 3, Reporting, documents the soundness of the implemented security controls and consolidates all findings into the final output. This output includes reports that provide a summary of key findings and actionable recommendations, as well as provisions for all information derived from the assessment.

2. Assessment Activities

The following activities describe techniques that assist an Evaluation Team when assessing a system. These activities must be thoroughly developed and documented prior to the beginning of any assessment. Additionally, the activities must be specific to the technology and systems being assessed as well as able to determine the appropriate compliance level: low, moderate or high.

2.1 Phase 1: Planning

The Application Evaluator reviews the Security Assessment Test Plan to understand the scope of the assessment before reviewing the organization security policies, procedures, and requirements. As system documentation is received, the Application Evaluator reviews the documentation to ensure he/she has a full understanding of both the system being assessed, and the components being evaluated. To ensure an efficient onsite application test, the Application Evaluator confirms access to the application using assigned test accounts. The Application Evaluator also determines any additional requests required to conduct the assessment. These requests are communicated with the Lead Evaluator so that he/she can reach out to both the system's point of contact (POC) and the organization facilitator to ensure a successful assessment.

2.2 Phase 2: Assessment

The application assessment consists of tool selection, application testing, and personnel interviews. All activities must be able to determine the appropriate compliance level: low, moderate, or high.

2.2.1 Application Testing

The Application Evaluator will test the application to ensure proper software development techniques, use of supported software, and that the confidentiality, integrity and availability (CIA) of data processed by the application adheres to the defined policies, procedures, and standards. The Application Evaluator will use the test accounts and corresponding roles to perform the following:

- Assess if input parameters passed to the application are checked and validated
- Determine if application administrators can remotely access the application via organization-approved standards
- Examine implemented access control and identification and authentication techniques
- Test to determine if the application is susceptible to cross-site scripting (XSS), structured query language (SQL) injection, or other vulnerabilities, as applicable

- Examine sensitive information to determine if it is encrypted before being passed between the application and browser

2.2.2 Tools

Various tools are used during the assessment. In some cases, evaluators have their own tool preferences while in others the testing environment dictates which tools must be used. The following non-exhaustive list provides a sample list of tool types that all evaluators must be familiar with to test applications:

- **Automated Structured Query Language (SQL) Injection**—Automates the process of downloading the schema and contents of a database that is vulnerable to both visible and blind SQL injection attacks
- **Cryptographic Protocol and Cipher Analysis**—Assesses cryptographic protocols in use, strength of ciphers supported, and validity of digital certificates
- **Disassembler and Decompiler**—Unpacks executable files or decompile interpreted code (ex: Java) to find sensitive information that can be used to exploit the application
- **Fuzzers**—Creates malformed input used to provide random data to an application's parameters
- **Open Source Enumeration Scanners**—Discovers publicly available application misconfigurations
- **Network Port Mapper/Scanner**—Performs network exploration or security auditing through User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) port scanning
- **Network Protocol Analyzer**—Intercepts and logs traffic passing over a network as well as decodes and analyzes the contents according to the appropriate protocol specifications
- **Network Vulnerability Scanner**—Scans systems for security vulnerabilities found via services, ports, and system patch levels
- **Session Analyzer**—Analyzes session variables (cookies) and their generation algorithms
- **Web Application Proxy**—Intercepts, modifies, and tests communications between a client browser and Web application
- **Web Server Vulnerability Scanner**—Identifies vulnerabilities in Web server configurations and patch levels
- **Web Services Tool**—Tests communications and security between web services

2.2.3 Interviews

Initial discussions and follow-on interviews are conducted as necessary with the application developer or maintainer to confirm potential findings. These interviews are conducted with both the Application Evaluator and the Management and Operations (M&O) Evaluator present. The technical questions help supplement and corroborate the M&O interview questions. They also serve to provide more in-depth analysis for certain controls requiring additional scrutiny. Questions are tailored to the application environment and its implementations.

2.3 Phase 3: Reporting

The Application Evaluator must document all weaknesses and forward their report to the Lead Evaluator for consolidation and discussion. Additionally, the Application Evaluator must discuss any Moderate or High findings with the support staff prior to the out-brief so it is not the first time staff are exposed to the findings and supporting evidence.

During this phase, it is beneficial for the closure evidence to be presented and reviewed by the Application Evaluator. Since evidence is very difficult to verify once the Evaluation Team has left, it is best to present this evidence while on site. However, all testing and change control procedures must be adhered to as this could result in a finding. If closure evidence is confirmed, the finding should not be removed from the report, but it can be closed if the Application Evaluator determines that the provided evidence is adequate to close the finding.

The reporting phase includes a documentation of the soundness of the implemented security controls. The actual findings are consolidated into a final report.

3. Assessing Security Controls

This section outlines a list of the security controls specified in NIST SP 800-53 as well as the corresponding checks and procedures used to verify that Web applications, Web services, and thick-client applications are in compliance with NIST 800-53 and organization requirements. Check and procedure entries of 'N/A' indicate that the security control lacks an applicable application test.

3.1 Access Control (AC)

Table 1 lists AC checks and procedures.

Table 1. Access Control Requirement Evaluation

Requirement	Checks and Procedures
AC-1 Access Control Policy and Procedures	N/A
AC-2 Account Management	For Web Applications and Thick-Client Applications: Ensure each user has a unique account if user accounts are necessary. • Check potentially vulnerable user accounts: inactive, temporary, training, test, demo, default • Extract user account data from the production system for analysis including: account identifier, first name, last name, enabled / disabled status, role, creation date, last login date, failed login date, failed login count, password change date, etc. • Perform analysis to discover accounts that are: ○ Enabled and have never been used ○ Enabled and have been unused for greater than the days allowed for maximum password age ○ Enabled with high privileges that are inactive ○ Enabled with high privileges that have failed logins due to incorrect passwords ○ Disabled due to failed logins with incorrect passwords ○ Enabled and default (especially with default password) ○ Group / system accounts Ensure appropriate account management features exist, such as: • Automatic suspension of temporary and emergency accounts • Automatic suspension of inactive accounts • Audit and notification of account creation, modification, disabling and termination actions

Requirement	Checks and Procedures
AC-3 Access Enforcement	For Web Applications and Web Services: Ensure that resources requiring authorization perform adequate authorization checks before a user can access them. • Use a Web application proxy tool to strip session identifiers or cookies from the request • Attempt to directly access application resources without logging in using those identifiers and cookies Ensure that the application has a logoff feature and that the session token is invalidated on the Web server when the user logs out. • Using a Web application proxy tool, log out of the Web application and attempt to re-use the session token to access site resources. Ensure that the application enforces its access control model such that any parameters available to an attacker would not afford additional service. • Using a Web application proxy tool, attempt manipulation of parameters, form fields, uniform resource locator (URL) query strings, client-side script code and values, and session tokens. Ensure that session tokens are changed when the user moves from an encrypted protected resource to a non-encrypted protected resource and vice-versa. • Using a Web application proxy tool, note the session ID/token assigned before logging in to an encrypted protected site. • Log in and check the session ID/token. If it remains the same then the same session token is being re-used pre and post authentication. Ensure the application implements measures to prevent Cross-Site Request Forgery Attacks. • Check for a CSRFTOKEN in the HTML • If using ASP.NET, maintain the ViewState • Check for double submit cookies • Challenge-Response • Check to see if the application checks the HTML Referer Header Additionally for Web Services and Thick-Client Applications: Ensure network access control lists (ACLs) are in place and effective. Ensure all privileged functions are appropriately protected (vertical/horizontal privilege escalations). Ensure all data source access is enforced through the application by verifying that the user is not able to make direct connections with data sources.

Requirement	Checks and Procedures
AC-4 Information Flow Enforcement	For Web Applications: Ensure that the application enforces information flow control policies and enforcement mechanisms to control information flow between designated sources and destinations (networks and devices) within the application and between interconnected systems. In many cases flow control will depend on the type of information maintained by the application. • The application should not perform Cross-Domain JavaScript or Flash. • All Hypertext Transfer Protocol (HTTP) requests should be directed to the same domain (protocol, domain, port). • Inspect whether any external Web resources are loaded with the same domain as the application. Ensure that where the application requires the user to perform actions in a specific sequence, the sequence is enforced. • Using a Web application proxy tool, attempt to perform application steps that diverge from their intended order, i.e. skipping steps for enrollment, modifying parameters to disturb application flow. Ensure that all information that has been checked on the client side is then checked on the server side.
AC-5 Separation of Duties	N/A
AC-6 Least Privilege	For Web Applications, Web Services, and Thick-Client Applications: Ensure least privilege is enforced. • Review user privileges in the application against documented privilege requirements to ensure there are no excessive privileges assigned to users. • Determine which roles are exclusive and cannot be combined with other roles. Ensure that the application enforces its access control model such that any parameters available to an attacker would not afford vertical/horizontal privilege escalation. • Use a Web application proxy tool and attempt manipulation of form fields, URL query strings, client-side script values, and session tokens. • Attempt path traversal (e.g., ../etc/passwd)
AC-7 Unsuccessful Login Attempts	For Web Applications, Web Services, and Thick-Client Applications: Ensure that after entering an incorrect password some number of times within some time period the account is temporarily invalidated. Ensure the lockout persists for a minimum period of time.

Requirement	Checks and Procedures
AC-8 System Use Notification	For Web Applications and Thick-Client Applications: Ensure the application displays a warning banner in a prominent space and requires the user to acknowledge it before entering their credentials. The banner should notify users that: • They are accessing a <organization> information system • The <organization> maintains ownership and responsibility for its computer systems • Users must adhere to <organization> IS Policies, Standards and Procedures • Their usage may be monitored, recorded and audited • Unauthorized use is prohibited and subject to criminal and civil penalties • The use of the information system establishes the user's consent to any and all monitoring and recording of their activities Ensure the warning banner is developed in conjunction with legal counsel. Ensure clear privacy policies are posted on Web sites, major entry points to a Web site, and any Web page where substantial personal information from the public is collected. For Web Services: Ensure there is a system use notification wherever the service is supplied such as within the service responses or Web Services Description Language (WSDL).
AC-9 Previous Logon (Access) Notification	For Web Applications, Web Services, and Thick-Client Applications: Ensure there is no concurrent session control • Attempt to log in to the application simultaneously with the same user account via two different browsers or test machines. • If login is successful then concurrent sessions are not controlled.
AC-10 Concurrent Session Control	For Web Applications: Ensure that a session is locked/terminated and that it requires users to re-authenticate after a threshold of inactivity. • Log into the website but don't issue a request for a period of time • Attempt to navigate an authenticated portion of the site • If navigation is possible, the session is still valid For Thick-Client Applications: Ensure that after a session has been locked remotely, it is impossible to navigate to an authenticated portion of the site.
AC-11 Session Lock	For Web Applications: Ensure that permitted actions without identification or authentication cannot take place by requesting documentation specifying which user actions can be performed on the application without requiring identification or authentication. Then, determine whether the areas that do not require identification and authentication are justified.
AC-12 Session Termination	N/A
AC-14 Permitted Actions without Identification or Authentication	N/A

Requirement	Checks and Procedures
AC-16 Security Attributes	N/A
AC-17 Remote Access	N/A
AC-18 Wireless Access	For Web Applications: Ensure that the organization understands the terms and conditions of the external source as well as how the application data relates to it. For example • The application should not perform Cross-Domain JavaScript or Flash. • All HTTP requests should be directed to the same domain (protocol, domain, port). • Inspect whether any external Web resources are loaded with the same domain as the application. • No PII should be sent from the application to the external source. For Web Services: Ensure that the organization understands the terms and conditions of the external source.
AC-19 Access Control for Mobile Devices	N/A
AC-20 Use of External Information Systems	N/A
AC-22 Publicly Accessible Content	N/A
AC-21 Information Sharing	N/A
AC-23 Data Mining Protection	N/A
AC-24 Access Control Decisions	N/A
AC-25 Reference Monitor	N/A

3.2 Awareness and Training (AT)

There are no application checks and procedures in this section.

3.3 Audit and Accountability (AU)

Table 2 lists AU checks and procedures.

Table 2. Audit and Accountability Requirement Evaluation

Requirement	Checks and Procedures
AU-1 Audit and Accountability Policy and Procedures	N/A

Requirement	Checks and Procedures
AU-2 Auditable Events	For Web Applications, Thick-Client Applications and Web Services: Ensure the following events are audited: • User account management activities (password change, user creation, use of administrator privileges, etc.) • User account activities (password change, email update, login, etc.) • Application activities (shutdown, restart, errors, etc.) • Security policy modifications
AU-3 Content of Audit Records	For Web Applications, Thick-Client Applications, and Web Services: Ensure the application generates the following information for each event: • Date and Time • Component where the event occurred (ex: URL in a Web Application) • Type • User / Subject identity • Outcome (success or failure)
AU-4 Audit Storage Capacity	N/A
AU-5 Response to Audit Processing Failures	For Web Applications, Thick-Client Applications, and Web Services: Ensure actions are taken when processing failures are detected and noted within the audit logs. This is particularly important when auditing is done locally within the application as opposed to remotely.
AU-6 Audit Review, Analysis, and Reporting	For Web Applications, Thick-Client Applications, and Web Services: Ensure that the organization regularly reviews/analyzes Audit Logs for inappropriate or unusual activity according to an organization specified timeline.
AU-7 Audit Reduction and Report Generation	For Web Applications, Thick-Client Applications, and Web Services: Ensure the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.
AU-8 Time Stamps	For Web Applications, Thick-Client Applications, and Web Services: Ensure the application contains timestamps (date and time) for each logged event by executing transactions to verify that application audit records are created.
AU-9 Protection of Audit Information	For Web Applications, Thick-Client Applications, and Web Services: Ensure that application audit logs are protected from unauthorized access, modification, and deletion. If applicable, attempt to view/modify/delete audit information with a low privilege level account that should not have this access.
AU-10 Non-Repudiation	For Web Applications, Thick-Client Applications, and Web Services: Ensure application and system auditing contains the ability to determine whether an individual has taken a specific action in the application. If audit records are stored in a database, determine if user accounts can be cross-referenced to entries in the database log to provide for non-repudiation.
AU-11 Audit Record Retention	For Web Applications, Thick-Client Applications, and Web Services: Ensure the organization retains application audit records for an organization specified length of time.
AU-12 Audit Generation	For Web Applications, Thick-Client Applications, and Web Services: Ensure necessary reports are generated with the information defined in AU-2 and AU-3. This is particularly important when auditing is done locally within the application as opposed to remotely.

Requirement	Checks and Procedures
AU-13 Monitoring for Information Disclosure	N/A
AU-14 Session Audit	N/A
AU-15 Alternate Audit Capability	N/A
AU-16 Cross-Organizational Auditing	N/A

3.4 Certification, Accreditation, and Security Assessments (CA)

There are no application checks and procedures in this section.

3.5 Configuration Management (CM)

Table 3.3 lists CA checks and procedures.

Table 3. Configuration Management Requirement Evaluation

Requirement	Checks and Procedures
CM-1 Configuration Management Policy and Procedure	N/A
CM-2 Baseline Configuration	N/A
CM-3 Configuration Change Control	N/A
CM-4 Security Impact Analysis	N/A
CM-5 Access Restrictions for Change	N/A
CM-6 Configuration Settings	For Web Applications, Thick-Client Applications and Web Servers: Ensure configuration settings are up to date. • Use a Web Vulnerability Scanner or Network Vulnerability Scanner to scan the Web server hosting the application for the presence of: ○ Dangerous files/directories/Common Gateway Interfaces (CGIs) ○ Outdated server versions and installed software ○ Server configuration items (ex: multiple index files) ○ HTTP server options. • Review Web server, application server and any additional COTS configuration settings for security relevant parameters (PHP, ASP.Net, WebSphere, Apache, IIS, etc.).

Requirement	Checks and Procedures
CM-7 Least Functionality	For Web Applications and Thick-Client Applications: Ensure that the application is configured to provide only essential capabilities. • Use a Web or Network Vulnerability Scanner to scan for HTTP server options that are supported. Potentially dangerous HTTP methods may include: ○ PUT and DELETE – allows files to be placed on and removed from the host ○ CONNECT – allows a client to use the web server as a proxy ○ TRACE – used for debugging-purposes but could be used to mount a Cross Site Tracing Attack • Note that only the HEAD, GET, and POST methods are required for most web applications to function. • Attempt to uncover a hidden web server or application functionality via the following means ○ Automated scan using a Network Vulnerability Scanner or proxy ○ URL manipulation http://<webapplication>/admin/ ○ Comments in production code For Web Services: Ensure that any unnecessary Web services are disabled Ensure application roles employ a least privileged model where possible. Review the roles and privileges to ensure they are appropriately separated.
CM-8 Information System Component Inventory	N/A
CM-9 Configuration Management Plan	N/A
CM-10 Software Usage Restrictions	N/A
CM-11 User-Installed Software	N/A

3.6 Contingency Planning (CP)

There are no application checks and procedures in this section.

3.7 Identification and Authentication (IA)

Error! Reference source not found.4 lists IA checks and procedures.

Table 4. Identification and Authentication Requirement Evaluation

Requirement	Checks and Procedures
IA-1 Identification and Authentication Policy and Procedures	N/A

Requirement	Checks and Procedures
IA-2 User Identification and Authentication (Organizational Users)	For Web Applications and Thick-Client Applications: Ensure the application uniquely identifies and authenticates organizational users as per organization directives. In many cases, the level of authentication is commensurate with the data's value and thus may require two-factor authentication. Additionally for Web Services: Ensure all service accounts are authenticated by reviewing the following: • Access control for transaction to XML conversion processes • SAML assertions • Implementation of WS-Trust and WS-Federation if federated identity management is in use
IA-3 Device Identification and Authentication	N/A
IA-4 Identifier Management	For Web Applications, Web Services, and Thick-Client Applications: Ensure each user has a unique account by checking the appropriate logs. This is especially tricky to enforce when self-registration is permitted. Ensure accounts are disabled after specified period of inactivity.
IA-5 Authenticator Management	For Web Application and Thick-client Application: Ensure that the password complexity makes guessing passwords difficult and forces users to select a password comprising of an organization specified minimum complexity. Ensure that if default passwords are given to new users that these new passwords must be changed upon logon. Ensure password reuse is prohibited and the application forces users to select a number of unique passwords prior to reusing a previous one, determined by the organization. Ensure that the password change option is only available with authentication and does not contain any hidden values, including the username. Additionally, ensure that it asks the user for their previous password. Ensure the application enforces automatic expiration of passwords and enforces periodic password changes. Ensure that the application automatically forces users (including administrators) to change user and system account passwords after an organization specified number of days. Ensure that the user must respond to a secret answer or secret question or other predetermined information that is not easily guessable before passwords can be reset. Additionally, make sure that once the question has been answered, the user isn't dropped into an authenticated session, or given the forgotten password. Finally, make sure that the secret question cannot be enumerated after fresh logons (must be answered successfully first).

Requirement	Checks and Procedures
IA-6 Authenticator Feedback	For Web Applications and Thick-Client Applications: Ensure password information is not displayed when typed in by the user. Asterisks are typically used to obscure user input. Ensure that the application notifies users of their last day and login time as well as any unsuccessful login attempts. Ensure that major system actions such as password changes or account suspensions are sent to the user's registered email.
IA-7 Cryptographic Module Authentication	For Web Applications, Thick-Client Applications, and Web Services: Ensure certification based authentication is implemented correctly in reference to applicable laws, directives, policies, regulations, standards, and guidance for such authentication.
IA-8 Uniquely Identify and Authenticate (Non-Organizational Users)	For Web Applications and Thick-Client Applications: Ensure the application uniquely identifies and authenticates non-organizational users in accordance with the organization directives. Additionally for Web Services: Ensure all service accounts are authenticated by reviewing the following: • Access control for transaction to XML conversion processes • SAML assertions Implementation of WS-Trust and WS-Federation if federated identity management is in use.
IA-9 Service Identification and Authentication	N/A
IA-10 Adaptive Identification and Authentication	N/A
IA-11 Re-authentication	N/A

3.8 Incident Response (IR)

There are no application checks and procedures in this section.

3.9 Maintenance (MA)

There are no application checks and procedures in this section.

3.10 Media Protection (MP)

There are no application checks and procedures in this section.

3.11 Physical and Environmental Protection (PE)

There are no application checks and procedures in this section.

3.12 Planning (PL)

There are no application checks and procedures in this section.

3.13 Personnel Security (PS)

There are no application checks and procedures in this section.

3.14 Risk Assessment (RA)

There are no application checks and procedures in this section.

3.15 System and Services Acquisition (SA)

There are no application checks and procedures in this section.

3.16 System and Communications Protection (SC)

Error! Reference source not found.5 lists SC checks and procedures.

Table 5. System and Communications Protection Requirement Evaluation

Requirement	Checks and Procedures
SC-1 System and Communications Protection Policy and Procedures	N/A
SC-2 Application Partitioning	N/A
SC-3 Security Function Isolation	N/A

Requirement	Checks and Procedures
SC-4 Information in Shared Resources	For Web Applications: Ensure the application prevents unauthorized and unintended information transfer via shared system resources. • Review proxy servers for potential caching configuration and capabilities • Analyze use of HTTP GET parameters for sensitive data including authentication parameters, session tokens, and application specific data • Ensure the session token is non-persistent and is never written to the browser's history or cache. • Check to make sure autocomplete is disabled in the HTML FORM/INPUT • All HTML response headers or HTML meta tags should include: ◦ Expires: 0 ◦ Cache_control: no_cache ◦ Pragma: no_cache For Web Services: Ensure Web service/XML files are deleted from WAS/mid-tier servers in an unencrypted format. For Thick-Client Applications: Ensure source code is not present on any servers. Ensure appropriate thick client software operations for local or improper remote storage of sensitive data.
SC-5 Denial of Service Protection	For Web Applications and Thick-Client Applications: Ensure appropriate protections are in place to prevent DoS attacks in the application. Potential DoS attacks against the application include: • SQL wildcard attacks • Buffer overflows • User specified object allocation • Accessing underlying applications that can shut down the system For Web Services: Ensure appropriate firewall protections are in place to prevent networking DoS attacks. Ensure the XML parser protects against application level DoS attacks through: • Manipulating the XML (inserting, removing and reordering tags) • Sending excessively large XML payloads • Exploring input ranges and size • Investigating recursive tags
SC-6 Resource Priority	N/A
SC-7 Boundary Protection	N/A

Requirement	Checks and Procedures
SC-8 Transmission Confidentiality and Integrity	For Web Applications: Ensure that users are only asked to submit authentication credentials on pages that are served with TLS. • All transmitted credentials must be encrypted using TLS protocols. • The following command using OpenSSL should fail: <pre>openssl s_client -no_tls1 -no_ssl3 -connect <server>:443</pre> Ensure the application uses valid digital certificates (signature, host, date, etc.). • Digital certificates must be obtained from a valid certificate authority and must not be expired. • The following command using OpenSSL should pass: <pre>openssl s_client -CAfile <file> -connect <server>:443</pre> Ensure all credentials and data are being sent encrypted by using a Network Protocol Analyzer to sniff traffic from the browser to the web server. Ensure the application does not store unencrypted passwords. • Check the data supplied • The application may display a user password in the HTML page of the password reset page. Ensure that session tokens have the secure flag set, preventing them from being transmitted over HTTP. Ensure that if the application is using HTTPS; port 80 is not being used. Ensure that session tokens are not being transmitted in the URL query string. For Web Services: Ensure information requiring significant integrity is protected with appropriate cryptographic mechanisms. Can typically be performed with TLS, XML Encryption/XML Signatures, or WS-Security. Ensure all credentials and data are being sent encrypted by using a Network Protocol Analyzer to sniff traffic from the browser to the web server. Ensure that session tokens are not being transmitted in the URL query string. For Thick-Client Applications: Ensure that users are only asked to submit authentication credentials over encrypted channels. • All transmission of credentials must be encrypted. This can be determined by using a Network Protocol Analyzer to sniff traffic from the thick-client to the backend • Only ciphers compliant with organizational directives should be used Ensure the application does not store unencrypted passwords by requesting the relevant data.

Requirement	Checks and Procedures
SC-10 Network Disconnect	For Web Applications and Thick-Client Applications: Ensure that the session is terminated and that it requires users to re-authenticate. • Attempt to navigate an authenticated portion of the application after a network disconnect • If navigation is possible, the session is still valid
SC-11 Trusted Path	For Web Applications: Ensure that any attempts the application makes to verify trusted path are successful. For example, if CAPTCHA is employed, make sure the answer doesn't appear in a hidden form field.
SC-12 Cryptographic Key Establishment and Management	For Web Applications: Ensure the website uses an appropriate length key, such as 128-/256-bit encryption as defined by the organization. This can be determined by running OpenSSL.
SC-13 Cryptographic Protection	For Web Application: Ensure that only organizationally compliant ciphers are used by running OpenSSL. Ensure that only approved hash functions are implemented (e.g., SHA-256 and above). For Web Services and Thick-Client Applications: Ensure the service or application establishes connections with organizationally compliant algorithms.
SC-15 Collaborative Computing	N/A
SC-17 Public Key Infrastructure Certificates	N/A
SC-18 Mobile Code	For Web Services and Thick-client Application: Ensure client certificates are securely created and distributed.
SC-19 Voice Over Internet Protocol	For Web Application: Ensure that the application abides by the mobile code usage restrictions and implementation guidance specified by the organization if mobile code exists. Examples of mobile code technologies include Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript.
SC-20 Secure Name/Address Resolution Service (Authoritative Source)	N/A
SC-21 Secure Name/Address Resolution Service (Recursive and Caching Resolver)	N/A
SC-22 Architecture and Provisioning for Name/Address Resolution Service	N/A

Requirement	Checks and Procedures
SC-23 Session Authenticity	For Web Applications, Web Services and Thick-Client Applications: Ensure that the information system provides mechanisms to protect the authenticity of communicated sessions. These mechanisms should protect against man-in-the-middle attacks such as: • Session hijacking • Inserting false information into the session Ensure that the session token is of adequate length and cryptographically random to provide protection from guessing/forging attacks since session tokens that are predictable may also present vulnerability to session hijacking. • Collect a sufficient number of session token samples • Analyze the session token in an attempt to determine the generation algorithm • Attempt to forge a valid session token
SC-24 Fail in Known State	For Web Applications, Web Services and Thick-Client Applications: Ensure that the application does not expose sensitive data as a result of failures such as: • Buffer overflows • SQL Injection attacks • Attempting to visit an invalid address/file
SC-25 Thin Nodes	N/A
SC-26 Honeypots	N/A
SC-27 Platform Independent Applications	N/A
SC-28 Protection of Information at Rest	N/A
SC-29 Heterogeneity	N/A
SC-30 Concealment and Misdirection	N/A
SC-31 Covert Channel Analysis	N/A
SC-32 Information System Partitioning	N/A
SC-34 Non-Modifiable Executable Programs	N/A
SC-35 Honeyclients	N/A
SC-36 Distributed Processing and Storage	N/A
SC-37 Out-of-Band Channels	N/A
SC-38 Operations Security	N/A

Requirement	Checks and Procedures
SC-39 Process Isolation	N/A
SC-40 Wireless Link Protection	N/A
SC-41 Port and I/O Device Access	N/A
SC-42 Sensor Capability and Data	N/A
SC-43 Usage Restrictions	N/A
SC-44 Detonation Chambers	N/A

3.17 System and Information Integrity (SI)

Error! Reference source not found.6 lists SI checks and procedures.

Table 6. System and Information Integrity Requirement Evaluation

Requirement	Checks and Procedures
SI-1 System and Information Integrity Policy and Procedures	N/A
SI-2 Flaw Remediation	For Web Applications, Web Services, and Thick-Client Applications: Ensure that the Web server, application framework, and/or middleware technology is patched to the latest version.
SI-3 Malicious Code Protection	N/A
SI-4 Information System Monitoring	N/A
SI-5 Security Alerts, Advisories and Directives	For Web Applications, Web Services, and Thick-Client Applications: Ensure that any available security alerts/advisories from the product vendors whose underlying technologies are used for the application are received and reviewed by the appropriate personnel.
SI-6 Security Function Verification	N/A
SI-7 Software, Firmware, and Information Integrity	N/A
SI-8 Spam Protection	N/A

Requirement	Checks and Procedures
SI-10 Information Input Validation	For Web Application, Web Services, and Thick-client Application: Ensure that it is not possible to access pages or functions that require authentication without credentials. • Use SQL injection via a Web application proxy tool on the login screen to attempt authentication bypass • Using a Web application proxy tool, ensure that once a valid user has logged, in it is not possible to change parameters to reflect another user account. • Check to see if the admin role functionality is displayed in the URL and if so, can the URL be manipulated to gain admin privileges? • Check to see if “admin=true” in the URL query string or POST method gives additional access. For Web Applications and Thick-Client Applications: Ensure that the web application tests parameters for appropriate input validation and does not process scripts. Ensure that all user-generated input is encoded. Specifically test for: • SQL injection • Cross-Site Scripting (XSS) issues (both reflected and persistent) • Operating System (OS) command injection • Lightweight Directory Access Protocol (LDAP) injection • Object Relational Mapping (ORM) injection • Buffer Overflows • Malware payloads • Improper character sets Ensure that only certain types of files can be uploaded. Specifically check extensions such as .exe, .js, .cfm, .php, and .htm. For Web-Services: Ensure that the same checks hold as documented above, but additionally check for: Test Web service parameters for appropriate input validation, specifically test for: • XSS issues (if the Web service integrates with HTML pages) • XPATH injections • Simple Mail Transfer Protocol (SMTP) injections

Requirement	Checks and Procedures
SI-11 Error Handling	For Web Applications: Ensure that the application does not present application error messages to an attacker that could be used in an attack since verbose error message often provide additional information to an attacker. • Check the login page and make sure errors such as “user correct, password incorrect” or “user does not exist” do not appear (should be: either user or password is incorrect.) • Use a web application proxy to insert more characters than are specified in the HTML form field length in an attempt to produce verbose errors • Supply format type specifiers in an application input to crash the application input creating a core dump in the host folder Example: <code>http://hostname/html/en/index.htm%n%n%n</code> • Use vulnerable CGI scripts to print out stack trace data to a browser Example: <code>http://hostname/cgi-bin/query.cgi?name=john%x.%x.%x&code=123\$x.%x</code> Ensure that there is no sensitive data in the HTML that could lead an attacker to mount a focused attack. This typically occurs when developers leave information in HTML comments or the application renders names and addresses in HTML. For Web Services and Thick-client Application: Ensure that the Web service or thick-client application does not respond to unexpected inputs with verbose error messages.
SI-12 Information Handling and Retention	For Web Application and Thick-client Application: Ensure any application outputs such as printed or saved data is protected in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirement.
SI-13 Predictable Failure Prevention	N/A
SI-14 Non-Persistence	N/A
SI-15 Information Output Filtering	N/A
SI-16 Memory Protection	N/A
SI-17 Fail-Safe Procedures	N/A

3.18 Program Management (PM)

There are no application checks and procedures in this section.

4. References

1. FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.
2. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.
3. NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.
4. Open Web Application Security Project (OWASP), *OWASP Testing Guide*.
https://www.owasp.org/index.php/Main_Page

5. Acronyms

Acronym	Definition
AC	Access Control
ACL	Access Control List
ASP	Application Server Pages
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization (NIST 800-53 version 3)
CGI	Common Gateway Interface
CIA	Confidentiality, Integrity and Availability
CM	Configuration Management
COTS	Commercial Off The Shelf
CP	Contingency Planning
CSRF	Cross-Site Request Forgery
DES	Data Encryption Standard
DISA	Defense Information Systems Agency
DoS	Denial of Service
DMZ	De-Militarized Zone
DoD	Department of Defense
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTML	Hypertext Markup Language
HTTP	Hyper Text Transfer Protocol
IA	Identification and Authentication
ICMP	Internet Control Message Protocol
ID	Identifier
IIS	Internet Information Services
IP	Internet Protocol
IR	Incident Response
IS	Information Security
IT	Information Technology

Acronym	Definition
LDAP	Lightweight Directory Access Protocol
M&O	Management & Operations
MA	Maintenance
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Media Protection
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
PDF	Postscript Data Format
ORM	Object Relational Mapping
OWASP	Open Web Application Security Project
PE	Physical and Environmental Protection
PII	Personally Identifiable Information
PL	Planning
POC	Point of Contact
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SAML	Security Assertion Markup Language
SC	System and Communications Protection
SHA	Secure Hash Algorithm
SI	System and Information Integrity
SMTP	Simple Mail Transfer Protocol
SP	Special Publication
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SSP	System Security Plan
STIG	Security Technical Implementation Guide
SysAdmins	System Administrators

Acronym	Definition
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
WAS	Web Application Server
WS	Web Services
WSDL	Web Services Description Language
XML	eXtensible Markup Language
XSS	Cross-Site Scripting

Database Security Control Assessment Guide

The views, opinions and/or findings contained in this guide are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Approved for Public Release: 19-3536.
Distribution Unlimited.

©2019 The MITRE Corporation. All rights reserved.

Author(s): Nathan Adams
Harvey Rubinovitz

September 2015

Bedford, MA

MITRE

This page intentionally left blank.

Table of Contents

1.	Overview	1
1.1	Caveats	1
1.2	Assessment Methodology	2
1.2.1	Phase 1: Planning	2
1.2.2	Phase 2: Assessment	2
1.2.3	Phase 3: Reporting.....	2
2.	Assessment Activities	3
2.1	Phase 1: Planning.....	3
2.2	Phase 2: Assessment.....	3
2.2.1	Documentation Review.....	4
2.2.2	Database Assessment Script Output Review	4
2.2.3	Interviews	5
2.3	Phase 3: Reporting	5
3.	Assessing Security Controls	6
3.1.1	Access Control (AC)	6
3.1.2	Awareness and Training (AT)	9
3.1.3	Audit and Accountability (AU)	9
3.1.4	Security Assessment and Authorization (CA)	12
3.1.5	Configuration Management (CM)	12
3.1.6	Contingency Planning (CP)	15
3.1.7	Identification and Authentication (IA).....	16
3.1.8	Incident Response (IR).....	17
3.1.9	Maintenance (MA)	18
3.1.10	Media Protection (MP).....	18
3.1.11	Physical and Environmental Protection (PE).....	18
3.1.12	Planning (PL)	18
3.1.13	Personnel Security (PS)	18
3.1.14	Risk Assessment (RA).....	18
3.1.15	System and Services Acquisition (SA).....	18
3.1.16	System and Communications Protection (SC)	18
3.1.17	System and Information Integrity (SI).....	22
3.1.18	Program Management (PM).....	24
4.	References.....	25

5. Acronyms.....	26
------------------	----

List of Tables

Table 1. Access Control Configuration Compliance	6
Table 2. Audit and Accountability Configuration Compliance.....	10
Table 3. Configuration Management Database Configuration Compliance.....	12
Table 4. Contingency Planning Configuration Compliance.....	15
Table 5. Identification and Authentication Configuration Compliance	16
Table 6. System and Communications Protection Configuration Compliance.....	18
Table 7. System and Information Integrity Configuration Compliance	22

This page intentionally left blank.

1. Overview

This *Database Security Assessment Guide* is intended to serve as a practical guidance for information security (IS) engineers who conduct security control assessments for systems that must meet federal guidance. This guide focuses on testing and evaluation techniques for technical controls required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* as they relate to database installations. Parameters defined in this guide are considered industry best practice but may be modified by the organization as required.

The guide references the Security Technical Implementation Guides (STIG) and checklists developed by the Defense Information Systems Agency (DISA) for the Department of Defense (DoD). The combination of the DISA STIG and checklists will further be referred to as the DISA STIGs. The DISA STIGs provides descriptions and detailed tests for testing and validating security requirements. The STIG compliments organization documentation by providing guidance on identifying security vulnerabilities and verifying security configuration and parameter settings. Where there are no specific recommendations for a particular security requirement, the STIG recommendations will be used.

1.1 Caveats

The controls presented here are for a Federal Information Processing Standard (FIPS) 199 Moderate Impact rated system. Thus, controls for Low and High Impact rated systems may differ.

Some of the NIST SP 800-53 controls are not included: NIST SP 800-53 contains a broad set of required security standards; however, this guide only addresses those controls and sub-controls that are related to databases from the technical configuration perspective.

The Guide focuses on Oracle 11G: The guide assumes the database security assessors have an understanding of the Oracle Relational Database Management System (RDBMS), the supporting operating system environment, and database security concepts. In addition, database security evaluators may reference and make use of vendor, government, and industry best practices and recommendations. The concepts behind the requirements, checks and procedures in the guide are equally applicable to other database technologies.

ORACLE and OS Commands used: As a practical reference, this guide employs Structured Query Language (SQL) statements for operations within the database instance, and Operating System (OS) commands for operations at the OS level.

DISA STIG settings used: The database security assessment tests are derived from the Oracle Database STIGs. Where there are no specific recommendations for a particular parameter setting, the STIG recommendation will be used.

1.2 Assessment Methodology

The following sections define the three-phase assessment methodology on which this guide is based.

1.2.1 Phase 1: Planning

Phase 1 defines the assessment's scope, identifies goals, sets boundaries, and identifies assessment activities. This phase, as well as subsequent phases, requires the coordination of all involved parties. During this phase, the Evaluation Team reviews all security policies and procedures in accordance with the organization's security requirements. The team will then create assessment scenarios and premises and define assessment agreeable terms as approved by the organization.

1.2.2 Phase 2: Assessment

Phase 2 may have several steps depending on the assessment's objectives, scope, and goals as set forth in the Phase 1. These steps can be grouped by the nature of the activities involved. These activity groups are as follows:

- **Information Collection**—thorough research must be performed against the target system/application before any meaningful assessment can be conducted. Gathered data is analyzed as the assessment proceeds and when the assessment is complete. Prior to the assessment, pre-assessment planning requests for information/artifacts will need to be made in order to have an accurate understanding of the testing environment and to properly prepare for the assessment.
- **Enumeration**—activities that provide specific information about assessment targets. This information is often collected using appropriate software tools.
- **Testing and Review**—activities that typically involve both the automated testing of security vulnerabilities via software tools and the evaluation of particular aspects of the organization's security policies and practices by Assessment Team members.

1.2.3 Phase 3: Reporting

Phase 3 documents the soundness of the implemented security controls and consolidates all findings into the final output. This output includes reports that provide a summary of key findings and actionable recommendations, as well as provisions for all information derived from the assessment.

2. Assessment Activities

Assessment activities are grouped by the three phases—Planning, Assessment, and Reporting.

2.1 Phase 1: Planning

The Database Evaluator reviews the *Security Assessment Test Plan* to understand the scope of the assessment. Based on the scope, security policies and procedures in accordance with organization security requirements are reviewed. In preparation for the assessment phase, the Database Evaluator will review provided documentation and script output to increase familiarity with the target system and database. The Evaluator will determine any technical scripts, scans, or other requests to be made to ensure that the onsite assessment runs cleanly. During this time, any special requests for testing are provided to the Lead Evaluator for coordination with the system's Point of Contact (POC) and the organization facilitator. The Lead Evaluator will provide the system POC with the Oracle Database assessment script and execution instructions to be run in the target database environment.

To prepare for an assessment, the Database Evaluator reviews provided documentation. Available documentation may include the following:

- System Security Plan (SSP)
- Baseline configuration documents for each database
- Risk Assessment (RA)
 - Risk Acceptance Letters
- Policy Documents, such as listed below:
 - User Administration policy
 - Password change policy
 - Audit log retention and review policy
 - Backup procedures and policy
- Configuration Management (CM) policy document
 - Change Management policy document
- Database Environment Information
 - Assessment test script output
 - A copy of `Listener.ora`, `sqlnet.ora`, `tnsnames.ora` files
 - A copy of Directories/Files ownership and permissions

2.2 Phase 2: Assessment

The database assessment activities include documentation review, database assessment script output review, and personnel interviews. The database assessment script gathers information about the database installation that includes instance and configuration settings and parameters.

2.2.1 Documentation Review

The Database Evaluator will review documents provided by the organization. The review will assess whether the system documentation adequately describes implemented security controls and augments technical security control implementations. As a part of the assessment, the Database Evaluator will evaluate documentation such as, but not limited to, the System Security Plan (SSP), Risk Assessment (RA), and baseline configuration documents in accordance with organization guidelines and identify any discovered issues or concerns.

2.2.2 Database Assessment Script Output Review

The Database Evaluator must assess the organization's implementation of the database and database architecture to identify vulnerabilities. The database assessment script output includes information from the database that identifies potential security issues and concerns. The Evaluator must be familiar with the organization security guidance and the DISA STIG to effectively perform the security assessment.

In addition, the overall database environment must be evaluated. This evaluation is based upon sound database architecture principles. Issues to watch for include:

- Installation and Configuration
 - Installation and configuration security concerns involve installed database options, ownership, file layout, file/directory permissions, listener configurations, and parameter settings
- Database Account Management
 - Database account management concerns involve password management, account permissions, and database object ownership
- Database Access Configuration
 - Database access configuration security concerns involve default users and roles, public role assignment, auditing configuration, and privilege assignment
- System Availability/Maintenance
 - System availability/maintenance security concerns involve backup-recovery procedures, configuration management support, and support to development, test, and production application environments
- Auditing
 - Auditing security concerns involve configuring database auditing, implementing auditing procedures, following auditing guidelines and constraints

In order to properly evaluate the environment, the database evaluator needs to review copies of:

- `SQLNET.ora`
- `TNSNAMES.ora`
- `LISTENER.ora`

Files and directory permissions should be checked for the following:

- `$ORACLE_HOME/bin/` directory
- `$ORACLE_HOME/lib` directory
- Files in `$ORACLE_HOME/rdbms/log`
- `$ORACLE_HOME/rdbms` directory
- `$ORACLE_HOME/sqlplus` directory
- Files in `$ORACLE_HOME/network/trace` directory
- Files in `$ORACLE_HOME/rdbms/admin`
- Files in `$ORACLE_HOME/sqlplus/admin`
- `$ORACLE_HOME/network/admin` directory
- Spfile
- Control Filescygen
- Log files
- Data files

2.2.3 Interviews

The interview process supplements the information gathered from the database configuration data. It helps gather additional information and promotes interaction between the Evaluator and the system database administrator. Another primary area addressed during the interview process is the establishment and implementation of database related procedures such as backup and recovery, auditing, and user management. The interview process also serves as an opportunity for more in-depth analysis and exploration of the applicability of additional security controls. The interview questions serve as a starting point and are expected to lead to additional discussion. Depending on the environment, the questions asked may vary.

2.3 Phase 3: Reporting

The Database Evaluator must document all weaknesses following the organization reporting procedures and forward to the Lead Evaluator for consolidation and discussion during the out-briefs. The Database Evaluator should discuss any Moderate or High findings with support staff so that the out-brief is not the first time staff are exposed to the finding and the supporting evidence.

It is during this phase that the Database Evaluator also reviews any closure evidence if provided. While the finding is not removed from the report, the finding can be closed based on the Evaluator determining that the evidence provided is adequate to close the finding.

The reporting phase includes documentation of the soundness of the implemented security controls and the actual findings are consolidated into a final report.

3. Assessing Security Controls

Section 3 outlines a list of the security controls specified in NIST SP 800-53 and the corresponding checks and procedures used to verify database compliance during a security assessment. Several organization documents are used to identify database related security concerns, which are generally aligned with security controls. The DISA STIG documentation, along with other database security resources, provide specific and detailed guidance on testing and addressing specific database security issues. The example checks and procedures identified for each control in the following tables are drawn directly from the Oracle DISA STIG documentation. Checks and procedures entries of “N/A” indicate the security control does not have an applicable technical test to be conducted. Other members of the Evaluation Team may test these controls in other assessment areas.

3.1.1 Access Control (AC)

Table 1 lists the AC checks and procedures used to verify database configuration compliance.

Table 1. Access Control Configuration Compliance

Requirement	Checks and Procedures
AC-1 Access Control Policy and Procedures	DG0118: IAM (Information Assurance Manager) review of change in DBA assignments. Review the procedures and implementation evidence for monitoring changes to DBA role assignments and procedures for notifying the IAM of the changes for review. If procedures or implementation evidence does not exist, this is a Finding.
AC-2 Account Management	DG0070: DBMS user account authorization. Review procedures for ensuring authorization of new or re-assigned DBMS user accounts. Requests for user account access to the DBMS should include documented approval by an authorized requestor. Procedures should also include notification for a change in status, particularly cause for revocation of account access, to any DBMS accounts. Review the user accounts listed either in the script report or manually against the authorized user list. From SQL*Plus: <pre>select username from dba_users order by username;</pre> If procedures for DBMS user account authorization are incomplete or not implemented, this is a Finding. If any accounts listed are not clearly authorized, this is a Finding.

Requirement	Checks and Procedures
AC-3 Access Enforcement	DG0014: Default demonstration and sample database objects and applications should be removed. From SQL*Plus: <pre>select username from dba_users where username in ('SCOTT','HR','IX','OE','PM','SH','COMPANY', 'MFG','FINANCE','ANYDATA_USER','ANYDSET_USER', 'ANYTYPE_USER','AQJAVA','AQUSER','AQXMLUSER', 'GPFD','GPLD','MMO2','XMLGEN1','BLAKE','ADAMS', 'CLARK','JONES')or username like 'QS%'or username like 'USER%'or username like '%DEMO%'or username like 'SERVICECONSUMER%';</pre> If any usernames are listed, this is a Finding.
AC-4 Information Flow Enforcement	DG0152: DBMS network port, protocol and services (PPS) use. If Oracle Listener, JAVA Listener, Oracle Names or Connection Manager is not running on the local database host server, this check is NOT a Finding. Review the listener.ora file located by default in the ORACLE_HOME\network\admin directory or in the directory specified in the environment variable TNS_ADMIN defined for the listener process or service. View the "PORT=" parameter for any protocols defined. If any do not match an entry in the following list, then confirm that it is not a default or registered port for the service. View the cman.ora file in the ORACLE_HOME/network/admin directory. If the file does not exist, the database is not accessed via Oracle Connection Manager and this part of the check is NOT a Finding. View the "PORT=" parameter for any protocols defined. If any do not match an entry in the following list, then confirm that it is not a default or registered port for the service. If any non-default or non-registered ports are listed, this is a Finding. Default Oracle Listener Ports: 1521, 2483, 2484 Default Java Listener Ports: 2481, 2482 Default Oracle Names Listener Port: 1575 Default Connection Manager Ports: 1630, 1830 Registered ports MAY be listed at http://www.iana.org/assignments/port-numbers.
AC-5 Separation of Duties	DO0240: Oracle OS_ROLES parameter. From SQL*Plus: <pre>select value from v\$parameter where name='os_roles';</pre> If the value returned is not FALSE, this is a Finding.
AC-6 Least Privilege	DG0041: DBMS installation account use logging.

Requirement	Checks and Procedures
	Review documented and implemented procedures for monitoring the use of the DBMS software installation account in the System Security Plan. If use of this account is not monitored or procedures for monitoring its use do not exist or are incomplete, this is a Finding.
AC-7 Unsuccessful Login Attempts	DG0073: DBMS failed login account lock. From SQL*Plus: <pre>select profile ': ' limit from dba_profiles, (select limit as def_login_attempts from dba_profiles where profile = 'DEFAULT' and resource_name = 'FAILED_LOGIN_ATTEMPTS') where resource_name = 'FAILED_LOGIN_ATTEMPTS' and replace(limit, 'DEFAULT', def_login_attempts) IN ('UNLIMITED', NULL) or resource_name = 'FAILED_LOGIN_ATTEMPTS' and to_number(decode(limit, 'UNLIMITED', 10, 'DEFAULT', 10, limit)) > 3;</pre> If the DEFAULT profile is returned with a limit not less than or equal to 3, this is a Finding. If any non-DEFAULT profiles are returned with limits not documented and approved by the IAO, this is a Finding.
AC-8 System Use Notification	DG0179: DBMS warning banner. A warning banner displayed as a function of an Operating System or application login for applications that use the database makes this check NOT a Finding for all supported versions of Oracle.
AC-9 Previous Logon (Access) Notification	N/A
AC-10 Concurrent Session Control	N/A
AC-11 Session Lock	N/A
AC-12 Session Termination	DO0286: The Oracle INBOUND_CONNECT_TIMEOUT and SQLNET.INBOUND_CONNECT_TIMEOUT parameters should be set to a value greater than 0. Review the listener.ora file and the sqlnet.ora file. If the INBOUND_CONNECT_TIMEOUT_[listener-name] parameter does not exist for each listener found in the listener.ora and contain a value greater than 0, this is a Finding. If the SQLNET.INBOUND_CONNECT_TIMEOUT parameter does not exist in the sqlnet.ora and contain a value greater than 0, this is a Finding. NOTE: although the default value may provide adequate protection, assumes the default could lead to unanticipated changes in future product updates. Specify a value to manage the setting.

Requirement	Checks and Procedures
	NOTE: This control can also be met at the OS level.
AC-14 Permitted Actions without Identification or Authentication	N/A
AC-16 Security Attributes	DG0087: DBMS sensitive data labeling. If Oracle Label Security is not installed or database does not contain sensitive data, this check is NOT a Finding.
AC-17 Remote Access	DO6740: Oracle listener ADMIN_RESTRICTIONS parameter If a listener is not running on the local database host server, this check is NOT a Finding. Use the LSNRCTL utility and issue the STATUS [listener-name] command to locate the listener.ora file. Open the listener.ora file in a text editor or viewer. Locate the line with ADMIN_RESTRICTIONS_[listener-name] = ON where listener-name is the alias of the listener supplied by the DBA. If no such line is found, this is a Finding.
AC-18 Wireless Access	N/A
AC-19 Access Control for Mobile Devices	N/A
AC-20 Use of External Information Systems	N/A
AC-21 Information Sharing	N/A
AC-22 Publicly Accessible Content	N/A
AC-23 Data Mining Protection	N/A
AC-24 Access Control Decisions	N/A
AC-25 Reference Monitor	N/A

3.1.2 Awareness and Training (AT)

There are no database checks and procedures in this section.

3.1.3 Audit and Accountability (AU)

Table 2 lists the AU checks and procedures used to verify database configuration compliance.

Table 2. Audit and Accountability Configuration Compliance

Requirement	Checks and Procedures
AU-1 Audit and Accountability Policy and Procedures	N/A
AU-2 Auditable Events	DG0029: Database auditing. From SQL*Plus: <pre>select value from v\$parameter where name='audit_trail';</pre> If the value returned is NONE, this is a Finding.
AU-3 Content of Audit Records	DG0140: DBMS security data access. Determine the locations of DBMS audit, configuration, credential and other security data. Review audit settings for these files or data objects. If access to the security data is not audited, this is a Finding. If no access is audited, consider the operational impact and appropriateness for access that is not audited. If the risk for incomplete auditing of the security files is reasonable and documented in the System Security Plan, then do not include this as a Finding.
AU-4 Audit Storage Capacity	N/A
AU-5 Response to Audit Processing Failures	N/A
AU-6 Audit Review, Analysis, and Reporting	N/A
AU-7 Audit Reduction and Report Generation	DG0083: DBMS audit report automation. If the database being reviewed is not a production database, this check is NOT a Finding. Interview the database audit person or IAO to determine if an automated tool or procedure is used to report audit trail data. If an automated tool or procedure is not used, this is a Finding.
AU-8 Time Stamps	N/A
AU-9 Protection of Audit Information	DG0032: DBMS audit record access. From SQL*Plus: <pre>select value from v\$parameter where name='audit_trail';</pre> If none of the following values is displayed, this check is NOT a Finding. <pre>Oracle 11.1 - 11.2 = 'db' Oracle 11.1 - 11.2 = 'db_extended'</pre>

Requirement	Checks and Procedures
	Review access granted to the AUD\$ table. From SQL*Plus: <pre>select grantee from dba_tab_privs where table_name='AUD\$' and grantee not in ('DELETE_CATALOG_ROLE') and grantee not in (select grantee from dba_role_privs where granted_role='DBA') order by grantee;</pre> View access granted to the AUD\$ table against those authorized in the SSP. If any are not authorized, this is a Finding.
AU-10 Non-Repudiation	DG0025: DBMS encryption compliance. Review the DBMS documentation to determine where cryptography may be used and/or configured. If DBMS data/network encryption is not required, this check is NOT a Finding. For UNIX systems: <pre>\$ORACLE_HOME/OPatch/patch lsinventory -detail grep "Oracle Advanced Security"</pre> For Windows Systems: <pre>%ORACLE_HOME%/OPatch/patch lsinventory -detail find "Oracle Advanced Security"</pre> If DBMS data/network encryption is required and Oracle Advanced Security is not installed, this is a Finding. View the FIPS.ORA file found in the ORACLE_HOME/ldap/admin directory or the directory specified in the FIPS_HOME environment variable if set. If the file does not exist, it can be created. If SSLFIPS_140=TRUE is not set, this is a Finding. If SSL_CIPHER_SUITES is not defined, this is a Finding. If any cipher suite listed in SSL_CIPHER_SUITES value list is not included in the cipher suite list included below (and in this order), this is a Finding. FIPS 140-2 validated cipher suites for the Oracle SSL Libraries in the order of strongest to weakest: <pre>SSL_RSA_WITH_AES_256_CBC_SHA SSL_RSA_WITH_AES_128_CBC_SHA SSL_RSA_WITH_3DES_EDE_CBC_SHA SSL_RSA_WITH_RC4_128_SHA SSL_RSA_WITH_RC4_128_MD5 SSL_RSA_WITH_DES_CBC_SHA SSL_DH_anon_WITH_3DES_EDE_CBC_SHA SSL_DH_anon_WITH_RC4_128_MD5</pre>

Requirement	Checks and Procedures
	SSL_DH_anon_WITH_DES_CBC_SHA
AU-11 Audit Record Retention	DG0030: DBMS audit data maintenance. Review and verify the implementation of an audit trail retention policy. Verify that audit data is maintained for a minimum of one year. If audit data is not maintained for a minimum of one year, this is a Finding.
AU-12 Audit Generation	N/A
AU-13 Monitoring for Information Disclosure	N/A
AU-14 Session Audit	N/A
AU-15 Alternate Audit Capability	N/A
AU-16 Cross-Organizational Auditing	N/A

3.1.4 Security Assessment and Authorization (CA)

There are no database checks and procedures in this section.

3.1.5 Configuration Management (CM)

Table 3 lists the CM checks and procedures used to verify database configuration compliance.

Table 3. Configuration Management Database Configuration Compliance

Requirement	Checks and Procedures
CM-1 Configuration Management Policy and Procedure	DG0011: DBMS Configuration Management. If this is not a production system, this check is NOT a Finding. Review documentation and implementation evidence of CM procedures designed to prevent untested and uncontrolled software modifications to the production system. If none is defined and implemented, this is a Finding.
CM-2 Baseline Configuration	DG0021: DBMS software and configuration baseline. Review DBMS software baseline procedures and implementation evidence. Review the list of files, directories and details included in the current baseline for completeness. If DBMS software configuration baseline procedures do not exist, evidence of implementation does not exist, or baseline is not documented and current, this is a Finding.
CM-3 Configuration Change Control	N/A

Requirement	Checks and Procedures
CM-4 Security Impact Analysis	DG0010: DBMS software monitoring. Ask the DBA to describe/demonstrate any software modification detection procedures in place and request documents of these procedures for review. Verify by reviewing reports for inclusion of the DBMS executable and configuration files. If documented procedures and proof of implementation does not exist that includes review of the database software directories and database application directories, this is a Finding.
CM-5 Access Restrictions for Change	DG0017 : DBMS shared production/development use. If the DBMS host is not a shared production/development host, this check is NOT a Finding. Review all environment variables or other identifiers configured on the host system used by production DBAs, other users and developers to access the production and development DBMS. If the names or values of any identifiers do not clearly distinguish the development from the production applications, databases or database objects, this is a Finding. Check Windows service names and UNIX process names to review identifiers as well as environment variables used by DBAs and developers. Have the DBA display any other system level or local environment variables that reference the database installation directories or instances.
CM-6 Configuration Settings	DG0175: DBMS host and component STIG compliancy. If the DBMS host being reviewed is not a production DBMS host, this check is NOT a Finding. Review evidence of security hardening and auditing of the DBMS host platform with the IAO. If the DBMS host platform has not been hardened and received a security audit, this is a Finding. Review evidence of security hardening and auditing for all application(s) that store data in the database and all other separately configured components that access the database including web servers, application servers, report servers, etc. If any have not been hardened and received a security audit, this is a Finding. Review evidence of security hardening and auditing for all application(s) installed on the local DBMS host where security hardening and auditing guidance exists. If any have not been hardened and received a security audit, this is a Finding.
CM-7	N/A

Requirement	Checks and Procedures
Least Functionality	
CM-8 Information System Component Inventory	DG0019: DBMS software ownership. Ask the DBA/SysAdmin to demonstrate file and group ownership of the Oracle DBMS software and files and directories. On Windows systems: The Oracle DBMS software is usually installed using an account with administrator privileges. Ownership is assigned to the account used to install the DBMS software. The creation of a dedicated Oracle OS account and change of ownership of all files in the %ORACLE_HOME% and %ORACLE_BASE% directories and subdirectories should be performed prior to placing the DBMS system into production. On UNIX systems: <pre>find \$ORACLE_BASE /var/opt/oracle /etc/ora* \ /usr/local/bin/*ora* /usr/local/bin/db* ! -user oracle -o ! -group oinstall \ xargs ls -lR -d</pre> Where <code>oracle</code> is the Oracle owner account name and <code>oinstall</code> is the Oracle group owner account name. Review the resulting text file and note the owner/group ownership. If any files or directories belonging to the DBMS software are not owned by the designated Oracle OS owner and group accounts, this is a Finding. The owner and group ownership as well as file permissions for the following files (if present) should not be changed: <pre>extjob jssu nmb nmhs nmo oradism externaljob.ora coraenv dbhome oraenv</pre>
CM-9 Configuration Management Plan	N/A
CM-10 Software Usage Restrictions	
CM-11 User-Installed Software	

3.1.6 Contingency Planning (CP)

Table 4 lists the CP checks and procedures used to verify database configuration compliance.

Table 4. Contingency Planning Configuration Compliance

Requirement	Checks and Procedures
CP-1 Contingency Planning Policy and Procedure	DG0064: DBMS backup and restoration file protection. Review documented backup and restoration procedures to determine ownership and access during all phases of backup and recovery. Review file protections assigned to online backup and restoration files and tools. Review access, physical security protections and documented procedures for offline backup and restoration files and tools. If implementation evidence indicates that backup or restoration files are subject to corruption, unauthorized access or physical loss, this is a Finding.
CP-2 Contingency Plan	DG0020: DBMS backup and recovery testing. Review documented backup testing and recovery verification procedures noted or documented in the SSP. Review evidence of implementation of testing and verification procedures by reviewing logs from backup and recovery implementation. Logs may be in electronic or hardcopy and may include email or other notification. If backup testing and recovery verification are not documented or noted in the SSP, this is a Finding. If evidence of backup testing and recovery verification does not exist, this is a Finding.
CP-3 Contingency Training	N/A
CP-4 Contingency Plan Testing and Exercises	N/A
CP-6 Alternate Storage Site	N/A
CP-7 Alternate Processing Site	N/A
CP-8 Telecommunications Services	N/A
CP-9 Information System Backup	DG0013: Database backup procedures. Review the database backup procedures and implementation evidence. Evidence of implementation includes records of backup events and review of backup media. Evidence should match the backup plan as documented in the SSP.

Requirement	Checks and Procedures
	If backup procedures are not documented or are not implemented in accordance with the procedures, this is a Finding. If backups are not performed weekly or more often for Low impact systems, this is a Finding. If backups are not performed daily or more often for Medium impact systems, this is a Finding. If backup data for Medium impact systems is not secured and stored offline at an alternate site, this is a Finding. If backups for High impact systems do not include a redundant secondary system maintained at a separate physical site that can be activated without interruption or loss of data if the primary system fails, this is a Finding.
CP-10 Information System Recovery and Reconstitution	N/A
CP-11 Alternate Communications Protocols	N/A
C-12 Safe Mode	N/A
CP-13 Alternative Security Mechanisms	N/A

3.1.7 Identification and Authentication (IA)

Table 5 lists the IA checks and procedures used to verify database configuration compliance.

Table 5. Identification and Authentication Configuration Compliance

Requirement	Checks and Procedures
IA-1 Identification and Authentication Policy and Procedures	DG0066: DBMS temporary password procedures. If all database accounts are configured to authenticate using certificates or other credentials besides passwords, this check is NOT a Finding. Review documented procedures and evidence of implementation for assignment of temporary passwords for password-authenticated accounts. Review documented procedures for distribution of temporary passwords to users. Have the DBA demonstrate that the DBMS or applications accessing the database are configured to require a change of password by the user upon first use. If documented procedures and evidence do not exist or are not complete, or the DBMS or applications accessing the database are not configured to require a change of password by the user upon first use, this is a Finding.

Requirement	Checks and Procedures
IA-2 User Identification and Authentication (Organizational Users)	D03538: Oracle REMOTE_OS_AUTHENT parameter. From SQL*Plus: <pre>select value from v\$parameter where name='remote_os_authent';</pre> If the value returned does not equal FALSE, this is a Finding.
IA-3 Device Identification and Authentication	N/A
IA-4 Identifier Management	D03447: Oracle OS_AUTHENT_PREFIX parameter. From SQL*Plus: <pre>select value from v\$parameter where name='os_authent_prefix';</pre> If the value returned is OPS\$ or ops\$, this is a Finding.
IA-5 Authenticator Management	DG0068: DBMS application password display. Review policy and instructions included or noted in the SSP used to inform users and administrators not to enter database passwords at the command line. Review documented and implemented procedures used to monitor the DBMS system for such activity. If policy or instructions do not exist, proof of users and administrators being briefed does not exist or monitoring for compliance is not being performed to dissuade the practice of entering database passwords on the command line, this is a Finding.
IA-6 Authenticator Feedback	N/A
IA-7 Cryptographic Module Authentication	N/A
IA-8 Uniquely Identify and Authenticate (Non-Organizational Users)	N/A
IA-9 Service Identification and Authentication	N/A
IA-10 Adaptive Identification and Authentication	N/A
IA-11 Re-authentication	N/A

3.1.8 Incident Response (IR)

There are no database checks and procedures in this section.

3.1.9 Maintenance (MA)

There are no database checks and procedures in this section.

3.1.10 Media Protection (MP)

There are no database checks and procedures in this section.

3.1.11 Physical and Environmental Protection (PE)

There are no database checks and procedures in this section.

3.1.12 Planning (PL)

There are no database checks and procedures in this section.

3.1.13 Personnel Security (PS)

There are no database checks and procedures in this section.

3.1.14 Risk Assessment (RA)

There are no database checks and procedures in this section.

3.1.15 System and Services Acquisition (SA)

There are no database checks and procedures in this section.

3.1.16 System and Communications Protection (SC)

Error! Reference source not found. lists the SC checks and procedures used to verify database configuration compliance.

Table 6. System and Communications Protection Configuration Compliance

Requirement	Checks and Procedures
SC-1 System and Communications Protection Policy and Procedures	N/A
SC-2 Application Partitioning	DO0155: Oracle default tablespace assignment. From SQL*Plus: <pre>select username from dba_users where (default_tablespace= 'SYSTEM' or temporary_tablespace= 'SYSTEM') and username not in ('AURORA\$JIS\$UTILITY\$', 'AURORA\$ORB\$UNAUTHENTICATED', 'DBSNMP', 'MDSYS', 'ORDPL UGINS', 'ORDSYS', 'OSE\$HTTP\$ADMIN',</pre>

Requirement	Checks and Procedures
	'OUTLN', 'REPADMIN', 'SYS', 'SYSTEM', 'TRACESVR', 'MTSSYS', 'DIP'); If any non-default account records are returned, this is a Finding.
SC-3 Security Function Isolation	DG0110: DBMS host shared with a security service. Review the services and processes active on the DBMS host system. If the host system is a Windows server that also hosts other critical network services (e.g., domain controller), this is a Finding. If the host system is supporting any other security or directory services that do not use the DBMS to store information, this is a Finding.
SC-4 Information in Shared Resources	N/A
SC-5 Denial of Service Protection	N/A
SC-6 Resource Priority	N/A
SC-7 Boundary Protection	DG0186: DBMS network perimeter protection. Review the SSP to determine if the DBMS serves data to users or applications outside the local enclave. If the DBMS is not accessed outside of the local enclave, this check is NOT a Finding. If the DBMS serves applications available from a public network (e.g., the Internet), then confirm that the application servers are located in a DMZ or similar separate zone. If the DBMS is located inside the local enclave and is directly accessible to public users, this is a Finding. If the DBMS serves public-facing applications and is not protected from direct client connections and unauthorized networks, this is a Finding. If the DBMS serves public-facing applications and contains sensitive or classified information, this is a Finding.
SC-8 Transmission Confidentiality and Integrity	DG0093: Remote administrative connection encryption. Ask the DBA if the DBMS is accessed remotely for administration purposes. If it is not, this check is NOT a Finding. If it is, ask the DBA if the remote access to DBA accounts is made using remote access to the DBMS host or made directly to the database from a remote database client. If administration is performed using remote access to the DBMS host, review policy and procedures documented or noted in the SSP, along with evidence that remote administration of the DBMS is performed only via an encrypted connection protocol such as SSH or IPSec. If it is not, this is a Finding. If administration is performed from a remote database client, confirm that a dedicated database listener that encrypts communications exists for remote administrative communications. If a DBMS listener that encrypts traffic is not configured, this is a Finding.

Requirement	Checks and Procedures
	If any listeners on the DBMS host are configured to accept unencrypted traffic, review documented policy, procedures and evidence of training DBAs not to use the unencrypted listener for remote access to DBA accounts. If no such policy exists or the DBAs have not been instructed not to use the unencrypted connections, this is a Finding.
SC-10 Network Disconnect	N/A
SC-11 Trusted Path	N/A
SC-12 Cryptographic Key Establishment and Management	DG0166: Protection of DBMS asymmetric encryption keys. If no data is identified as being sensitive or classified by the Information Owner, in the SSP, this check is NOT a Finding. If no identified sensitive or classified data requires encryption by the Information Owner in the System Security Plan, this check is NOT a Finding. If the DBMS does not have Oracle Advanced Security installed, this check is NOT a Finding. For each asymmetric key identified as being used to encrypt sensitive data, verify the key owner is an application object owner or other non-DBA account. If the key owner listed is a DBA, this is a Finding. If any key owner is not the application object owner account or an account specific to the application as documented in the SSP, this is a Finding. If any asymmetric keys exist in the database whose private key is not encrypted, this is a Finding. Review the access permissions to asymmetric keys. Verify that any permission granted is authorized in the SSP for access to the key. Examine evidence that an audit record is created whenever the asymmetric key is accessed by other than authorized users. In particular, view evidence that access by a DBA or other system privileged account results in the generation of an audit record. This is required because system privileges that allow access to encryption keys may be used to access sensitive data where the privileged user does not have a job function need-to-know the data. If an audit record is not generated for unauthorized access to the asymmetric key, this is a Finding.
SC-13 Cryptographic Protection	N/A
SC-15 Collaborative Computing	N/A
SC-17 Public Key Infrastructure Certificates	N/A
SC-18 Mobile Code	N/A
SC-19	N/A

Requirement	Checks and Procedures
Voice Over Internet Protocol	
SC-20 Secure Name/Address Resolution Service (Authoritative Source)	N/A
SC-21 Secure Name/Address Resolution Service (Recursive and Caching Resolver)	N/A
SC-22 Architecture and Provisioning for Name/Address Resolution Service	N/A
SC-23 Session Authenticity	N/A
SC-24 Fail in Known State	N/A
SC-25 Thin Nodes	N/A
SC-26 Honeypots	N/A
SC-27 Platform Independent Applications	N/A
SC-28 Protection of Information at Rest	DG0090: DBMS sensitive data identification and encryption. If no data is identified as being sensitive or classified by the Information Owner, in the System Security Plan, this check is NOT a Finding. If no identified sensitive or classified data requires encryption by the Information Owner in the System Security Plan, this check is NOT a Finding. Review sensitive data stored in the database as identified in the SSP using <code>select</code> statements. Note in the SSP if the data is encrypted by column or by transparent encryption. Transparent data encryption is available only in Oracle versions 10.2 and later using Oracle Advanced Security. If transparent data encryption is specified, then verify it is enabled. By data columns: From SQL*Plus: <pre>select owner, table_name, column_name from dba_encrypted_columns;</pre> By tablespace: From SQL*Plus: <pre>select tablespace_name from dba_tablespaces where encrypted='YES';</pre>

Requirement	Checks and Procedures
	If columns within tables, tables and/or tablespaces listed in the SSP are required to be encrypted transparently are not listed above, this is a Finding. If the DBMS products are used to encrypt data, view the sensitive data fields required to be encrypted using <code>select</code> statements. If any data is displayed in human-readable format, this is a Finding.
SC-29 Heterogeneity	N/A
SC-30 Concealment and Misdirection	N/A
SC-31 Covert Channel Analysis	N/A
SC-32 Information System Partitioning	N/A
SC-34 Non-Modifiable Executable Programs	N/A
SC-35 Honeyclients	N/A
SC-36 Distributed Processing and Storage	N/A
SC-37 Out-of-Band Channels	N/A
SC-38 Operations Security	N/A
SC-39 Process Isolation	N/A
SC-40 Wireless Link Protection	N/A
SC-41 Port and I/O Device Access	N/A
SC-42 Sensor Capability and Data	N/A
SC-43 Usage Restrictions	N/A
SC-44 Detonation Chambers	N/A

3.1.17 System and Information Integrity (SI)

Table 7 lists the SI checks and procedures used to verify database configuration compliance.

Table 7. System and Information Integrity Configuration Compliance

Requirement	Checks and Procedures
SI-1 System and Information Integrity Policy and Procedures	N/A

Requirement	Checks and Procedures
SI-2 Flaw Remediation	DG0001: DBMS version support. From SQL*Plus: <pre>select banner from v\$version where banner like 'Oracle%';</pre> Verify the DBMS is one of the currently supported Oracle database versions. If the Oracle version is not currently supported or does not have extended support where specified, this is a Finding.
SI-3 Malicious Code Protection	DO6751: SQLNET.ALLOWED_LOGON_VERSION. View the <code>SQLNET.ORA</code> file in the <code>ORACLE_HOME/network/admin</code> directory or the directory specified in the <code>TNS_ADMIN</code> environment variable. Locate the following entry: <pre>SQLNET.ALLOWED_LOGON_VERSION = 10</pre> If the parameter does not exist nor is it set to a value of 10 or higher, this is a Finding.
SI-4 Information System Monitoring	N/A
SI-5 Security Alerts, Advisories and Directives	N/A
SI-6 Security Function Verification	N/A
SI-7 Software, Firmware, and Information Integrity	DG0050: DBMS software and configuration file monitoring. Review documented software and configuration monitoring procedures and implementation evidence to verify that monitoring of changes to database software libraries, related applications and configuration files is being performed weekly or more often. Verify that the list of files and directories being monitored is complete. If monitoring is not being performed weekly or more often, this is a Finding. If implementation evidence is not complete, this is a Finding.
SI-8 Spam Protection	N/A
SI-10 Information Input Validation	N/A
SI-11 Error Handling	N/A
SI-12 Information Handling and Retention	N/A
SI-13 Predictable Failure Prevention	N/A
SI-14 Non-Persistence	N/A

Requirement	Checks and Procedures
SI-15 Information Output Filtering	N/A
SI-16 Memory Protection	N/A
SI-17 Fail-Safe Procedures	N/A

3.1.18 Program Management (PM)

There are no application checks and procedures in this section.

4. References

1. Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*.
2. FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.
3. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.
4. NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.
5. National Security Agency (NSA) Guides to Secure Configuration.
6. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) *Oracle Database Security Check List*

5. Acronyms

Acronym	Definition
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CM	Configuration Management
CP	Contingency Planning
DBA	Database Administrator
DBMS	Database Management System
DISA	Defense Information Systems Agency
DMZ	De-Militarized Zone
DoD	Department of Defense
FIPS	Federal Information Processing Standards
IA	Identification and Authentication
IAO	Information Assurance Officer
IR	Incident Response
IS	Information Security
M&O	Management & Operations
MA	Maintenance
MP	Media Protection
N/A	Not Applicable
NIST	National Institute of Standards and Technology
PE	Physical and Environmental Protection
PL	Planning
POC	Point of Contact
PS	Personnel Security
RA	Risk Assessment
RDBMS	Relational Database Management System
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
SQL	Structured Query Language

Acronym	Definition
SSH	Secure Shell
SSP	System Security Plan
STIG	Security Technical Implementation Guide

Management and Operations Security Control Assessment Guide

The views, opinions and/or findings contained in this guide are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Approved for Public Release: 19-3536.
Distribution Unlimited.

©2019 The MITRE Corporation. All rights reserved.

Author(s): Nathan Adams
Jim Bielski
Carmella Thompson

September 2015

Baltimore, MD

MITRE

This page intentionally left blank.

Table of Contents

1. Overview.....	1
1.1 Caveats.....	1
1.2 Assessment Methodology	1
1.2.1 Phase 1: Planning.....	1
1.2.2 Phase 2: Assessment	1
1.2.3 Phase 3: Reporting.....	2
2. Management & Operational Assessment Activities	3
2.1 Planning Phase.....	3
2.2 Assessment Phase	3
2.2.1 Documentation Review	3
2.2.2 ATO Document Reviews.....	5
2.2.3 PIA REVIEW	5
2.2.4 Personnel Interviews.....	5
2.2.5 Facilities Tour.....	7
2.2.6 Overall Analysis of Implemented Processes	8
2.3 Reporting Phase	8
3. Detail Assessment Procedures	9
3.1 Access Control (AC).....	9
3.2 Awareness and Training (AT)	11
3.3 Audit and Accountability (AU)	12
3.4 Security Assessment and Authorization (CA).....	14
3.5 Configuration Management (CM)	15
3.6 Contingency Planning (CP)	17
3.7 Identification and Authentication (IA)	18
3.8 Incident Response (IR)	20
3.9 Maintenance (MA).....	21
3.10 Media Protection (MP)	22
3.11 Physical and Environmental Protection (PE)	22
3.12 Planning (PL).....	24
3.13 Personnel Security (PS)	25
3.14 Risk Assessment (RA).....	26
3.15 System and Services Acquisition (SA).....	26
3.16 System and Communications Protection (SC)	28
3.17 System and Information Integrity (SI).....	31

3.18	Program Management (PM)	32
4.	References.....	35
5.	List of Acronyms	36

List of Tables

Table 1.	Access Control Requirement Evaluation	9
Table 2.	Awareness and Training Requirement Evaluation	11
Table 3.	Audit and Accountability Requirement Evaluation.....	12
Table 4.	Security Assessment and Authorization Requirement Evaluation	14
Table 5.	Configuration Management Requirement Evaluation	15
Table 6.	Contingency Planning Requirement Evaluation.....	17
Table 7.	Identification and Authentication Requirement Evaluation	19
Table 8.	Incident Response Requirement Evaluation	20
Table 9.	Maintenance Requirement Evaluation.....	21
Table 10.	Media Protection Requirement Evaluation.....	22
Table 11.	Physical and Environmental Protection Requirement Evaluation.....	22
Table 12.	Planning Requirement Evaluation	24
Table 13.	Personnel Security Requirement Evaluation	25
Table 14.	Risk Assessment Requirement Evaluation	26
Table 15.	System and Services Acquisition Requirement Evaluation.....	26
Table 16.	System and Communications Protection Requirement Evaluation	28
Table 17.	System and Information Integrity Requirement Evaluation	31
Table 18.	Program Management Requirement Evaluation.....	32

This page intentionally left blank.

1. Overview

This *Management and Operational(M&O) Control Assessment Guide* is intended to serve as a practical guidance for information security (IS) engineers who conduct security control assessments for systems that must meet federal guidance. This guide focuses on testing and evaluation techniques for Management & Operations (M&O) controls required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*.

Parameters defined in this guide are considered industry best practice but may be modified by organizations as required. Management controls involve those safeguards and countermeasures that manage information and information system security and the associated risks to organization assets and operations. Operational controls support day-to-day procedures and mechanisms to protect organization information and information systems.

1.1 Caveats

The procedures must be updated as NIST 800-53 security controls and requirements are updated to reflect the most current security requirements. The controls to be evaluated will dictate the interview, observations, document evaluation, and examination process.

The controls presented here are for a Federal Information Processing Standard (FIPS) 199 Moderate Impact rated system. Thus, controls for Low and High Impact rated systems may differ.

1.2 Assessment Methodology

The following sections define the three-phase assessment methodology on which the guide is based.

1.2.1 Phase 1: Planning

The Planning Phase defines the assessment's scope, identifies goals, sets boundaries, and identifies assessment activities. This phase, as well as subsequent phases, requires the coordination of all involved parties. During this phase, the Assessment Team reviews all security policies and procedures in accordance with organization security requirements. The team will then create assessment scenarios and premises and define assessment agreeable terms as approved by the organization.

1.2.2 Phase 2: Assessment

The Assessment Phase, Phase 2, may have several steps depending on the assessment's objectives, scope, and goals as set forth in Planning Phase. These steps can be grouped by the nature of the activities involved. These activity groups are as follows:

- **Information Collection**—performs thorough research against the target system/application before any meaningful assessment can be conducted. Prior to the assessment, pre-assessment planning requests for information/artifacts are made in order to have an accurate understanding of the testing environment and to properly prepare for the assessment. Data gathered is analyzed as the assessment proceeds and when the assessment is complete.
- **Enumeration**—provides specific information about assessment targets. This information is often collected using appropriate software tools.
- **Testing and Review**—typically involves both the automated testing of security vulnerabilities via software tools and the evaluation of particular aspects of the organization's security policies and procedures by the Assessment Team.

1.2.3 Phase 3: Reporting

The Reporting Phase, Phase 3, documents the soundness of the implemented security controls and consolidates all findings into the final output. This output includes reports that provide a summary of key findings and actionable recommendations, as well as provisions for all information derived from the assessment.

2. Management & Operational Assessment Activities

Section 2 provides an overview of the M&O Evaluator's responsibilities. The M&O Evaluator is responsible for conducting the management and operational control portion of the security control assessment.

2.1 Planning Phase

The M&O Evaluator reviews the Security Control Assessment Test Plan to understand the assessment's scope. Based on the scope, the organization security policies, requirements and procedures are reviewed to ensure an understanding of those that are applicable to this assessment. As system documentation is received, the M&O Evaluator reviews the documentation to ensure they have full knowledge of the system to be assessed and the assessment scope. The M&O Evaluator also determines any additional requests to ensure that the onsite assessment runs smoothly. During this time, any special testing requests are provided to the Lead Evaluator so they can contact the system's point of contact (POC) and the organization facilitator to ensure all requirements for the assessment are complete. The M&O Evaluator will review the interview templates and modify their evaluation procedures as needed.

2.2 Assessment Phase

The M&O assessment activities consists of documentation review, security document evaluations, personnel interviews, facilities tour (if in scope) and overall analysis of implemented processes. The activities and the detailed supporting processes and procedures must be at an adequate level to determine compliance with controls at each system impact level: Low, Moderate, and High.

2.2.1 Documentation Review

The documentation review determines if the technical aspects of policies, standards, procedures, security plans, contingency plans, and risk assessments are current and comprehensive. This is an ongoing process and occurs during all security control assessment phases. All requested documents are reviewed by the M&O Evaluator prior to the interviews to have a good understanding of the M&O processes and procedures in place. The requested documents and the receipt status are noted in the Security Control Assessment Test Plan. The documents to be reviewed could include:

- Administrator/Operator manuals, user manuals, or training materials
- Application and Business Description—includes underlying technology if not documented in the System Design Document (SDD), Version Description Document (VDD), or System Security Plan (SSP)
- Application or system backup, storage requirements, and procedures

- Audit process documentation
- Baseline Security Configurations—including for each platform and the application within scope and baseline network configurations
- Configuration and change management process—including examples of Change Requests (CR)
- Contingency Plan (CP)—includes evidence of any exercises
- Data retention and media handling/sanitization procedures
- Detailed system/network architecture diagrams
- Host and Network Intrusion Detection/Prevention procedures
- Identification and Authentication (IA) controls—including any discretionary access control for roles and privileges if not documented in the SDD, VDD, or SSP
- Incident Response (IR) procedures—including evidence of simulations or actual execution of IR procedures
- Information System Risk Assessment (ISRA)
- Interconnection agreements/memorandum of agreements/memorandum of understandings (MOA/MOU)
- Open corrective action plans (CAP)—includes items from previous security assessments
- Operations & Maintenance (O&M) manual
- Privacy Impact Assessment (PIA)
- Rules of Behavior (RoB)—includes corresponding evidence of user acceptance and acknowledgment
- Security Awareness and Training (AT) material—including evidence of staff who have completed training
- Security management processes
- System Design Document (SDD)
- System inventory for hardware and software
- System Security Plan (SSP)
- Uniformed Resource Locators (URL) for all Web application interfaces within the assessment's scope not documented in the SDD, VDD, or SSP
- Version Description Document (VDD)
- Vulnerability and security patch management processes

2.2.2 ATO Document Reviews

While the M&O Evaluator needs to review much of the documentation received, the M&O Evaluator performs a detailed evaluation of the documents that are key to the system receiving an Authority to Operate (ATO)—the SSP, the ISRA, and the CP. The documentation evaluation performed by the M&O Evaluator should ensure that security documentation is accurate and complete, as well as compliant with all organization policies, procedures, and guidance. The implementation of all management, operational, and technical security controls (whether planned or in place) should be described in accordance with organization requirements.

During the SSP evaluation, the M&O Evaluator reviews the requirements noted in the most current version of NIST 800-53 to ensure that all control implementation requirements are addressed in the SSP. The completed evaluations are shared with the Business Owner and the Information System Security Officer (ISSO) during a session dedicated to documentation discussion—the evaluations should not be discussed during their interviews. To expedite the discussion, the evaluations can be provided to the Business Owner and the ISSO prior to the review meeting.

If organization guidance is not followed or if any required controls are not completely addressed, only one issue per document is noted in the finding as incomplete or inadequate SSP, ISRA, or CP. These findings are generally considered Low/Moderate findings and should reference the detailed evaluation provided in the recommended corrective action. These documentation findings are just that, “documentation findings,” as there still may be additional findings associated with the control implementation that will be found during the assessment.

2.2.3 Privacy Impact Assessment Review

Another key document to be reviewed is the Privacy Impact Assessment (PIA). Although no detailed evaluation is performed on the PIA, the M&O Evaluator should ensure that a PIA was performed as required by organization policy.

2.2.4 Personnel Interviews

Documenting security controls does not ensure that the control is properly implemented. The M&O Evaluator, as well as the technical evaluators, must still ensure that the controls, as documented, are adequate and properly implemented. The M&O Evaluator and the technical evaluators use the interview process to ensure the controls are implemented as stated, that the documentation is understood and followed, and that updates and changes are properly distributed to all support staff as needed.

Key information to confirm security controls are properly implemented is gained through personnel interviews. The M&O Evaluator and technical evaluators interview the designated subject matter experts (SME) identified in the Security Control Assessment Test Plan. These SMEs have specific knowledge of overall system security requirements as well as a detailed understanding of the information system’s operational functions. Staff with

responsibilities associated with a role listed below may be interviewed by the M&O Evaluator depending on the assessment's scope:

- Business Owner
- Application Developer
- Configuration Manager
- Contingency Planning Manager
- Database Administrator (DBA)
- Data Center Manager
- Facilities Manager
- Firewall Administrator
- Human Resources (HR) Manager
- Information System Security Officer (ISSO)
- Media Custodian
- Network Administrator
- Program Manager
- Security Utilities Administrator
- System Administrator (SysAdmin)
- System Owner
- Training Manager

The interviews are based on individual roles and responsibilities, the organizational structure of the data center/facility hosting the system, and/or the security assessment's scope. Although the initial identification of interviewees is determined during the Assessment Planning Phase, as the interview process is conducted additional interviewees may be identified. The M&O Evaluator is involved in interviews of technical support staff to ensure that M&O controls are followed as stated.

Interview templates address all control families based on specific functions or roles. Some role based interview templates (e.g., ISSO, Business Owner) address multiple control families. If personnel support multiple functions (e.g., configuration management and contingency planning), several interview templates may be used during an interview session or the questions may need to be adjusted to avoid asking an individual the same question twice. The interview template questions focus not only on areas for which the interviewee may be directly responsible, but also include questions to validate that documented policies and procedures are understood, followed by support staff, and documented controls are implemented consistently across the organization. Although a policy or procedure may exist that implies a control is properly implemented, interviews with staff using the policy or procedures may reveal they are either not being consistently used or are being bypassed completely. An example of this would be if staff have no knowledge of the procedure, it would be a finding.

Suggested interview templates are as follows:

- Application Developer Interview Template

- Awareness Training (AT) Interview Template
- Business Owner Interview Template
- Configuration Management (CM) Interview Template
- Contingency Planning (CP) Interview Template
- Database Administrator(DBA) Interview Template
- Human Resource/Personal Security (HR/PS) Interview Template
- Information System Security Officer/Security Officer (ISSO/SO) Interview Template
- Incident Response (IR) Interview Template
- Physical and Environmental (PE), Maintenance(MA), Media Protection (MP) Interview Template
- System Administration (SysAdmin) Interview Template

Interview templates provide a series of questions that are used by the M&O Evaluator to ensure the control is implemented correctly. The questions are based on the organization test objectives. During the background overview or in response to other questions, the interviewee may partially or completely cover the response to another question in the questionnaire. In that case, some questions may not be asked again; however, the M&O Evaluator should ensure that the control was adequately addressed earlier. If necessary, the Evaluator could state “Although the implementation of this control may have been covered partially during an earlier response, I would like to go over the implementation of the control again.” Additionally, some questions may not need to be asked based on the response to prior questions. Not all questions in the interview template need to be asked; they are there for reference to guide interview discussions. The Evaluator is responsible for ensuring that all controls are covered, thus it is important to at least review each set of questions to ensure that the responses to the control implementation are adequately addressed.

Based on answers to the questions, additional information or artifacts should be requested to support the response. For example, if the SSP states that CM procedures are in place, the Evaluator should request copies of these procedures and review them to ensure they satisfy organization requirements. It is important that the document request be made to thoroughly test a process (i.e., a specific Change Request (CR) and corresponding audit reports or logs that reflect the change).

The interview templates can also be used to capture responses. A simple way to capture these responses is to record the responses electronically with track changes on to highlight the responses.

2.2.5 Facilities Tour

If the scope of the assessment includes the Physical and Environmental Protection Controls, a physical tour of the facility is conducted. The assessment of these controls is also based on observations that may begin as the M&O Evaluator enters the building that houses the data center. The facility assessment includes the data center, any supporting areas such as the areas housing telecommunications equipment, the support staff work

environment, the exterior of the building, physical access control systems, internal and external monitoring equipment and supporting systems, and power and backup power equipment. During the tour, assessment of the Maintenance Controls and the Media Protection Controls are also completed.

Technical Evaluators may accompany the M&O Evaluator, to gain an understanding of the components that are being assessed.

Based on the procedures noted during the tour, the M&O Evaluator requests and reviews any additional supporting documentation.

2.2.6 Overall Analysis of Implemented Processes

The M&O Evaluator should be in continuous communication with other Evaluation Team members, including the Network, Database, Operating System, and Application Evaluators. The M&O Evaluator should review the overall findings of technical evaluators to determine if any technical findings or group of findings indicate a greater management or operational control weakness. These weaknesses could indicate a failure of a documented procedures or adherence to the procedure. An example might be an inconsistency in 'like' component baselines or patch levels, the documented procedure and the response to the interviews indicate that there are strong procedures in place. However, the results of the technical assesment indicate that the procedures may not be followed or there are problems with the documented procedures; therefore, there may still be an M&O finding.

2.3 Reporting Phase

The M&O Evaluator must document all weaknesses following organization reporting procedures and forward them to the Lead Evaluator for consolidation and discussion during the out-briefs. The M&O Evaluator should discuss any Moderate or High findings with support staff, so the out-brief is not the first time staff are exposed to the finding and supporting evidence.

During the Reporting Phase, the M&O Evaluator reviews any closure evidence, if provided. While the finding is not removed from the report, the finding can be closed based on the Evaluator determining the evidence is adequate to close the finding.

The Reporting Phase includes documentation of the implemented security controls' soundness. The actual findings are consolidated into a final report.

3. Detail Assessment Procedures

Section 3 provides checks and procedures that the M&O Evaluator uses to evaluate each security control. It can be used as a guide to ensure that each control is adequately evaluated based on the procedures being followed. It is not used during the onsite, but rather for planning based on the scope of the assessment. Interview templates used during the onsite assessment that address each control are referenced in the control's checks and procedures. When organization or NIST guidance is modified, the checks and procedures must be reviewed, as well as, the interview templates used during the onsite.

In order to evaluate the Management and Operational security controls, it is important that the NIST SP 800-53 controls associated with the system's security level and the SSP be reviewed for key information on each control's implementation. For each control, the review of these documents is not listed, although it is critical to ensure the proper implementation of the control. The interview questions and associated documents to be requested to assess the control are documented in the referenced interview templates.

3.1 Access Control (AC)

Table 1 lists AC checks and procedures.

Table 1. Access Control Requirement Evaluation

Requirement	Checks and Procedures
AC-1 Access Control Policy and Procedures	1. Examine policies and/or procedures. 2. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template)
AC-2 Account Management	1. Review any documented account management procedures. 2. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template) 3. Participate in all administrators technical interviews to confirm account management 4. Examine documentation directly associated with the account management process based on interview results based on interview results
AC-3 Access Enforcement	1. Review any documented account management procedures 2. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) 3. Examine documentation directly associated with the account management process based on interview results based on interview results
AC-4	1. Confirmed thought technical testing

Requirement	Checks and Procedures
Information Flow Enforcement	- Participate in all administrators technical interviews. Reference the following interview template: - SysAdmins (SysAdmin Interview Template)
AC-5 Separation of Duties	- Review access control policies and procedures. - Interview the following: - ISSO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) - SysAdmins (SysAdmin Interview Template) - Application Developer (Application Developer Interview Template) - Examine documentation directly associated with the account management process based on interview results based on interview results.
AC-6 Least Privilege	- Review account policy and procedures. - Review list of privileged system accounts. - Interview the following to determine roles and responsibilities: - Business Owner (Business Owner Interview Template) - ISSO (ISSO/SO Interview Template) - Participate in all administrators technical interviews. Reference the following Interview Template: - SysAdmins (SysAdmin Interview Template)
AC-7 Unsuccessful Login Attempts	Technical test.
AC-8 System Use Notification	Technical test.
AC-9 Previous Logon (Access) Notification	Technical test.
AC-10 Concurrent Session Control	- Technical test. - Interview the following to confirm the need for concurrent sessions: - ISSO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template)
AC-11 Session Lock	Technical test.
AC-12 Session Termination	Technical test.
AC-14 Permitted Actions without Identification or Authentication	- Review access control policies and procedures. - Interview the following: - ISSO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) - SysAdmins (SysAdmin Interview Template)
AC-16 Security Attributes	N/A
AC-17 Remote Access	- Review procedures addressing remote access. - Obtain list of remote access accounts. - Interview the following: - SysAdmins (SysAdmin Interview Template) - ISSO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) - Application Developer (Application Developer Interview Template).
AC-18	Review any procedures addressing wireless implementation and use.

Requirement	Checks and Procedures
Wireless Access	2. Interview specific personnel responsible for authorizing, monitoring, or controlling the use of wireless technologies: • SysAdmins (SysAdmin Interview Template)
AC-19 Access Control for Mobile Devices	1. Review any procedures addressing access control for portable and mobile devices. 2. Interview specific personnel responsible for the use of portable and mobile devices to access the information system: • ISSO (ISSO/SO Interview Template) • SysAdmins (SysAdmin Interview Template)
AC-20 Use of External Information Systems	1. Review any procedures addressing the use of external information systems. 2. Interview personnel responsible for the use of monitoring, controlling, or using organization-controlled portable storage media: • ISSO (ISSO/SO Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template).
AC-21 Information Sharing	1. Review any procedures addressing information sharing. 2. Interview personnel responsible for the information sharing: • ISSO (ISSO/SO Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template).
AC-22 Publicly Accessible Content	1. Review procedures addressing public websites and publicly accessible content. 2. Determine if the application is accessible from external information systems. 3. Interview the following: • SysAdmins (SysAdmin Interview Template) • ISSO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template)
AC-23 Data Mining Protection	N/A
AC-24 Access Control Decisions	N/A
AC-25 Reference Monitor	N/A

3.2 Awareness and Training (AT)

Table 2 lists AT checks and procedures.

Table 2. Awareness and Training Requirement Evaluation

Requirement	Checks and Procedures
AT-1 Security Awareness and Training Policy and Procedures	1. Examine policies and/or procedures. 2. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template)
AT-2 Security Awareness	1. Interview the following to determine if security awareness training is provided to users:

	• Business Owner (Business Owner Interview Template and AT Interview Template) • ISSO (ISSO/SO Interview Template and AT Interview Template) • HR/PS (AT Interview Template) • Application Developer (Application Developer Interview Template) • SysAdmins (SysAdmin Interview Template).
AT-3 Security Training	1. Interview the following to determine if role-based training is provided to specific users: • Business Owner (Business Owner Interview Template) • ISSO (ISSO/SO Interview Template) • HR/PS (AT Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template). 2. Examine the training documents or relevant training language
AT-4 Security Training Records	1. Request records. 2. Interview the following to determine if security training records are maintained: • ISSO (ISSO/SO Interview Template and AT Interview Template) • HR/PS (AT Interview Template)
AT-5 Contacts with Security Groups and Associations	3. Interview the following to determine if security training records are maintained: • ISSO (ISSO/SO Interview Template and AT Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template).

3.3 Audit and Accountability (AU)

Table 3 lists AU checks and procedures.

Table 3. Audit and Accountability Requirement Evaluation

Requirement	Checks and Procedures
AU-1 Audit and Accountability Policy and Procedures	1. Review any documented audit and accountability policy and/or procedure. 2. Interview the following using the associated Interview Template questions: • ISSO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) • Application Developer (Application Developer Interview Template) 3. Examine documentation directly associated with the account management process based on interview results based on interview results.
AU-2 Auditable Events	1. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template)

Requirement	Checks and Procedures
	2. Examine documentation directly associated with the audit process based on interview results.
AU-3 Content of Audit Records	1. Technical Test. 2. Review any documentation related to audit records for audit events identified. 3. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template).
AU-4 Audit Storage Capacity	1. Technical Test. 2. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template).
AU-5 Response to Audit Processing Failures	1. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template).
AU-6 Audit Review, Analysis, and Reporting	1. Review any documentation on audit review and follow-up processes and procedures. 2. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template) 3. Examine documentation directly associated with the Audit review, analysis and reporting based on interview results based on interview results.
AU-7 Audit Reduction and Report Generation	1. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template) 2. Examine documentation directly associated with the Audit Reduction and report generation capabilities to determine of real-time audit review, analysis and reporting supports after the fact investigations of security incidents.
AU-8 Time Stamps	1. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template).

Requirement	Checks and Procedures
AU-9 Protection of Audit Information	1. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template).
AU-10 Non-Repudiation	1. Interview the following using the associated interview template: • ISSO (ISSO/SO Interview Template) • SysAdmins (SysAdmin Interview Template)
AU-11 Audit Record Retention	1. Interview the following using the associated interview template: • ISSO (ISSO/SO Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template).
AU-12 Audit Generation	1. Interview the following using the associated interview template: • ISSO (ISSO/SO Interview Template) • SysAdmins (SysAdmin Interview Template).
AU-13 Monitoring for Information Disclosure	N/A
AU-14 Session Audit	N/A
AU-15 Alternate Audit Capability	N/A
AU-16 Cross-Organizational Auditing	N/A

3.4 Security Assessment and Authorization (CA)

Table 4 lists CA checks and procedures.

Table 4. Security Assessment and Authorization Requirement Evaluation

Requirement	Checks and Procedures
CA-1 Security Assessment and Authorization Policies and Procedures	1. Examine security assessment and authorization policies and procedures. 2. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template)
CA-2 Security Assessments	1. Examine security assessment and authorization policies and procedures. 2. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) 3. Review results of any assessment reports/plans or POA&Ms.
CA-3 Information System Connections	1. Examine documentation related to information system connection agreements. 1. Interview the following personnel to discuss any interconnection requirements:

Requirement	Checks and Procedures
	• ISSO • Business Owner
CA-5 Plan of Action and Milestones (POA&M)	1. Review any outstanding POA&Ms. 2. Discuss strategy/method for updating POA&Ms. 3. Review assessment plan/reports for outstanding findings. 4. Interview the following personnel to discuss POA&M requirements: • ISSO (ISSO/SO Interview Template): • Business Owner (Business Owner Interview Template)
CA-6 Security Authorization	1. Interview the following personnel: • ISSO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) 2. Review the SSP to determine recent security authorization.
CA-7 Continuous Monitoring	1. Interview personnel using the following: • ISSO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) • SysAdmins (SysAdmin Interview Template)
CA-8 Penetration Testing	N/A
CA-9 Internal System Connections	1. Technical Test

3.5 Configuration Management (CM)

Table 5 lists CA checks and procedures.

Table 5. Configuration Management Requirement Evaluation

Requirement	Checks and Procedures
CM-1 Configuration Management Policy and Procedure	1. Examine policies and/or procedures. 2. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template and CM Interview Template) • Business Owner (Business Owner Interview Template)
CM-2 Baseline Configuration	1. Interview the following using the associated interview template questions: • ISSO/SO (CM Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template) 2. Interview other relevant SMEs based on results of the interviews.
CM-3 Configuration Change Control	1. Interview the following using the associated interview template questions: • Business Owner (Business Owner Interview Template and CM Interview Template) • ISSO/SO (ISSO/SO Interview Template and CM Interview Template) • CM (CM Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template) 2. Interview other relevant SMEs based on results of the interviews.

Requirement	Checks and Procedures
CM-4 Security Impact Analysis	- Interview the following using the associated interview template questions: - Business Owner (Business Owner Interview Template and CM Interview Template) - ISSO/SO (ISSO/SO Interview Template and CM Interview Template) - CM (CM Interview Template) - SysAdmins (SysAdmin Interview Template) - Review CM process to determine if security impact analysis is performed.
CM-5 Access Restrictions for Change	- Interview the following using the associated interview template questions: - Business Owner (Business Owner Interview Template and CM Interview Template) - ISSO/SO (ISSO/SO Interview Template and CM Interview Template) - Interview other relevant SMEs based on results of the interviews.
CM-6 Configuration Settings	- Coordinate with the application/infrastructure specific tester. - Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template and CM Interview Template) - SysAdmins (SysAdmin Interview Template) - Interview other relevant SMEs based on results of the interviews.
CM-7 Least Functionality	- Coordinate with the application/infrastructure specific tester. - Interview the following using the associated interview template questions: - Business Owner (Business Owner Interview Template and CM Interview Template) - ISSO/SO (ISSO/SO Interview Template and CM Interview Template) - SysAdmins (SysAdmin Interview Template) - Interview other relevant SMEs based on results of the interviews.
CM-8 Information System Component Inventory	- Coordinate with the application/infrastructure specific tester. - Interview the following using the associated interview template questions: - Business Owner (Business Owner and CM Interview Templates) - ISSO/SO (ISSO/SO Interview Template and CM Interview Template) - CM (CM Interview Template) - SysAdmins (SysAdmin Interview Template) - Application Developer (Application Developer Interview Template). - Interview other relevant SMEs based on results of the interviews.
CM-9 Configuration Management Plan	- Review the Configuration Management Plan. - Interview the following using the associated interview template questions: - Business Owner (Business Owner Interview Template and CM Interview Template) - ISSO/SO (ISSO/SO Interview Template and CM Interview Template) - CM (CM Interview Template)

Requirement	Checks and Procedures
	• SysAdmins (SysAdmin Interview Template) 3. Interview other relevant SMEs based on results of the interviews.
CM-10 Software Usage Restrictions	1. Examine policies for software usage restrictions.
CM-11 User-Installed Software	1. Examine policies for user-installed software.

3.6 Contingency Planning (CP)

Table 6 lists CP checks and procedures.

Table 6. Contingency Planning Requirement Evaluation

Requirement	Checks and Procedures
CP-1 Contingency Planning Policy and Procedure	1. Examine policies and/or procedures. 2. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template)
CP-2 Contingency Plan	1. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template and CP Interview Template) • Business Owner (Business Owner Interview Template and CP Interview Template) • CP (CP Interview Template) • Key Personnel with CP responsibilities (CP Interview Template) • Application Developer (Application Developer Interview Template) 2. Examine contingency plan and ensure it meets requirements of AGENCY.
CP-3 Contingency Training	1. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template and CP Interview Template) • Business Owner (Business Owner Interview Template and CP Interview Template) • CP (CP Interview Template) • Application Developer (Application Developer Interview Template) • Key Personnel with CP responsibilities (CP Interview Template) 2. Examine the Training Plan or relevant information within the CP
CP-4 Contingency Plan Testing and Exercises	1. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template and CP Interview Template) • Business Owner (Business Owner Interview Template and CP Interview Template) • CP (CP Interview Template) • Application Developer (Application Developer Interview Template) • Key Personnel with CP responsibilities (CP Interview Template) 2. Examine results of tabletop exercises and ensure AGENCY template is used; ensure it meets requirements of AGENCY.

Requirement	Checks and Procedures
CP-6 Alternate Storage Site	1. Examine CP policies and procedures related to alternate storage facilities. 2. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template and CP Interview Template) • Business Owner (Business Owner Interview Template and CP Interview Template) • CP (CP Interview Template) 3. Review the CP plan for alternate storage site requirements.
CP-7 Alternate Processing Site	1. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template and CP Interview Template) • Business Owner (Business Owner Interview Template and CP Interview Template) • CP (CP Interview Template) 2. Examine the contingency plan for alternate processing site requirements.
CP-8 Telecommunications Services	1. Interview the telecommunications POC to determine if alternate telecommunications services including agreements are in place: • CP (CP Interview Template) 2. Determine if telecommunication requirements are part of the Contingency Plan
CP-9 Information System Backup	1. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template and CP Interview Template) • Business Owner (Business Owner Interview Template and CP Interview Template) 2. Examine the SSP and the Contingency Plan to determine in place backup requirements.
CP-10 Information System Recovery and Reconstitution	1. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template and CP Interview Template) • Business Owner (Business Owner Interview Template and CP Interview Template) 2. Examine the SSP and the Contingency Plan to determine system recovery and reconstitution requirements.
CP-11 Alternate Communications Protocols	N/A
CP-12 Safe Mode	N/A
CP-13 Alternative Security Mechanisms	N/A

3.7 Identification and Authentication (IA)

Table 7 lists IA checks and procedures.

Table 7. Identification and Authentication Requirement Evaluation

Requirement	Checks and Procedures
IA-1 Identification and Authentication Policy and Procedures	1. Review any documented Identification and Authentication Policy and Procedures. 2. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) 3. Examine documentation based on interview results based on interview results.
IA-2 User Identification and Authentication (Organizational Users)	1. Review any documented Identification and Authentication Policy and Procedures. 2. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) • SysAdmins (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template) 3. Examine documentation based on interview results based on interview results.
IA-3 Device Identification and Authentication	1. Review any documented Identification and Authentication Policy and Procedures. 2. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • SysAdmin (SysAdmin Interview Template) 3. Examine documentation based on interview results based on interview results.
IA-4 Identifier Management	1. Review any documented Identification and Authentication Policy and Procedures. 2. Interview the following using the associated interview template questions: • SysAdmin (SysAdmin Interview Template) 3. Examine documentation based on interview results based on interview results.
IA-5 Authenticator Management	1. Review any documented Identification and Authentication Policy and Procedures. 2. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • SysAdmin (SysAdmin Interview Template) 3. Examine documentation based on interview results.
IA-6 Authenticator Feedback	1. Technical Test
IA-7 Cryptographic Module Authentication	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
IA-8 Uniquely Identify and Authenticate (Non-Organizational Users)	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
IA-9 Service Identification and Authentication	N/A
IA-10 Adaptive Identification and Authentication	N/A

Requirement	Checks and Procedures
IA-11 Re-authentication	N/A

3.8 Incident Response (IR)

Table 8 lists IR checks and procedures.

Table 8. Incident Response Requirement Evaluation

Requirement	Checks and Procedures
IR-1 Incident Response Policy and Procedures	1. Review any documented Incident Response Policy and procedures. 2. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Incident Response (IR Interview Template) • SysAdmin (SysAdmin Interview Template) 3. Examine documentation based on interview results.
IR-2 Incident Response Training	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Incident Response (IR Interview Template) • SysAdmin (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template). 2. Examine training information and other relevant documentation based on interview results.
IR-3 Incident Response Testing	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Incident Response (IR Interview Template) • SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
IR-4 Incident Handling	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Incident Response (IR Interview Template) • SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
IR-5 Incident Monitoring	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Incident Response (IR Interview Template) • SysAdmin (SysAdmin Interview Template). • Application Developer (Application Developer Interview Template). 2. Examine documentation based on interview results.
IR-6 Incident Reporting	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Incident Response (IR Interview Template) • Business Owner (Business Owner Interview Template) • Application Developer (Application Developer Interview Template). 2. Examine documentation based on interview results.
IR-7 Incident Response Assistance	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Incident Response (IR Interview Template) • SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
IR-8	1. Interview the following using the associated interview template questions:

Requirement	Checks and Procedures
Incident Response Plan	• ISSO/SO (ISSO/SO Interview Template) • Incident Response (IR Interview Template) • SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
IR-9 Information Spillage Response	N/A
IR-10 Integrated Information Security Analysis Team	N/A

3.9 Maintenance (MA)

Table 9 lists MA checks and procedures.

Table 9. Maintenance Requirement Evaluation

Requirement	Checks and Procedures
MA-1 System Maintenance Policy and Procedures	1. Review any documented maintenance policy and procedures. 2. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Facilities Manager (PE, MA, and MP Checklist) 3. Examine maintenance records; manufacturer/vendor maintenance specifications; other relevant documents or records.
MA-2 Controlled Maintenance	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Facilities Manager (PE, MA, and MP Checklist) 2. Examine maintenance records.
MA-3 Maintenance Tools	1. Review authorized list of tools. 2. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Facilities Manager (PE, MA, and MP Checklist) 3. Examine maintenance records.
MA-4 Non-Local Maintenance	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Facilities Manager (PE, MA, and MP Checklist) 2. Examine procedures and documentation addressing non-local maintenance for the information system.
MA-5 Maintenance Personnel	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Facilities Manager (PE, MA, and MP Checklist) 2. Examine service provider contracts and/or service level agreements (SLA) and list of authorized personnel, maintenance records.
MA-6 Timely Maintenance	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Facilities Manager (PE, MA, and MP Checklist)

Requirement	Checks and Procedures
	2. Examine service provider contracts and SLAs, inventory, and availability of spare parts.

3.10 Media Protection (MP)

Table 10 lists MP checks and procedures.

Table 10. Media Protection Requirement Evaluation

Requirement	Checks and Procedures
MP-1 Media Protection Policy and Procedures	1. Review any documented policy and procedures. 2. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Facilities Manager (PE, MA, and MP Checklist)
MP-2 Media Access	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Facilities Manager (PE, MA, and MP Checklist) 2. Observe automated mechanisms implementing access restrictions to media storage areas.
MP-3 Media Marking	1. Interview the following using the associated interview template questions: • Facilities Manager (PE, MA, and MP Checklist) 2. Observe media markings.
MP-4 Media Storage	1. Interview the following using the associated interview template questions: • Facilities Manager (PE, MA, and MP Checklist) 2. Observe media storage.
MP-5 Media Transport	1. Interview the following using the associated interview template questions: • Facilities Manager (PE, MA, and MP Checklist) 2. Observe media transport containers. 3. Review information system media transport records and audit records.
MP-6 Media Sanitization	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Facilities Manager (PE, MA, and MP Checklist) 2. Examine media sanitization and destruction records, methods
MP-7 Media Use	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Facilities Manager (PE, MA, and MP Checklist) 2. Examine media use records, methods.
MP-8 Media Downgrading	N/A

3.11 Physical and Environmental Protection (PE)

Table 11 lists PE checks and procedures.

Table 11. Physical and Environmental Protection Requirement Evaluation

Requirement	Checks and Procedures
PE-1 Physical and Environmental Protection Policy and Procedures	1. Review any documented policy and procedures. 2. Interview the following using the associated interview template questions: • Facilities Manager (PE, MA, and MP Checklist)

Requirement	Checks and Procedures
PE-2 Physical Access Authorizations	- Interview the following using the associated interview template questions: - Facilities Manager (PE, MA, and MP Checklist) - Examine documentation based on interview results.
PE-3 Physical Access Control	- Interview the following using the associated interview template questions: - Facilities Manager (PE, MA, and MP Checklist) - Observe control implementation. - Examine documentation based on interview results.
PE-4 Access Control for Transmission Medium	- Interview the following using the associated interview template questions: - Facilities Manager (PE, MA, and MP Checklist) - Observe control implementation. - Examine documentation based on interview results.
PE-5 Access Control for Output Devices	- Interview the following using the associated interview template questions: - Facilities Manager (PE, MA, and MP Checklist) - Observe control implementation. - Examine documentation based on interview results.
PE-6 Monitoring Physical Access	- Interview the following using the associated interview template questions: - Facilities Manager (PE, MA, and MP Checklist) - Observe control implementation. - Examine documentation based on interview results.
PE-8 Visitor Access Records	- Interview the following using the associated interview template questions: - Facilities Manager (PE, MA, and MP Checklist) - Observe control implementation. - Examine documentation based on interview results access records.
PE-9 Power Equipment and Power Cabling	- Interview the following using the associated interview template questions: - Facilities Manager (PE, MA, and MP Checklist) - Observe control implementation. - Examine documentation based on interview results access records.
PE-10 Emergency Shutoff	- Interview the following using the associated interview template questions: - Facilities Manager (PE, MA, and MP Checklist) - Observe control implementation. - Examine documentation based on interview results access records.
PE-11 Emergency Power	- Interview the following using the associated interview template questions: - Facilities Manager (PE, MA, and MP Checklist) - Observe control implementation. - Examine documentation based on interview results access.
PE-12 Emergency Lighting	- Interview the following using the associated interview template questions: - Facilities Manager (PE, MA, and MP Checklist) - Observe control implementation. - Examine documentation based on interview results access.
PE-13 Fire Protection	- Interview the following using the associated interview template questions: - Facilities Manager (PE, MA, and MP Checklist) - Observe control implementation.

Requirement	Checks and Procedures
	3. Examine documentation based on interview results access.
PE-14 Temperature and Humidity Controls	1. Interview the following using the associated interview template questions: Facilities Manager (PE, MA, and MP Checklist) 2. Observe control implementation.
PE-15 Water Damage Protection	1. Interview the following using the associated interview template questions: Facilities Manager (PE, MA, and MP Checklist) 2. Observe control implementation.
PE-16 Delivery and Removal	1. Interview the following using the associated interview template questions: Facilities Manager (PE, MA, and MP Checklist) 2. Observe control implementation. 3. Examine documentation based on interview results access.
PE-17 Alternate Work Site	1. Interview the following using the associated interview template questions: Facilities Manager (PE, MA, and MP Checklist) 2. Examine documentation based on interview results access.
PE-18 Location of Information System Components	1. Interview the following using the associated interview template questions: Facilities Manager (PE, MA, and MP Checklist) 2. Observe control implementation.
PE-19 Information Leakage	N/A
PE-20 Asset Monitoring and Tracking	N/A

3.12 Planning (PL)

Table 12 lists PL checks and procedures.

Table 12. Planning Requirement Evaluation

Requirement	Checks and Procedures
PL-1 Security Planning Policy and Procedures	1. Review security planning policies and procedures. 2. Interview the following using the associated interview template questions: - ISSO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template)
PL-2 System Security Plan	1. Review and evaluate the system security plan. 2. Interview the following using the associated interview template questions: - ISSO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template)
PL-4 Rules of Behavior	1. Interview the following using the associated interview template questions: - ISSO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) 2. Review RoBs for information system users.

Requirement	Checks and Procedures
PL-7 Security Concept of Operations	N/A
PL-8 Information Security-Architecture	- Interview the following using the associated interview template questions: - ISSO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) - Review supporting documentation.
PL-9 Central Management	N/A

3.13 Personnel Security (PS)

Table 13 lists PS checks and procedures.

Table 13. Personnel Security Requirement Evaluation

Requirement	Checks and Procedures
PS-1 Personnel Security Policy and Procedures	- Review personnel security policies and procedures. - Interview the following using the associated interview template questions: - HR/PS (HR/PS Interview Template) - ISSO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template)
PS-2 Position Risk Determination	- Interview the following using the associated interview template questions: - HR/PS (HR/PS Interview Template) - Review position categorization and list of risk designations for organizational positions.
PS-3 Personnel Screening	- Interview the following using the associated interview template questions: - HR/PS (HR/PS Interview Template) - Review procedures addressing personnel screening.
PS-4 Personnel Termination	- Interview the following using the associated interview template questions: - HR/PS (HR/PS Interview Template) - Review procedures addressing personnel termination.
PS-5 Personnel Transfer	- Interview the following using the associated interview template questions: - HR/PS (HR/PS Interview Template) - Review procedures addressing personnel transfers.
PS-6 Access Agreements	- Interview the following using the associated interview template questions: - HR/PS (HR/PS Interview Template) - Review sample access agreements for organizational information and information systems.
PS-7 Third-Party Personnel Security	- Interview the following using the associated interview template questions: - HR/PS (HR/PS Interview Template) - Review third-party personnel security agreements.
PS-8 Personnel Sanctions	- Interview the following using the associated interview template questions: - HR/PS (HR/PS Interview Template) - Review personnel sanctions.

3.14 Risk Assessment (RA)

Table 14 lists RA checks and procedures.

Table 14. Risk Assessment Requirement Evaluation

Requirement	Checks and Procedures
RA-1 Risk Assessment Policy and Procedures	1. Review any documented Risk Assessment Policy and Procedures. 2. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) 3. Examine documentation based on interview results.
RA-2 Security Categorization	1. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) 2. Examine documentation based on interview results.
RA-3 Risk Assessment	1. Interview the following using the associated interview template questions: • ISSO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) 2. Examine documentation based on interview results.
RA-5 Vulnerability Scanning	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
RA-6 Technical Surveillance Countermeasures Survey	N/A

3.15 System and Services Acquisition (SA)

Table 15 lists SA checks and procedures.

Table 15. System and Services Acquisition Requirement Evaluation

Requirement	Checks and Procedures
SA-1 System and Services Acquisition Policy and Procedures	1. Review any documented System and Services Acquisition Policy And procedures 2. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) 3. Examine documentation based on interview results.
SA-2 Allocation of Resources	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) 2. Examine documentation based on interview results.
SA-3 System Development Life Cycle	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) 2. Examine documentation based on interview results

Requirement	Checks and Procedures
SA-4 Acquisition Process	- Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) - Examine documentation based on interview results.
SA-5 Information System Documentation	- Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) - Application Developer (Application Developer Interview Template) - Examine documentation based on interview results.
SA-8 Security Engineering Principles	- Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - Application Developer (Application Developer Interview Template) - Examine documentation based on interview results.
SA-9 External Information System Services	- Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) - Examine documentation based on interview results.
SA-10 Developer Configuration Management	- Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - Application Developer (Application Developer Interview Template) - Examine documentation based on interview results.
SA-11 Developer Security Testing and Evaluation	- Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - Application Developer (Application Developer Interview Template) - Examine documentation based on interview results.
SA-12 Supply Chain Protection	- Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) - Examine documentation based on interview results
SA-13 Trustworthiness	- Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) - Examine documentation based on interview results
SA-14 Criticality Analysis	N/A
SA-15 Development Process, Standards, and P2 Tools	N/A
SA-16 Developer-Provided Training	N/A
SA-17 Developer Security Architecture and Design	N/A

Requirement	Checks and Procedures
SA-18 Tamper Resistance and Detection	N/A
SA-19 Component Authenticity	N/A
SA-20 Customized Development of Critical Components	N/A
SA-21 Developer Screening	N/A
SA-22 Unsupported System Components	N/A

3.16 System and Communications Protection (SC)

Table 16 lists SC checks and procedures.

Table 16. System and Communications Protection Requirement Evaluation

Requirement	Checks and Procedures
SC-1 System and Communications Protection Policy and Procedures	1. Review any documented System and Communications Protection Policy and procedures. 2. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • SysAdmin (SysAdmin Interview Template) 3. Examine documentation based on interview results.
SC-2 Application Partitioning	1. Technical test. 2. Participate in the interview of the following: • SysAdmin (SysAdmin Interview Template) 1. Examine documentation based on interview results.
SC-3 Security Function Isolation	1. Technical test. 2. Participate in the interview of the following: • SysAdmin (SysAdmin Interview Template) 3. Examine documentation based on interview results.
SC-4 Information in Shared Resources	1. Technical test 2. Participate in the interview of the following: • SysAdmin (SysAdmin Interview Template) 3. Examine documentation based on interview results.
SC-5 Denial of Service Protection	1. Technical test 2. Participate in the interview of the following: • SysAdmin (SysAdmin Interview Template) 3. Examine documentation based on interview results 4. Interview other relevant SMEs.
SC-6 Resource Priority	N/A
SC-7 Boundary Protection	1. Technical test 2. Participate in the interview of the following: • SysAdmin (SysAdmin Interview Template) 3. Examine documentation based on interview results. 4. Interview other relevant SMEs

Requirement	Checks and Procedures
SC-8 Transmission Confidentiality and Integrity	1. Technical test 2. Participate in the interview of the following • SysAdmin (SysAdmin Interview Template) 3. Examine documentation based on interview results
SC-10 Network Disconnect	1. Technical test. 2. Participate in the interview of the following • SysAdmin (SysAdmin Interview Template) 3. Examine documentation based on interview results
SC-11 Trusted Path	N/A
SC-12 Cryptographic Key Establishment and Management	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • SysAdmin (SysAdmin Interview Template) • Application Developer (Application Developer Interview Template) 2. Examine documentation based on interview results.
SC-13 Cryptographic Protection	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
SC-14 Public Access Protections	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
SC-15 Collaborative Computing Devices	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
SC-16 Transmission of Security Attributes	N/A
SC-17 Public Key Infrastructure Certificates	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
SC-18 Mobile Code	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
SC-19 Voice Over Internet Protocol	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
SC-20	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template)

Requirement	Checks and Procedures
Secure Name/Address Resolution Service (Authoritative Source)	• SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
SC-21 Secure Name/Address Resolution Service (Recursive and Caching Resolver)	1. Interview the following using the associated interview template questions: • SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
SC-22 Architecture and Provisioning for Name/Address Resolution Service	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
SC-23 Session Authenticity	1. Technical Test
SC-24 Fail in Known State	1. Technical Test
SC-25 Thin Nodes	N/A
SC-26 Honeypots	N/A
SC-27 Platform Independent Applications	N/A
SC-28 Protection of Information at Rest	1. Technical Test
SC-29 Heterogeneity	N/A
SC-30 Concealment and Misdirection	N/A
SC-31 Covert Channel Analysis	N/A
SC-32 Information System Partitioning	1. Technical Test
SC-34 Non-Modifiable Executable Programs	N/A
SC-35 Honeyclients	N/A
SC-36 Distributed Processing and Storage	N/A
SC-37 Out-of-Band Channels	N/A
SC-38 Operations Security	N/A
SC-39 Process Isolation	N/A
SC-40 Wireless Link Protection	N/A

Requirement	Checks and Procedures
SC-41 Port and I/O Device Access	N/A
SC-42 Sensor Capability and Data	N/A
SC-43 Usage Restrictions	N/A
SC-44 Detonation Chambers	N/A

3.17 System and Information Integrity (SI)

Table 17 lists SI checks and procedures.

Table 17. System and Information Integrity Requirement Evaluation

Requirement	Checks and Procedures
SI-1 System and Information Integrity Policy and Procedures	- Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - SysAdmin (SysAdmin Interview Template) - Application Developer (Application Developer Interview Template). - Examine documentation based on interview results.
SI-2 Flaw Remediation	- Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - SysAdmin (SysAdmin Interview Template) - Application Developer (Application Developer Interview Template). - Examine documentation based on interview results.
SI-3 Malicious Code Protection	- Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - SysAdmin (SysAdmin Interview Template) - Application Developer (Application Developer Interview Template) - Examine documentation based on interview results.
SI-4 Information System Monitoring	- Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - SysAdmin (SysAdmin Interview Template) - Application Developer (Application Developer Interview Template) - Examine documentation based on interview results.
SI-5 Security Alerts, Advisories and Directives	- Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - SysAdmin (SysAdmin Interview Template) - Application Developer (Application Developer Interview Template) - Examine documentation based on interview results.
SI-6 Security Function Verification	N/A
SI-7 Software, Firmware, and Information Integrity	- Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template)

Requirement	Checks and Procedures
	SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
SI-8 Spam Protection	1. Interview the following using the associated interview template questions: SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
SI-10 Information Input Validation	1. Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - SysAdmin (SysAdmin Interview Template) - Developer (SysAdmin Interview Template) 2. Examine documentation based on interview results.
SI-11 Error Handling	1. Technical Test 2. Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - SysAdmin (SysAdmin Interview Template) - Developer (SysAdmin Interview Template) 3. Examine documentation based on interview results. Examine documentation based on interview results.
SI-12 Information Output Handling and Retention	1. Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
SI-13 Predictable Failure Prevention	N/A
SI-14 Non-Persistence	N/A
SI-15 Information Output Filtering	N/A
SI-16 Memory Protection	1. Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - SysAdmin (SysAdmin Interview Template) 2. Examine documentation based on interview results.
SI-17 Fail-Safe Procedures	N/A

3.18 Program Management (PM)

Table 18 lists PM checks and procedures.

Table 18. Program Management Requirement Evaluation

Requirement	Checks and Procedures
PM-1 Information Security Program Plan	1. Interview the following using the associated interview template questions: ISSO/SO (ISSO/SO Interview Template)

Requirement	Checks and Procedures
	Business Owner (Business Owner Interview Template) 2. Examine documentation based on interview results.
PM-2 Senior Information Security Officer	1. Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) 2. Examine documentation based on interview results.
PM-3 Information Security Resources	1. Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) 2. Examine documentation based on interview results.
PM-4 Plan of Action and Milestones Process	1. No Test
PM-5 Information System Inventory	1. No Test
PM-6 Information Security Measures of Performance	1. Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) 2. Examine documentation based on interview results.
PM-7 Enterprise Architecture	1. No Test
PM-8 Critical Infrastructure Plan	1. Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) 2. Examine documentation based on interview results.
PM-9 Risk Management Strategy	1. Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) 2. Examine documentation based on interview results.
PM-10 Security Authorization Process	3. Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) 4. Examine documentation based on interview results.
PM-11 Mission/Business Process Definition	1. Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) 2. Examine documentation based on interview results.
PM-12 Insider Threat Program	1. Interview the following using the associated interview template questions: - ISSO/SO (ISSO/SO Interview Template) - Business Owner (Business Owner Interview Template) 2. Examine documentation based on interview results.
PM-13	1. Interview the following using the associated interview template questions:

Requirement	Checks and Procedures
Information Security Workforce	• ISSO/SO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) 2. Examine documentation based on interview results.
PM-14 Testing, Training, and Monitoring	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) 2. Examine documentation based on interview results.
PM-15 Contacts with Security Groups and Associations	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) 2. Examine documentation based on interview results.
PM-16 Threat Awareness Program	1. Interview the following using the associated interview template questions: • ISSO/SO (ISSO/SO Interview Template) • Business Owner (Business Owner Interview Template) 2. Examine documentation based on interview results.

4. References

1. FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.
2. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.
3. NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.

5. List of Acronyms

Acronym	Definition
AC	Access Control
AT	Awareness and Training
ATO	Authority to Operate
AU	Audit and Accountability
CAP	Corrective Action Plan
CM	Configuration Management
CP	Contingency Planning
CR	Change Request
DAC	Discretionary Access Control
DBA	Database Administrator
HR	Human Resources
IA	Identification and Authentication
IP	Internet Protocol
IR	Incident Response
IS	Information Security
ISSO	Information System Security Officer
M&O	Management & Operations
MA	Maintenance
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Media Protection
O&M	Operations & Maintenance
PE	Physical and Environmental Protection
PIA	Privacy Impact Assessment
PL	Planning
POA&M	Plan of Action and Milestones
POC	Point of Contact
PS	Personnel Security
RA	Risk Assessment

Acronym	Definition
RoB	Rules of Behavior
SA	System and Services Acquisition
SC	System and Communications Protection
SDD	System Design Document
SI	System and Information Integrity
SLA	Service Level Agreement
SO	Security Officer
STIG	Security Technical Implementation Guide
SysAdmin	System Administrator
URL	Uniformed Resource Locator
VDD	Version Description Document

Network Security Control Assessment Guide

The views, opinions and/or findings contained in this guide are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Approved for Public Release: 19-3536.
Distribution Unlimited.

©2019 The MITRE Corporation. All rights reserved.

Author(s): Nathan Adams
Milton Shomo

September 2015

McLean, VA

MITRE

This page intentionally left blank.

Table of Contents

1. Overview	1
1.1 Caveats	1
1.2 Assessment Methodology	2
1.2.1 Phase 1: Planning	2
1.2.2 Phase 2: Assessment	2
1.2.3 Phase 3: Reporting	2
2. Assessment Activities	3
2.1 Phase 1: Planning	3
2.2 Phase 2: Assessment	4
2.2.1 Documentation Review	4
2.2.2 Network Architecture Review	4
2.2.3 Device Configuration Review	4
2.2.4 Interviews	5
2.3 Phase 3: Reporting	5
3. Assessing Security Controls	6
3.1 Access Control (AC)	6
3.2 Awareness and Training (AT)	10
3.3 Audit and Accountability (AU)	10
3.4 Certification, Accreditation, and Security Assessments (CA)	12
3.5 Configuration Management (CM)	12
3.6 Contingency Planning (CP)	16
3.7 Identification and Authentication (IA)	16
3.8 Incident Response (IR)	18
3.9 Maintenance (MA)	18
3.10 Media Protection (MP)	19
3.11 Physical and Environmental Protection (PE)	19
3.12 Planning (PL)	19
3.13 Personnel Security (PS)	19
3.14 Risk Assessment (RA)	19
3.15 System and Services Acquisition (SA)	19
3.16 System and Communications Protection (SC)	19
3.17 System and Information Integrity (SI)	22
4. References	24

5. List of Acronyms.....	25
--------------------------	----

List of Tables

Table 1. Access Control Requirement Evaluation	6
Table 2. Audit and Accountability Requirement Evaluation	11
Table 3. Configuration Management Requirement Evaluation.....	13
Table 4. Identification and Authentication Requirement Evaluation.....	16
Table 5. System and Communications Protection Requirement Evaluation.....	19
Table 6. System and Information Integrity Requirement Evaluation	22

This page intentionally left blank.

1. Overview

This *Network Security Control Assessment Guide* is intended to serve as a practical guidance for information security (IS) engineers who conduct network infrastructure security control assessments systems that must meet federal guidance. This guide focuses on testing and evaluation techniques for technical controls required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*. Parameters defined in this guide are considered industry best practice but may be modified by the organization as required.

1.1 Caveats

The controls presented here are for a Federal Information Processing Standard (FIPS) 199 Moderate Impact rated system. Thus, controls for Low and High Impact rated systems may differ.

This guide focuses on technical testing of Cisco routers and switches that use the Internetworking Operating System (IOS) and Cisco firewalls such as the Adaptive Security Appliance (ASA). The network security evaluator, who is a subject matter expert (SME) on Cisco IOS/ASA, will use this guide as a reference when conducting network infrastructure security assessments.

This Network Assessment guide:

- Focuses on Cisco routers and switches that use IOS and Cisco firewalls using the ASA OS. It does not address the newer Nexus data center switches that run the NX-OS. However, the concepts behind the requirements, checks and procedures in the guide are equally applicable to other network technologies.
- Provides the Network Security Evaluator a reference for conducting network infrastructure security assessments. The evaluator is familiar with configuring numerous network devices and services such as routers, switches, and firewalls using the command line interface, including using commands in the User Exec and Privileged Exec modes.
- Agrees with some Cisco IOS settings that are enabled or disabled by default and presents these settings with other recommended settings. Note, some default settings do not normally appear when issuing the “show run” command, and some default settings in previous IOS versions are different from current IOS versions.
- Recommends, as a best security practice, explicitly enabling or disabling some settings.
- Provides sample Cisco commands for easy reference in verifying the security implementation of many required controls.
- Refers the evaluator in cases where sample Cisco commands are not available to the reference documents listed in this guide.

- Refers the evaluator when there are no specific recommendations for a particular parameter setting to the Defense Information Systems Agency (DISA) Secure Technical Implementation Guides (STIG).

The configuration settings contained in Section 3 should not be considered an authoritative checklist as there may be more than one way to implement the intent of a particular control. In addition, there may be valid business or functional reasons for a particular device setting that deviates from what is presented here.

1.2 Assessment Methodology

The following sections define the three-phase assessment methodology on which the guide is based.

1.2.1 Phase 1: Planning

The first phase, Planning, defines the assessment's scope, identifies goals, sets boundaries, and identifies assessment activities. This phase, as well as subsequent phases, requires the coordination of all involved parties. During this phase, the Evaluation Team reviews all security policies and procedures in accordance with the organization's security requirements. The team will then create assessment scenarios and premises and define assessment agreeable terms as approved by the organization.

1.2.2 Phase 2: Assessment

Phase 2 may have several steps depending on the assessment's objectives, scope, and goals as set forth in Planning Phase. These steps can be grouped by the nature of the activities involved. These activity groups are as follows:

- **Information Collection**—thorough research must be performed against the target system/application before any meaningful assessment can be conducted. Data gathered is analyzed as the assessment proceeds and when the assessment is complete. Prior to the assessment, pre-assessment planning requests for information/artifacts will need to be made in order to have an accurate understanding of the testing environment and to properly prepare for the assessment.
- **Enumeration**—activities that provide specific information about assessment targets. This information is often collected using appropriate software tools.
- **Testing and Review**—activities that typically involve both the automated testing of security vulnerabilities via software tools and the evaluation of particular aspects of the organization's security policies and practices by Assessment Team members.

1.2.3 Phase 3: Reporting

Phase 3, Reporting, documents the soundness of the implemented security controls and consolidates all findings into the final output. This output includes reports that provide a summary of key findings and actionable recommendations, as well as provisions for all information derived from the assessment.

2. Assessment Activities

Assessment activities should be grouped by the three phases—Planning, Assessment, and Reporting.

2.1 Phase 1: Planning

The Network Evaluator reviews the *Security Assessment Test Plan* to understand the scope of the assessment. Based on the scope, security policies and procedures in accordance with organization security requirements are reviewed. As documentation is received on the system, the Network Evaluator will review to ensure that the Evaluator has full knowledge of the system to be assessed and the components to be evaluated during the assessment phase. The Evaluator will determine any technical scripts, scans, or other requests to be made to ensure that the onsite assessment runs clear. During this time, any special requests for testing are provided to the Lead Evaluator so the Evaluator can contact the system's point of contact (POC) and the organization facilitator to ensure all requirements for the test are complete. The Network Evaluator will then create assessment scenarios, update the testing strategy, and select tools to be used. To prepare for this assessment, the Network Evaluator should review the following documentation prior to the assessment:

- Network diagrams depicting both the logical and physical network architecture
- Baseline configuration documents for each type of device
- List of required firewall open ports based upon applications traversing the firewalls
- System Security Plan (SSP)
- Risk Assessment (RA)
- Configuration Management (CM) policy document
- Change Management policy document
- Asset Management policy document
- Related documents, such as listed below:
 - Network device configuration review policy
 - Firewall rule set review policy
 - Password change policy
 - Audit log retention and review policy
 - Sample network-related change ticket
 - Sample network device asset management record
- Output for each network device from the Cisco IOS commands:
 - `show run`
 - `show version`
 - `show ip ssh`
 - `show ip interface brief`
 - `show logging`
 - `show snmp group`

– show cdp

2.2 Phase 2: Assessment

The network infrastructure assessment activities consist of a documentation review, network architecture review, device configuration review, and personnel interviews. The activities and the detailed supporting processes and procedures must be at an adequate level to determine compliance with controls at each system impact level: Low, Moderate, and High.

2.2.1 Documentation Review

The Network Evaluator will review documents provided by the organization. The review will assess whether the system documentation adequately describes implemented security controls and augments technical security control implementations. As a part of the assessment, the team will evaluate documentation such as, but not limited to, the SSP, Information System Risk Assessment, Contingency Plan and Baseline Configuration Guide in accordance with organization guidelines and provide feedback.

2.2.2 Network Architecture Review

The overall network architecture must be evaluated. This evaluation should be based upon sound network architecture principles. Issues to watch for include:

- One-arm routing and one-armed firewalls
- Firewalls bypassed by an external entity (i.e., untrusted external connections) or a device (e.g., switch)
- Zones, tiers, environments (e.g., development) that are not separated properly (i.e., most require a firewall at their border)
- Properly designed De-Militarized Zones (DMZ)
- Proper network device placement (i.e., overall, are devices placed properly in the network design)
- Virtualized environment (e.g. servers in different zones cannot be virtualized on one physical server)

2.2.3 Device Configuration Review

The vast majority of the work performed by the Network Evaluator is devoted to device configuration review. Network device configurations must be examined to determine if the organization controls have been properly implemented.

The Network Evaluator must understand the intent of each control, determine if a technical implementation is required to meet the control, and then determine the necessary configuration parameters required to implement that control.

2.2.4 Interviews

Initial discussions and follow-on interviews are conducted as necessary with the network administrator to confirm potential findings. These interviews are conducted with both the Network Evaluator and the Management and Operations (M&O) Evaluator present. The technical questions help supplement and corroborate the M&O interview questions. They also serve to provide more in-depth analysis for certain controls requiring additional scrutiny. Questions are tailored to the network environment and its implementations.

2.3 Phase 3: Reporting

The Network Evaluator must document all weaknesses following the organization reporting procedures and forward to the Lead Evaluator for consolidation and discussion during the daily briefings. The Network Evaluator should discuss any Medium or High findings with the system support staff upon discovery, so that the daily briefing is not the first time staff is exposed to the finding and the supporting evidence.

It is during this phase that the Network Evaluator also reviews any closure evidence if provided. While the finding is not removed from the report, the finding can be closed based on the Evaluator determining that the evidence provided is adequate to close the finding.

The reporting phase includes a documentation of the soundness of the implemented security controls and the actual findings are consolidated into a final report.

3. Assessing Security Controls

The following sections provide guidance on the IOS commands that could be implemented for each relevant control and concepts that support control implementation validation. This section should not be considered an authoritative checklist as there may be more than one way to implement the intent of a particular control. In addition, there may be valid business reasons for a particular device setting that deviates from what is presented here.

For controls listed as N/A, implementation of this control may not be supported by Cisco, may not be related to technical implementation of network devices, or may require a process or procedure to implement (i.e., no technical solution).

3.1 Access Control (AC)

Table 1 lists AC checks and procedures.

Table 1. Access Control Requirement Evaluation

Requirement	Checks and Procedures
AC-1 Access Control Policy and Procedures	N/A
AC-2 Account Management	Ensure that the authentication server TACACS+ or similar authentication and authorization system is used to centrally manage network device administrator accounts. For switches and routers: <pre>aaa new-model aaa authentication login list-name tacacs+ local aaa authentication enable default group tacacs+ enable aaa authorization config-commands aaa authorization exec default group tacacs+ local tacacs-server host x.x.x.x tacacs-server key xxxxxxxx</pre> For firewalls: <pre>aaa-server server-group protocol tacacs+ aaa-server server-group host x.x.x.x key xxxxxxxx aaa authentication ssh console server-group LOCAL aaa authentication enable console server-group LOCAL aaa authentication serial console server-group LOCAL aaa authorization command server-group LOCAL</pre> Ensure one account is defined locally on the router/switch for use in an emergency. For switches and routers: <pre>username account_name password 15 xxxxxxxx</pre> For firewalls:

Requirement	Checks and Procedures
	<pre>username account_name password xxxxxxxx encrypted</pre>
AC-3 Access Enforcement	Ensure administrative line Access Control Lists (ACL) are used to restrict traffic to administrative ports. <pre>access-list access_list_number remark VTY ACCESS CONTROL LIST access-list access_list_number permit authorized_administrative_host_IP access-list access_list_number deny any log</pre> <pre>line vty 0 4 access-class access_list_number in</pre> If the internal Hyper Text transfer Protocol Secure (HTTPS) server is used for device administration, ensure ACL is used to restrict access. For switches and routers: <pre>ip http access-class {access-list-number access- list-name}</pre> For firewalls: <pre>http source_IP_address mask source_interface</pre> If SNMP is used for device management, ensure access to SNMP information is restricted. For switches and routers: <pre>snmp-server community community_string RO access- list-number</pre> For firewalls: <pre>snmp-server host interface {hostname ip_address}</pre> For switches running CatOS ensure IP permit statements are configured to control access to the device. <pre>set ip permit enable set ip permit addr [mask] [telnet ssh snmp all]</pre> Ensure administrative line, HTTP, SNMP ACLs and IP Permit statements are sufficiently restrictive. Controls should be configured to only allow access from specific hosts or a relatively small management sub-net. Ensure CON, AUX, and VTY lines are protected by a password. <pre>line vty 0 4 password 7 xxxxxxxxxx</pre> Ensure username/password authentication is required for access to the HTTP interface. <pre>ip http authentication {aaa enable local tacacs}</pre> AAA is the preferred authentication method. SNMP should be configured for RO, unless required for operations and properly documented in the SSP and RA. The SNMP configuration lines should only contain "RO" and not Read-Write ("RW").

Requirement	Checks and Procedures
	<code>snmp-server community community_string RO</code>
AC-4 Information Flow Enforcement	The border device should be configured to block inbound Internet Protocol (IP) packets with a source address that contains an IP address from the internal network (i.e. RFC 1918 addresses), any local host loopback addresses, the link-local IP address range (169.254.00/16), Internet Assigned Number Authority (IANA) unallocated addresses, or any reserved private address in the source field. Allowing these IP packets into the network could facilitate spoofing and other attack scenarios. Verify ACLs are in place to restrict this type of traffic: <pre> access-list 101 deny ip 169.254.0.0 0.0.255.255 any log access-list 101 deny ip 10.0.0.0 0.255.255.255 any log access-list 101 deny ip 172.16.0.0 0.15.255.255 any log access-list 101 deny ip 192.168.0.0 0.0.255.255 any log access-list 101 permit ip any any </pre> Firewalls must have ACLs in place to properly limit traffic between zones. Examine all ACLs to determine if they are appropriate to protect the environment. Avoid the use of the keyword “any” for source, destination, or port designations. Ensure SNMP, NTP, and authentication traffic use the devices loopback address as the source address for this traffic. For switches and routers: <pre> snmp-server trap-source loopback0 ntp source loopback0 ip tacacs source-interface loopback0 </pre> For firewalls: <pre> snmp-server host loopback0 {hostname ip_address} ntp server ip_address loopback0 aaa-server server_group loopback0 </pre>
AC-5 Separation of Duties	N/A
AC-6 Least Privilege	N/A
AC-7 Unsuccessful Log-on Attempts	Ensure switches and routers are configured to reset the SSH interface after three (3) unsuccessful log-on attempts. <pre>ip ssh authentication-retries 3</pre>
AC-8 System Use Notification	Ensure that warning banners are deployed on network devices allowing SSH or HTTP(S) access. The login banner, which includes a legal notice, should not include any network architecture information or router configuration details. For Cisco switches, routers, and firewalls: <pre> banner login [appropriately worded banner] banner motd [appropriately worded banner] </pre>

Requirement	Checks and Procedures
AC-9 Previous Logon (Access) Notification	N/A
AC-10 Concurrent Session Control	N/A
AC-11 Session Lock	Ensure that the VTY, CON, and AUX inactivity timeout value is set to fifteen (15) minutes or less. For switches and routers: <pre> line con 0 exec-timeout 15 0 line aux 0 exec-timeout 15 0 line vty 0 4 exec-timeout 15 0 </pre> For firewalls: <pre> ssh timeout 15 console timeout 15 </pre> Ensure a timeout value for incomplete SSH connection attempts is defined. For switches and routers (default is 120 seconds): <pre> ip ssh time-out 60 </pre>
AC-12 Session Termination	N/A
AC-14 Permitted Actions without Identification or Authentication	N/A
AC-16 Security Attributes	N/A

Requirement	Checks and Procedures
AC-17 Remote Access	Ensure the auxiliary port is disabled if a secured modem providing encryption and authentication is not connected. The use of Plain Old Telephone Service (POTS) lines to modems connecting to network devices provides clear text of authentication traffic over commercial circuits that could be captured and used to compromise the network. Additionally, war dial attacks on the device could degrade the device and the production network. Secured modem devices must be able to authenticate users and must negotiate a key exchange before full encryption takes place. The modem will provide full encryption capability (Triple Data Encryption Standard -3DES) or stronger. Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be explicitly authorized, in writing, by the CIO or his/her designated representative. <pre> line aux 0 no exec transport input none </pre>
AC-18 Wireless Access	The organization prohibits the installation of wireless access points (WAP) to organization information systems unless explicitly authorized, in writing, by the organization CIO or his/her designated representative.
AC-19 Access Control for Mobile Devices	N/A
AC-20 Use of External Information Systems	N/A
AC-21 Information Sharing	N/A
AC-22 Publicly Accessible Content	N/A
AC-23 Data Mining Protection	N/A
AC-24 Access Control Decisions	N/A
AC-25 Reference Monitor	N/A

3.2 Awareness and Training (AT)

There are no network device checks and procedures in this section.

3.3 Audit and Accountability (AU)

Table 2 lists AU checks and procedures.

Table 2. Audit and Accountability Requirement Evaluation

Requirement	Checks and Procedures
AU-1 Audit and Accountability Policy and Procedures	N/A
AU-2 Auditable Events	Ensure all ACLs have a “log” keyword following every deny statement. Ensure all ACLs contain an explicit “deny any log” statement at the end of the ACL. An example configuration is depicted below: <pre> access-list 100 permit tcp source_address source_port destination_address destination_port access-list 100 deny tcp source destination log access-list 100 permit udp source_address source_port destination_address destination_port access-list 100 deny any log </pre> Ensure command auditing/accounting is configured on the device. For switches and routers: <pre> aaa accounting exec default start-stop group tacacs+ aaa accounting commands 1 default start-stop group tacacs+ aaa accounting commands 15 default start-stop group tacacs+ aaa accounting system default start-stop group tacacs+ </pre> For firewalls: <pre> aaa accounting ssh console server_group aaa accounting command server_group </pre> Ensure logging is set to at least Level 6 Informational.
AU-3 Content of Audit Records	N/A
AU-4 Audit Storage Capacity	N/A
AU-5 Response to Audit Processing Failures	N/A
AU-6 Audit Monitoring, Analysis, and Reporting	N/A
AU-7 Audit Reduction and Report Generation	N/A
AU-8 Time Stamps	Ensure logging is configured to include message timestamps. For switches and routers: <pre> service timestamp log datetime show-timezone msec </pre>

Requirement	Checks and Procedures
	For firewalls: logging timestamp Ensure the configuration of primary and secondary NTP time servers in order to synchronize the time among network devices and servers. To set NTP time servers: <pre>ntp server ntp_server_address prefer ntp server ntp_server_address</pre>
AU-9 Protection of Audit Information	N/A
AU-10 Non-Repudiation	N/A
AU-11 Audit Retention	N/A
AU-12 Audit Generation	Ensure logging is enable and sending log data to a syslog server. The log level should be set to Informational (level 6). For switches and routers: <pre>logging buffered log_buffer_size informational logging console informational logging trap informational logging log_host_IP</pre> For firewalls: <pre>logging enable logging buffer-size log_buffer_size logging buffered informational logging trap informational logging asdm informational logging host interface_to_access_log_host log_host_IP</pre>
AU-13 Monitoring for Information Disclosure	N/A
AU-14 Session Audit	N/A
AU-15 Alternate Audit Capability	N/A
AU-16 Cross-Organizational Auditing	N/A

3.4 Certification, Accreditation, and Security Assessments (CA)

There are no network device checks and procedures in this section.

3.5 Configuration Management (CM)

Table 3 lists CM checks and procedures.

Table 3. Configuration Management Requirement Evaluation

Requirement	Checks and Procedures
CM-1 Configuration Management Policy and Procedures	N/A
CM-2 Baseline Configuration	Ensure IOS and ASA versions are consistent across all like devices. Ensure device baselines have been properly implemented across all like devices. Examine device configurations and verify that all configuration items are still in use. For instance, all Virtual Local Area Networks (VLAN) and ACLs that are defined should be actually used. Ensure baseline documents are complete and contain all common configuration lines required for the system.
CM-3 Configuration Change Control	N/A
CM-4 Security Impact Analysis	N/A
CM-5 Access Restrictions for Change	N/A
CM-6 Configuration Settings	Ensure the use of Transmission Control Protocol (TCP) keepalives to kill sessions where the remote side has died. Stale connections use resources and could potentially be hijacked to gain unauthorized access. For switches and routers: <pre>service tcp-keepalives-in service tcp-keepalives-out</pre> Ensure the maximum wait interval for establishing a TCP connection request to the network device set to ten (10) seconds or less. For switches and routers: <pre>ip tcp synwait-time 10</pre> Ensure all unused interfaces are placed in administrative shutdown mode. Examine the output from the “show ip interface brief” command. An interface with a Protocol of “down” must have a status of “administratively down” as shown in the example below: <pre> InterfaceIP Address OK? Method Status Protocol FastEthernet0/0 10.1.1.2 YES NVRAM up up FastEthernet0/1 10.1.1.3 YES NVRAM administratively down down </pre> When using Spanning Tree Protocol (STP), ensure STP Portfast Bridge Protocol Data Unit (BPDU) Guard is enabled, which allows network administrators to enforce the STP topology on ports enabled with Portfast. By default, STP BPDU Guard is disabled.

Requirement	Checks and Procedures
	To enable STP BPDU at the global level: <pre>spanning-tree portfast bpduguard default</pre> To enable STP BPDU at the interface level: <pre>interface FastEthernet0/1 spanning-tree portfast spanning-tree bpduguard enable</pre> Ensure VLAN 1 is not used and is placed in administrative shutdown mode. VLAN1 is the default VLAN on Cisco switching devices, which all ports are assigned to by default, including management ports. As a result, VLAN1 may unwisely span the entire network, if not appropriately pruned. <pre>interface Vlan1 no ip address shutdown</pre> Cisco-proprietary VLAN Trunking Protocol (VTP) may simplify switch management; however, VTP is in server mode by default, potentially exposing VLAN information. If possible, turn off VTP (CatOS) or place in transparent mode. If VTP is necessary, then ensure appropriate setup of management domains and assign a strong password to the VTP management domain. <pre>set vtp mode off or vtp mode transparent or vtp domain domain_name vtp password xxxxxxxx</pre> Ensure border router has ACLs in place to block inbound Internet Control Message Protocol (ICMP) traffic. The border device should be configured to ensure that the ingress ACL blocks all inbound ICMP traffic message types with the exception of Echo Reply (type 0), Time Exceeded (type 11), and Destination Unreachable (type 3). Other types of ICMP traffic could be utilized in a Denial-of-Service (DoS) attack. Ensure border router has ACLs in place to block outbound ICMP traffic. The border device should be configured to ensure that the outbound ACL blocks all ICMP traffic message types with the exception of Echo, Parameter Problem, Source Quench, and Destination Unreachable—Fragmentation Needed and Don't Fragment. Other types of ICMP traffic could be utilized in a DoS attack. If a Cisco Content Services Switch is utilized in the environment ensure the configuration conforms to the guidance provided in "Cisco Content Services Switch Security Configuration Guide" and a paper titled, "Improve Security of the CSS11000 and CSS11500".
CM-7 Least Functionality	Ensure the bootp server is disabled. The default is enabled. This is rarely needed and may open a security hole. <pre>no ip bootp server</pre> Ensure Cisco Discovery Protocol (CDP) service is disabled. There have been published DoS attacks that use CDP. CDP should be completely disabled unless there is a need for it. To disable CDP globally: <pre>no cdp run</pre>

Requirement	Checks and Procedures
	To disable CDP at the interface level: <pre>interface FastEthernet0/1 ip address x.x.x.x x.x.x.x no cdp enable</pre> Ensure source routing is disabled. Source routing is a feature of IP whereby individual packets can specify routes. It is used in several kinds of attacks. <pre>no ip source-routing</pre> Ensure gratuitous Address Resolution Protocol (ARP) is disabled. A spoofed gratuitous ARP message can cause network-mapping information to be stored incorrectly, affecting networking performance. <pre>no ip gratuitous-arp</pre> Ensure ICMP unreachable notifications, mask replies, proxy arp and redirects are disabled on all external interfaces of the premise router. <pre>interface FastEthernet 0/0 ip address x.x.x.x x.x.x.x no ip redirect no ip unreachable no ip proxy-arp no ip mask-reply</pre> Disable IP classless routing. By default, a Cisco router will make an attempt to router almost any IP packet. If a packet arrives addressed to a subnet of a network that has no default network route, then IOS will, with IP classless routing, forward the packet along the best available route to a super-net of the addressed subnet. This feature is often not needed. On the network devices where it is not needed, disable it: <pre>no ip classless</pre> Disable the Dynamic Host Configuration Protocol (DHCP) server. By sending a large packet to the DHCP port, it is possible to freeze the router's processing engine. <pre>no ip dhcp server</pre> Ensure Cisco Networking Service (CNS) is not in use. The device configuration should not contain commands similar to the following: <pre>diagnostic cns publish cisco.cns.device.diag_results diagnostic cns subscribe cisco.cns.device.diag_commands</pre> Ensure TFTP, File Transfer Protocol (FTP), and Berkeley Software Distribution (BSD) r-command servers are disabled. These services are disabled by default. Review all Cisco configuration to verify that none of the following statements are present: <pre>tftp-server enable ftp-server enable ip rcmd rcp-enable ip rcmd rsh-enable . . line vty 0 4 transport input rlogin telnet</pre>

Requirement	Checks and Procedures
	Ensure loading of remote IOS and configurations is disabled. Upon boot-up, if a router does not find a valid Cisco IOS in Flash, it will perform a TFTP, or network, boot. "Service config" allows a router to load its startup configuration from a remote device. Unless the router absolutely needs it, disable network boot and auto-loading. If required, these features should be documented in the SSP. <pre>no boot network no service config</pre> Ensure the TCP and User Datagram Protocol (UDP) small server services are disabled. These services are disabled by default after Cisco IOS 11.3. Review all Cisco configurations to verify none of the following statements are present: <pre>service tcp-small-servers service udp-small-servers</pre> Ensure all unused device ports and interfaces are placed in administrative shutdown mode.
CM-8 Information System Component Inventory	N/A
CM-9 Configuration Management Plan	N/A
CM-10 Software Usage Restrictions	N/A
CM-11 User-Installed Software	N/A

3.6 Contingency Planning (CP)

There are no network device checks and procedures in this section.

3.7 Identification and Authentication (IA)

Table 4 lists IA checks and procedures.

Table 4. Identification and Authentication Requirement Evaluation

Requirement	Checks and Procedures
IA-1 Identification and Authentication Policy and Procedures	N/A
IA-2 User Identification and Authentication (Organizational Users)	Ensure Trivial File Transfer Protocol (TFTP) is not enabled. The configuration file should not contain any lines that begin: <pre>tftp-server</pre>

Requirement	Checks and Procedures
IA-3 Device Identification and Authentication	Ensure NTP messages are authenticated. Since NTP is used to ensure accurate log file timestamp information, NTP could pose a security risk if a malicious user were able to falsify NTP information. <pre> ntp authenticate ntp authentication-key key_number md5 authentication_key ntp trusted-key key_number </pre>
IA-4 Identifier Management	N/A
IA-5 Authenticator Management	Remove default user accounts. The account name “cisco” should not appear in the following command: <pre>username cisco privilege 15 password xxxxxxxx</pre> Ensure devices are configured to only support SSH. For switches and routers: <pre> line vty 0 4 transport input ssh </pre> For firewalls verify the following command is not present: <pre>telnet source_IP_address mask source_interface</pre> and contains one or more of the following commands: <pre>ssh source_IP_address mask source_interface</pre> If the device’s internal Web server is used to manage the device, ensure connections are restricted to HTTPS only. For Cisco switches and routers: <pre> no ip http-server ip http secure-server </pre> For firewalls: <pre> http server enable http source_IP_address mask source_interface </pre> Ensure all passwords are encrypted in the configuration file. For Cisco switches and routers: <pre>service password-encryption</pre> For firewalls ensure the “encrypted” key word is used: <pre> enable password encrypted_password encrypted passwd encrypted_password encrypted username account_name password encrypted_password encrypted privilege 15 </pre> Ensure SNMP configuration does not use default community strings. For switches, routers, and firewalls:

Requirement	Checks and Procedures
	<pre>snmp-server community community_strings_other_than_"public/read/write"</pre> Ensure SNMP community strings conform to organization requirements for strong passwords. If community strings have been removed from the configuration files so this information can be obtained through the network administrator interview process. Ensure all local account passwords conform to organization requirements for strong passwords. Passwords should be encrypted in the configuration file so this information can be obtained through the network administrator interview process. Ensure all VTY, CON, and AUX passwords conform to organization requirements for strong passwords. Passwords should be encrypted in the configuration file so this information can be obtained through the network administrator interview process. Ensure enable passwords conform to organization requirements for strong passwords. Passwords should be encrypted in the configuration file so this information can be obtained through the network administrator interview process.
IA-6 Authenticator Feedback	N/A
IA-7 Cryptographic Module Authentication	N/A
IA-8 Uniquely Identify and Authenticate (Non- Organizational Users)	N/A
IA-9 Service Identification and Authentication	N/A
IA-10 Adaptive Identification and Authentication	N/A
IA-11 Re-authentication	N/A

3.8 Incident Response (IR)

There are no network device checks and procedures in this section.

3.9 Maintenance (MA)

There are no network device checks and procedures in this section.

3.10 Media Protection (MP)

There are no network device checks and procedures in this section.

3.11 Physical and Environmental Protection (PE)

There are no network device checks and procedures in this section.

3.12 Planning (PL)

There are no network device checks and procedures in this section.

3.13 Personnel Security (PS)

There are no network device checks and procedures in this section.

3.14 Risk Assessment (RA)

There are no network device checks and procedures in this section.

3.15 System and Services Acquisition (SA)

There are no network device checks and procedures in this section.

3.16 System and Communications Protection (SC)

Table 5 lists SC checks and procedures.

Table 5. System and Communications Protection Requirement Evaluation

Requirement	Checks and Procedures
SC-1 System and Communications Protection Policy and Procedures	N/A
SC-2 Application Partitioning	N/A
SC-3 Security Function Isolation	N/A
SC-4 Information in Shared Resources	N/A
SC-5 Denial-of-Service Protection	N/A
SC-6 Resource Priority	N/A

Requirement	Checks and Procedures
SC-7 Boundary Protection	If Border Gateway Protocol (BGP) is used, ensure it is securely configured. Ensure that strong ACLs are used to permit and deny traffic on port 179 between authorized devices, specify which version of BGP shall be used, and configure a maximum prefix to prevent a mistake or mishap by peers from causing the router to be over utilized by filling the routing and BGP tables. Refer to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-54, <i>Border Gateway Protocol</i> for configuration recommendations.
SC-8 Transmission Confidentiality and Integrity	N/A
SC-10 Network Disconnect	N/A
SC-11 Trusted Path	N/A
SC-12 Cryptographic Key Establishment and Management	N/A
SC-13 Cryptographic Protection	Ensure SSH version 2 is supported. For switches and routers: <pre>ip ssh version 2</pre> For firewalls: <pre>ssh version 2</pre> For Cisco devices, ensure the “enable secret” command is set. Without the enable secret command, the enable password command uses weak encryption to protect the password. Cisco defined Type 7 encryption algorithm is known to be weak. Type 5 uses an MD5 hash, which is much stronger. <pre>enable secret 5 encrypted_password</pre> Ensure SNMP version 3 is supported for devices that utilize SNMP. Verify version 3 and priv Level (authenticates packet with MD5 or SHA algorithms, encrypts packet using CBC-DES algorithm) is specified for all SNMP server groups and hosts: <pre>snmp-server group group_name v3 priv snmp-server host host-addr v3 priv</pre> Ensure the username command is not configured to use Cisco 7 password hash but uses MD5 instead. <pre>username secret</pre> Ensure switch and router TACACS server keys are not transmitted in the clear. <pre>tacacs-server key 7 string</pre>
SC-14 Public Access Protections	N/A

Requirement	Checks and Procedures
SC-15 Collaborative Computing	N/A
SC-16 Transmission of Security Attributes	N/A
SC-17 Public Key Infrastructure Certificates	N/A
SC-18 Mobile Code	N/A
SC-19 Voice Over Internet Protocol	N/A
SC-20 Secure Name /Address Resolution Service (Authoritative Source)	N/A
SC-21 Secure Name /Address Resolution Service (Recursive or Caching Resolver)	N/A
SC-22 Architecture and Provisioning for Name /Address Resolution Service	N/A
SC-23 Session Authenticity	N/A
SC-24 Fail in Known State	N/A
SC-25 Thin Nodes	N/A
SC-26 Honeypots	N/A
SC-27 Platform Independent Applications	N/A
SC-28 Protection of Information at Rest	N/A
SC-29 Heterogeneity	N/A
SC-30 Concealment and Misdirection	N/A
SC-31	N/A

Requirement	Checks and Procedures
Covert Channel Analysis	
SC-32 Information System Partitioning	N/A
SC-34 Non-Modifiable Executable Programs	N/A
SC-35 Honeyclients	N/A
SC-36 Distributed Processing and Storage	N/A
SC-37 Out-of-Band Channels	N/A
SC-38 Operations Security	N/A
SC-39 Process Isolation	N/A
SC-40 Wireless Link Protection	N/A
SC-41 Port and I/O Device Access	N/A
SC-42 Sensor Capability and Data	N/A
SC-43 Usage Restrictions	N/A
SC-44 Detonation Chambers	N/A

3.17 System and Information Integrity (SI)

Table 6 lists SI checks and procedures.

Table 6. System and Information Integrity Requirement Evaluation

Requirement	Checks and Procedures
SI-1 System and Information Integrity Policy and Procedures	N/A
SI-2 Flaw Remediation	Examine the output from the <code>show version</code> command to determine the specific software release used by the device. Determine if the vendor has announced recommended patches, bug fixes, upgrades, or end-of-life/end-of-sale notifications for these releases.
SI-3 Malicious Code Protection	N/A
SI-4	N/A

Requirement	Checks and Procedures
Information System Monitoring	
SI-5 Security Alerts, Advisories and Directives	N/A
SI-6 Security Function Verification	N/A
SI-7 Software, Firmware, and Information Integrity	N/A
SI-8 Spam Protection	N/A
SI-10 Information Input Validation	N/A
SI-11 Error Handling	N/A
SI-12 Information Output Handling and Retention	N/A
SI-13 Predictable Failure Prevention	N/A
SI-14 Non-Persistence	N/A
SI-15 Information Output Filtering	N/A
SI-16 Memory Protection	N/A
SI-17 Fail-Safe Procedures	N/A

4. References

1. Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*.
2. FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.
3. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.
4. NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.
5. NIST SP 800-54, *Border Gateway Protocol Security*.
6. Systems Defense Information Agency (DISA) Secure Technical Implementation Guide (STIG) *Infrastructure Router Cisco* Version 8, Release 9, January 12, 2012,
7. DISA STIG *L2 Switch Cisco*, Version 8, Release 3, January 11, 2012,
8. DISA STIG *L3 Switch Cisco*, Version 8, Release 9, January 12, 2012.
9. Center for Internet Security (CIS) *Security Configuration Benchmark For Cisco Firewall*.
10. CIS *Cisco IOS Benchmark*.

5. List of Acronyms

Acronym	Definition
3DES	Triple Data Encryption Standard
AAA	Authentication Authorization and Accounting
AC	Access Control
ACL	Access Control List
ARP	Address Resolution Protocol
ASA	Adaptive Security Appliance
AT	Awareness and Training
AU	Audit and Accountability
AUX	Auxiliary
BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Unit
BSD	Berkeley Software Distribution
CDP	Cisco Discovery Protocol
CM	Configuration Management
CNS	Cisco Networking Service
CON	Console
CP	Contingency Planning
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DMZ	De-Militarized Zone
DoD	Department of Defense
DoS	Denial-of-Service
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IA	Identification and Authentication
IANA	Internet Assigned Number Authority
ICMP	Internet Control Message Protocol
IOS	Internetworking Operating System

Acronym	Definition
IP	Internet Protocol
IR	Incident Response
IS	Information Security
LLDP	Link Layer Discovery Protocol
M&O	Management & Operations
MA	Maintenance
MP	Media Protection
MS	Microsoft
N/A	Not Applicable
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
PE	Physical and Environmental Protection
PL	Planning
POC	Point of Contact
POTS	Plain Old Telephone Service
PS	Personnel Security
RA	Risk Assessment
RO	Read Only
RW	Read-Write
SA	System and Services Acquisition
SC	System and Communications Protection
SDD	System Design Document
SI	System and Information Integrity
SME	Subject Matter Expert
SNMP	Simple Network Management Protocol
SP	Special Publication
SSH	Secure Shell
SSP	System Security Plan
STIG	Security Technical Implementation Guide
STP	Spanning-Tree Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network

Acronym	Definition
VTP	VLAN Trunking Protocol
VTY	Virtual TTY
WAP	Wireless Access Point

Unix Security Control Assessment Guide

The views, opinions and/or findings contained in this guide are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Approved for Public Release: 19-3536.
Distribution Unlimited.

©2019 The MITRE Corporation. All rights reserved.

Author(s): Nathan Adams
Jim Finegan

September 2015

McLean, VA

MITRE

This page intentionally left blank.

Table of Contents

1. Overview	1
1.1 Caveats	1
1.2 Assessment Methodology	2
1.2.1 Phase 1: Planning	2
1.2.2 Phase 2: Assessment	2
1.2.3 Phase 3: Reporting	2
2. Assessment Activities	3
2.1 Phase 1: Planning	3
2.2 Phase 2: Assessment	3
2.2.1 Architecture Review	3
2.2.2 Documentation Review	3
2.2.3 Interviews	4
2.2.4 System Configuration Review	4
2.3 Phase 3: Reporting	4
3. Assessing Security Controls	5
3.1 Access Control (AC)	5
3.2 Awareness and Training (AT)	13
3.3 Audit and Accountability (AU)	13
3.4 Security Assessment and Authorization (CA)	16
3.5 Configuration Management (CM)	16
3.6 Contingency Planning (CP)	18
3.7 Identification and Authentication (IA)	18
3.8 Incident Response (IR)	20
3.9 Maintenance (MA)	20
3.10 Media Protection (MP)	20
3.11 Physical and Environmental Protection (PE)	20
3.12 Planning (PL)	20
3.13 Personnel Security (PS)	20
3.14 Risk Assessment (RA)	21
3.15 System and Services Acquisition (SA)	21
3.16 System and Communications Protection (SC)	21
3.17 System and Information Integrity (SI)	24
3.18 Program Management (PM)	26

4. References.....	1
5. Acronyms.....	2

List of Tables

Table 1. Access Control Requirement Evaluation	5
Table 2. Audit and Accountability Requirement Evaluation	13
Table 3. Configuration Management Requirement Evaluation	16
Table 4. Contingency Planning Requirement Evaluation	18
Table 5. Identification and Authentication Requirement Evaluation	19
Table 6. System and Communications Protection Requirement Evaluation	21
Table 7. System and Information Integrity Requirement Evaluation.....	24

This page intentionally left blank.

1. Overview

This *UNIX Security Control Assessment Guide* is intended to serve as a practical guidance for information security (IS) engineers who conduct network infrastructure security control assessments for systems that must meet federal guidance. This guide focuses on testing and evaluation techniques for technical controls required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. Parameters defined in this guide are considered industry best practice but may be modified by the organization as required. These controls include both technical configuration items and Management & Operations (M&O) policies and procedures.

The NIST 800-53 contain a broad set of required security standards; however, this guide will only address those controls and sub-controls that are related to the UNIX (Solaris) Operating System (OS) from the technical configuration perspective.

The guide also references the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) developed for the Department of Defense (DoD). Where there are no specific organization recommendations for a particular parameter setting, the STIG setting will be used. The STIGs provide detailed settings for UNIX configurations and are used as a security authority for UNIX, along with the Center for Internet Security (CIS) and Sun Microsystems/Oracle. These three authorities are recognized by the National Checklist Program (NCP), defined by the NIST SP 800-70, as the repository of publicly available security checklists (or benchmarks) that provide detailed low-level guidance on setting OS and application security configurations. Where there are no specific organization recommendations for a particular parameter setting, the STIG setting will be used.

1.1 Caveats

The controls presented here are for a Federal Information Processing Standard (FIPS) 199 Moderate rated system. Thus, controls for Low and High rated systems may differ.

This guide focuses on Solaris UNIX OS versions 10-11, but there are many similarities between these versions and version 12. Additionally, the concepts behind the requirements, checks and procedures in the guide are equally applicable to other UNIX-like operating systems such as Linux. The guide assumes the UNIX Security Evaluators have an understanding of the Solaris UNIX OS. The UNIX Evaluators should be familiar with implementing configurations on the Solaris UNIX OS using the command line interface and understand both internal and external considerations when assessing a security control. For completeness, the guide presents the technical assessment configurations and checks, along with operational and management control assessment to provide an overall security posture for the UNIX OS. The guide agrees with some settings on Solaris UNIX OS that are enabled or disabled by default.

As a practical guide, the security assessment includes a detailed review of the Solaris UNIX technical test output that includes OS command outputs. The UNIX technical test output provides a technical reference that should be combined with examination of system documentation and interviews with the UNIX System Administrators (SysAdmins) and

security staff whose roles and responsibilities include providing adequate security for the Solaris UNIX OS. The types of tests and analysis documented in this guide for Solaris UNIX OS can be used as a reference when establishing testing guidance for other operating systems.

1.2 Assessment Methodology

The following sections define the three-phase assessment methodology on which the guide is based.

1.2.1 Phase 1: Planning

The first phase, Planning, defines the assessment's scope, identifies goals, sets boundaries, and identifies assessment activities. This phase, as well as subsequent phases, requires the coordination of all involved parties. During this phase, the Evaluation Team reviews all security policies and procedures in accordance with Organization security requirements. The team will then create assessment scenarios and premises and define assessment agreeable terms as approved by the organization.

1.2.2 Phase 2: Assessment

Phase 2 may have several steps that depend on the assessment's objectives, scope, and goals as set forth in the Planning Phase. These steps can be grouped by the nature of the activities involved. These activity groups are as follows:

- **Information Collection**—thorough research must be performed against the target system/application before any meaningful assessment can be conducted. Data gathered is analyzed as the assessment proceeds and when the assessment is complete. Prior to the assessment, pre-assessment planning requests for information/artifacts will need to be made in order to have an accurate understanding of the testing environment and to properly prepare for the assessment.
- **Enumeration**—activities that provide specific information about assessment targets. This information is often collected using appropriate software tools.
- **Testing and Review**—activities that typically involve both the automated testing of security vulnerabilities via software tools and the evaluation of particular aspects of the organization's security policies and practices by Assessment Team members.

1.2.3 Phase 3: Reporting

Phase 3, Reporting, documents the soundness of the implemented security controls and consolidates all findings into the final output. This output includes reports that provide a summary of key findings and actionable recommendations, as well as provisions for all information derived from the assessment.

2. Assessment Activities

The activities are grouped by Planning, Assessment, and Reporting phases.

2.1 Phase 1: Planning

The UNIX Evaluator reviews the *Security Assessment Test Plan* to understand the assessment's scope. Based on the scope, security policies and procedures are reviewed in accordance with organization security requirements. As system documentation is received, the UNIX Evaluator will review the documents to ensure he/she has full knowledge of the system to be assessed and the components for which they are responsible for evaluating during the Assessment Phase. The Evaluator will determine any technical scripts or other requests to be made to ensure that the onsite assessment runs smoothly. During this time, any special testing requests are provided to the Lead Evaluator so the Evaluator can contact the system's point of contact (POC) and organization facilitator to ensure all test requirements are complete. The UNIX Evaluator will then create assessment scenarios, update the testing strategy, review technical guidance, and establishes technical testing requirements. Identify and plan the assessment with knowledge provided that includes Internet Protocol (IP) addresses mapped to hardware and software. Prepare port and vulnerability scanning procedures using the most current versions of tools. Prepare UNIX profiles in the vulnerability scanner with the information obtained from documentation and meeting requests, which may include SysAdmin credentials while running the vulnerability scans. Credentials are requested by the assessor but are not absolutely necessary. Request local administrator assistance in placing the scanning device in the proper zones to scan the target hosts interfaces. The interfaces to scan will be determined and verified upon the receipt of the command-line audit tool output.

2.2 Phase 2: Assessment

The following activities are performed during the Assessment Phase documentation review, Configuration review, and Interviews.

2.2.1 Architecture Review

Review documentation provided that depicts the implemented system design for compliance with the architecture requirements as documented in the System Security Plan (SSP) or other organization documents.

2.2.2 Documentation Review

The Evaluator will review documents provided by the organization. The review will assess whether the system documentation adequately describes implemented security controls and augments technical security control implementations. As a part of the assessment, the Assessment Team will evaluate documentation such as but not limited to, the System Security Plan (SSP), Risk Assessment (RA), and Contingency Plan, in accordance with organization guidelines and provide feedback.

2.2.3 Interviews

The OS Administrator interview will be conducted with both the UNIX Evaluator and the M&O Evaluator present. The UNIX Evaluator will focus on the processes and procedures for installing, supporting, and maintaining the operating systems, including secure baseline installation, access control, identification and authentication, backup and restoration, flaw remediation, and use of antivirus products. The technical questions serve to provide more in-depth analysis for certain controls requiring additional scrutiny. Questions serve as a starting point only and based on the interview responses may lead to additional or more in-depth questions or information requests. The UNIX Evaluator documents any specific technology or components related questions.

2.2.4 System Configuration Review

The Evaluator must analyze the OS configuration to determine the security posture of the OS.

2.3 Phase 3: Reporting

The UNIX Evaluator documents all weaknesses following organization reporting procedures and forwards to the Lead Evaluator for consolidation and discussion during the out-briefs. The UNIX Evaluator should discuss any Moderate or High findings with OS support staff so that the out-brief is not the first time staff are exposed to the finding and the supporting evidence.

It is during this phase that the UNIX Evaluator also reviews any closure evidence, if provided. If the closure evidence is found to satisfy the requirement to close the finding, the status of the finding is changed; however, it will still appear on the report as a closed finding. The Reporting Phase includes documentation of the implemented security controls soundness. The actual findings are consolidated into a final report.

3. Assessing Security Controls

Section 3 outlines a list of the security controls specified in NIST 800-53 and the corresponding checks and procedures used to verify the Solaris UNIX OS is in compliance. Checks and procedures entries of “N/A” indicate the security control does not have an applicable technical test to be conducted. These controls will be tested in other assessment areas by other members of the Evaluation Team.

3.1 Access Control (AC)

Table 1 lists AC checks and procedures.

Table 1. Access Control Requirement Evaluation

Requirement	Checks and Procedures
AC-1 Access Control Policy and Procedures	N/A
AC-2 Account Management	1. Disable default system accounts. a. Verify that unnecessary system accounts are locked by configuring an invalid shell (prevents su). i. Set the shell for SYSTEM accounts except ROOT to an INVALID shell (i.e. not active in <code>/etc/shells</code>). b. Renaming active default accounts are not recommended for Solaris. c. Verify that system accounts except for root have their passwords locked in <code>/etc/shadow</code>. Investigate further system accounts that are not locked. 2. Require the use of unique and separate administrator accounts for administrator and non-administrator activities. a. Examine the <code>/etc/passwd</code>, <code>/etc/group</code>, and <code>/etc/shadow</code> files for inconsistencies that affect system integrity. b. Ensure UIDs and GIDs are consistent for privileges and repeatable across multiple hosts. c. System Administrative accounts should be assigned group membership. d. Ensure that the UID and GID of zero is assigned to the root user only. 3. Implement centralized control of user access administrator functions. a. Examine the OS and interview about Network Information Service (NIS, NIS+) and LDAP services usage and if utilized for account centralization. b. If accounts are updated manually or inputted in an ad-hoc manner, then it's possible that there are inconsistencies present in the implementation of UIDs and GIDs. 4. Regulate the access provided to contractors and define security requirements for contractors. a. Verify whether the assigned UID/GID for contractors is excessive, (in)active, and defined as a contractor type account. i. Does the password file contain identification of contractors? 5. Revoke employee access rights upon termination. Physical access and system access must be revoked immediately following employee termination.

Requirement	Checks and Procedures
	a. Analysis and interview questions can include procedures of terminated employee and any servers in any environment where remote access virtual private network (VPN) is used. b. Did the terminated employee have dedicated servers assigned and is there a process/procedure which the organization utilizes to scrub any access to these other hosts which may belong to the terminated employee? i. Applicable if remote access is possible and physical access has been denied. 6. Review information systems accounts every 365(L); 180(M); and 90(H) days. a. Can the organization provide documentation (reports, procedures) that validates the establishing; activating, modifying, reviewing, disabling, and removing accounts are being performed. b. Is the review of information system accounts procedure scheduled for periodic review and verified against another document that identifies any changes to the organization personnel (whether voluntary or involuntary)? c. Are there instances when the review is done on an ad-hoc basis (whenever the need arises or situation warrants, surprise or scheduled audits)? d. Are automated mechanisms employed that support the management of information system accounts? i. Identify within the organization the group which performs this activity as part of their Roles and Responsibilities (R&R)? ii. Is there another facet of review that verifies if the management of accounts procedure is accurate and complete (e.g., review report sent to another pair of eyes that examines a bona-fide listing of employees/account names with the periodic review of system accounts)? iii. Does the procedure include any documentation (reports) that is generated and forwarded to another group or department for validation? e. Verify valid accounts on the OS by examining the inactivity/expiration settings and password change policy and documenting any accounts that do not meet policy. 7. Configure the information system to terminate temporary and emergency accounts automatically after one (1) hour of inactivity. a. Interview and review documentation that explains a process or a paper trail for adding temporary/emergency accounts. b. Examine Solaris OS and Identify temporary and emergency accounts. i. /etc/passwd contains information in the 5th field ii. Recommended practice would be to include information in the 5th field that displays "temporary/emergency" language. c. Solaris UNIX does not have hourly settings only daily d. /etc/shadow- Temporary/Emergency accounts should have an inactive=1(one day) value set. e. Integrity procedure would include if account management is done manually, are the accounts checked for accuracy by running the "pwck" command? 8. Review information system accounts every thirty (30) days.

Requirement	Checks and Procedures
	a. Is there documentation generated that determines the establishing, activating, modifying, reviewing, disabling, and removing information system accounts are being performed. b. Identify the department responsible for the monitoring of system accounts? c. Are there any reports/notifications produced? If so how are they collected? Who reviews the information? d. Are reviews conducted as a scheduled procedure? e. Who in the organization is the custodian for this information? 9. Review, track, and monitor privileged accounts/roles. a. Privileged roles include, for example, key management, network and system administration, database administration, web administration. b. See #8 (above) for evaluation of privileged account procedures. 10. Employ automated mechanisms to support the management of information system accounts. a. Describe the process of the automated mechanism(s) for account management? b. Is there a plan to meet this control if the primary mechanism is not available? c. Examine OS to identify and confirm the possible utilities (services) that perform this control? d. Examine a report that displays this control in action? 11. Configure the information system to terminate temporary and emergency accounts automatically after fifteen (15) minutes of inactivity. a. UNIX does not have hourly settings only daily b. <code>/etc/shadow</code> - Temporary/Emergency accounts should have an <code>inactive=1</code> (one day) value set. 12. Configure the information system to disable inactive accounts automatically after 365(L); 180(M) and 90(H) days. a. <code>/etc/shadow</code> should have the <code>inactive = 365(L); 180(M) 90(H)</code> days value set for all user accounts. 13. Employ automated mechanisms to inspect user account creation, modification, disabling, and termination. a. Ensure the automated mechanism notifies appropriate personnel of the user account management actions. 14. Examine OS for ACTIVE audit services and configurations. a. <code>auditd</code> daemon; Examine <code>/etc/security/audit_control</code> for the applicable flags and <code>naflags "am, ad"</code>.
AC-3 Access Enforcement	1. Examine OS for implementations of Encryption (FIPS 140-2) 2. Cryptographic Library has moved away from MD5 based hashes to secure hash a. <code>/etc/security/policy.conf</code> & <code>/etc/security/crypt.conf</code> i. <code>CRYPT_DEFAULT=5</code> or <code>6</code> (the new password is encrypted with the <code>crypt_sha256</code> algorithm or the <code>crypt_sha512</code> algorithm) ii. <code>CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6</code> iii. Only one <code>CRYPT_ALGORITHMS_ALLOW</code> or <code>CRYPT_ALGORITHMS_DEPRECATED</code> value can be specified. Whichever is listed first in the file takes precedence. iv. The algorithm specified for <code>CRYPT_DEFAULT</code> must either be specified for <code>CRYPT_ALGORITHMS_ALLOW</code> or not be specified for <code>CRYPT_ALGORITHMS_DEPRECATED</code>.

Requirement	Checks and Procedures
	v. <code>CRYPT_ALGORITHMS_DEPRECATED</code> - Specifies the algorithm for new passwords that is to be deprecated. For example, to deprecate use of the traditional UNIX algorithm, specify <code>CRYPT_ALGORITHMS_DEPRECATED= unix</code> and change <code>CRYPT_DEFAULT</code> to another algorithm, such as <code>CRYPT_DEFAULT=1</code> for BSD and Linux MD5 vi. If <code>CRYPT_DEFAULT</code> is not specified, the default is <code>_unix</code>. b. PKGINST: <code>SUNWn2cp</code> i. UltraSPARC-T2 Crypto Provider (SunSSH With OpenSSL PKCS#11 Engine Support FIPS 140-2 hardware crypto acceleration of symmetric crypto algorithms which is important to the data transfer speed) c. Interview and review documentation (if applicable), for Crypto Accelerator software card and firmware updates. i. Identify Crypto Accelerators devices (<code>/dev/ncp0</code>) d. Interview (if applicable), if there is a procedure for PKCS #11 interface to generate self-signed certificate(s) and access to the key store through the use of the Solaris cryptographic framework. e. Applications should not use <code>crypt()</code> to store or verify user passwords but should use the functions described on <code>pam(3PAM)</code> instead. 3. SSH Configuration. a. SUN SSH (<code>openssh</code>) – Verify SSH Packages installed b. Uncomment Protocol 2 (<code>/etc/sshd_config</code>) i. Ensure SSH Protocol version 1 and Protocol version 1 compatibility mode is not used c. <code>RSAAuthentication yes</code> (Digital certificates) d. F-Secure/SSH Tectia offer different configurations analysis e. <code>X11Forwarding</code> (default is “yes”) i. X11 forwarding should be disabled unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. 4. PAM Configurations for the stack a. <code>pam_deny</code>– PAM authentication, account, session and password management PAM module to deny operations b. Disallowing SSH authentication and any services not explicitly defined c. Remove all of the lines that include <code>rhosts_auth.so.1</code> d. Password-History PAM Module : PAM Module implementing password-reuse-prevention via “history” mechanism, for use with local password files 5. MOUNT Options for partitions a. File systems on the Solaris servers mount options that prevent device and suid files from being created on common temp partitions. 6. Restricted Root Access to the Console a. Check for any entries in <code>SULOG</code> that exist for root other than the console b. <code>CONSOLE=/dev/console /etc/default/login</code> is not commented.

Requirement	Checks and Procedures
	i. Enhance accountability of administrative access, direct logon to the root account should be denied. This configuration forces users to login to their account and use the su command to access root. Root can still be accessed directly at the system console c. Identify if root has logged in over the network and sshd is not running 7. OS requires strong I&A, with encryption for password and data, for all remote accesses (access from other than the system console) 8. Checksum (cksum) file permissions - (No World access) and should be set to "ON" and contain "sha256" algorithm. 9. Check Permissions on User Home Directories - ensure user home directories have initial permissions of 700, and never more permissive than 750. 10. Ensure all network daemons have permissions of 755, or more restrictive 11. Ensure all system commands have permissions of 755, or more restrictive. 12. (/etc, /bin, /usr/bin, /sbin, and /usr/sbin) 13. The /etc directory - houses most of the configuration and security files for Solaris 14. The /bin directory - home to all of the most used commands. 15. The /usr/bin is a standard directory on Unix-like operating systems that contains most of the executable files (i.e., ready-to-run programs) that are not needed for booting (i.e., starting) or repairing the system. There are more than 1900 executable files in /usr/bin on a typical system 16. The /sbin directory, whose contents include vital system utilities that are necessary before the /usr directory has been mounted (i.e., attached logically to the main filesystem). 17. The /usr/sbin directory contains non-vital system utilities that are used after booting (i.e., starting the system) by the system administrator. daemons - crond, pppd, sshd and xinetd. 18. Ensure all system log files have permissions of 640, or more restrictive. 19. Ensure all manual page files (i.e., files in the man and cat directories) have permissions of 644, or more restrictive 20. Ensure all system library files have permissions of 755, or more restrictive. 21. SNMP needs to have permissions of 700 or more restrictive 22. Default umask for Users has a default umask setting of 077 23. Ensure that the /etc/passwd file has permissions of 644, or more restrictive. 24. Audit data files have permissions of 640, or more restrictive. 25. Adequate permissions for the log files permissions are set 26. Verify if X11 connections and X11 forwarding are enabled and justified 27. Permissions of database directories and application files should be more restrictive 28. Disable vold - Solaris uses to mount floppies and CDs without root permissions. 29. ROOT HOME does not contain directories or files that are world writable 30. Ensure that the owner of all NIS/NIS+/yp files is root, sys, or bin
AC-4 Information Flow Enforcement	1. Examine OS and identify any LOCAL/REMOTE IP ADDRESS a. Analysis includes investigation of suspect IP Addresses present. 2. Identify misconfigurations in network configurations a. Resources of suspect IP Addresses include the "netstat output"; "Routing Tables: IPv4"; "TCP: IPv4/IPv6";

Requirement	Checks and Procedures
	"UDP" and "ifconfig" information as your source for System IP Addresses. b. Ensure that there are no duplicate hostnames with different IP Addresses listed. i. UNIX Clusters/Farms ensure that the <code>etc/hosts</code> file contains accurate IP Addresses on each server - note any discrepancies. c. VERIFY accurate network security settings: NDD d. VERIFY default gateway e. VERIFY if server is behaving as a router f. NFS client/server existence and connectivity g. Unnecessary Services – offline – and Monitoring h. Buffer overflows (executable stack) i. Is Syslog on LOCAL servers prevented from accepting messages from network (except for Central Log Server)? i. Change <code>LOG_FROM_REMOTE=syslogd</code> to <code>LOG_FROM_REMOTE=NO</code> ii. check for <code>LISTEN</code> on UDP 514 3. Identify usage of segregation of traffic and data flows to applicable zones. a. Examine the "ifconfig" output and determine if the interfaces are configured to allow separation of information and security processes on separate interfaces. Correlate to the netstat output – Identify services that accept connectivity on all interfaces. Example - <code>sshd port 22 LISTEN *.*.</code> b. Separation of APPLICATION DATA- SECURITY - BACKUP – MANAGEMENT Interfaces. 4. TCP wrappers support for services. a. SUNWtcpd Package Check– The <code>tcpd</code> program implements TCP wrappers. b. Examine <code>/etc/hosts.allow</code>, (daemon,client) pairs that are granted access. c. Examine <code>/etc/hosts.deny</code>, (daemon,client) pairs that are denied access.
AC-5 Separation of Duties	1. Are there separate roles and responsibilities (R&R) for Security staff and System Administration? a. Check <code>/etc/groups</code> and <code>/etc/user_attr</code> for Security/Audit like role(s) and membership. b. Examine the Search PATH for Root, ensure that the current directory (.) does not exist. 2. Is Solaris Role Based Access Control (RBAC) implemented? a. Maintain a limited group of administrators with access based upon the users' roles and responsibilities. 3. Is there a tier system in place for access and resolution of system issues (i.e. availability, troubleshooting)? a. Ensure that information system support functions are divided among separate individuals. Production/Development Separation (Best Practices) 4. Describe and analyze the R&R workflows during testing functions? a. Ensure that information system testing functions (i.e. user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.
AC-6 Least Privilege	1. Examine the <code>root</code> account UID/GID settings and any account that shares root privileges 2. Examine <code>root</code> HOME Directory file contents and permissions

Requirement	Checks and Procedures
	3. Restrict the use of application and database accounts and management utilities to only authorized application and database administrators. a. Examine OS for application and database accounts and files obtained from world write files assembly and look for matches of (non)privileged accounts that have access to utilities and SUID/GID files on server. Ensure that permissions are adequate for Group(s). b. Verify that application and database accounts exist only on hosts that need to have those services 4. Examine all services that are active and identify any services that are enabled under privileged accounts and are not utilizing less privileged accounts 5. Examine <code>cron</code> configurations – and verify if the <code>cron</code> utilities are assigned restricted UIDs/GIDs and the scripts/utilities of the <code>crontabs</code> have secure permissions. 6. Review existing <code>crontab</code> files – Identify any that have zero (0) bytes. An empty file can occur if the <code>crontab</code> command with no option is typed and saved changes and exited the file. 7. Examine the <code>cron.deny</code> and <code>cron.allow</code> files for permissions and existence. 8. File ownership and permissions a. Identify and mitigate un-owned files b. Ensure that world writable directories will only be allowed if they are public directories and have the sticky bit set i. Public directories need to be owned by <code>root</code> or an application user ii. Public directories need to be group owned by <code>root</code>, <code>sys</code>, <code>bin</code>, <code>other</code> or an application group
AC-7 Unsuccessful Log-on Attempts	1. Examine the unsuccessful log on attempts settings for the Baseline a. Policy - Identify the number of consecutive, failed authentication attempts i. Analyze the <code>RETRIES</code> parameter b. Policy - Identify consecutive, unsuccessful authentication attempts allowed i. Analyze the <code>LOCK_AFTER_RETRIES</code> parameter c. Ensure logging is implemented for the <code>root</code> filesystem. d. Configured per-user in the <code>/etc/user_attr</code> file i. Analyze the <code>lock_after_retries=</code> parameter (NO only for ROOT) 2. For TIME Lockouts: a. Install the COMSpamll package and Configure PAM b. Identify the "login auth required pam_login_limit.so.1 count_limit=5 timeout_account=300" c. Identify the "other auth required pam_login_limit.so.1 count_limit=5 timeout_account=300" (<code>sshd.conf</code>) 3. LDAP implementation: Interview/examine if LDAP and <code>pam_ldap</code> is configured correctly. 4. Identify the <code>/var/adm/loginlog</code> file (600/Perms.-Group SYS). 5. Examine the <code>/etc/default/login</code> file: a. <code>SYSLOG=YES</code> b. <code>SYSLOG_FAILED_LOGINS=0</code> (All failed logins are logged) 6. Identify the <code>/var/adm/authlog</code> file (600/Perms.-Group SYS). a. Verify that "auth.notice" <TAB> <code>/var/adm/authlog</code> exists.

Requirement	Checks and Procedures
AC-8 System Use Notification	1. Configure the information system to display a warning banner automatically prior to granting access to potential users. 2. Examine /etc/issue a. /etc/issue 3. SSH – Examine “Banner” a. /etc/issue 4. Examine organization control for System Use Notification compliance.
AC-9 Previous Logon (Access) Notification	1. This functionality is not available for users, except ROOT logins (DEFAULT) at the console. 2. SSH - The "PrintLastLog" setting - (/etc/ssh/sshd_config) specifies whether sshd should display the date and time when the user last logged in.
AC-10 Concurrent Session Control	N/A 1. SOLARIS CAN ONLY LIMIT THE TOTAL # OF SESSIONS, NOT INDIVIDUAL OR CONCURRENT SESSIONS TO THE SERVER 2. SSH: There is no built-in functionality to limit the number of concurrent sessions for a user to a single session.
AC-11 Session Lock	Applicable only if a Common Desktop Environment (CDE) is in place 1. CDE - Set Default Screen Lock for CDE Users (Security Policy in Organization) that reflects that the default timeout is 30 minutes of keyboard/mouse inactivity before a password-protected screen saver is invoked by the CDE session manager. 2. SSH – can abandon login sessions if no input is done a. Uncomment TIMEOUT=900 in /etc/default/login
AC-12 Session Termination	Ensure the system is configured to terminate remote sessions after a defined level of inactivity.
AC-14 Permitted Actions without Identification or Authentication	1. Insecure transmission protocols a. LDAP and R-utilities 2. Identify files that have no user a. Look for world/other write-execute permissions 3. Identify files that are world/group writeable a. Look for world/other write-execute permissions on files that have system capabilities. 4. Identify NFS server-related daemons – Examine the NFS mounts in /etc/dfs/dfstab and ensure permissions are secure and anonymous access has authentication enabled 5. Review unnecessary services enabled on server
AC-16 Security Attributes	N/A
AC-17 Remote Access	1. Interview System Administrators about their remote access capabilities and procedures. a. Include end to end tools utilization for access to the servers b. Identify any configurations which exempt the remote access workflow. i. Contractors, consultants, and 3rd party support
AC-18 Wireless Access Restrictions	N/A
AC-19 Access Control for Mobile Devices	N/A
AC-20 Use of External Information Systems	N/A
AC-21 Information Sharing	N/A

Requirement	Checks and Procedures
AC-22 Publicly Accessible Content	N/A
AC-23 Data Mining Protection	N/A
AC-24 Access Control Decisions	N/A
AC-25 Reference Monitor	N/A

3.2 Awareness and Training (AT)

There are no UNIX specific checks and procedures for these controls.

3.3 Audit and Accountability (AU)

Error! Reference source not found. lists AU checks and procedures.

Table 2. Audit and Accountability Requirement Evaluation

Requirement	Checks and Procedures
AU-1 Audit and Accountability Policy and Procedures	N/A
AU-2 Auditable Events	1. Ensure the audit service (<code>auditd</code>) is enabled on the server. 2. Examine OS for system audit configurations (audit events grouped into audit classes) for failed and/or successful audit events. a. Attributable events – Events that can be attributed to a user. b. Nonattributable events – Events that occur at the kernel-interrupt level or before a user is authenticated. c. Synchronous events – Events that are associated with a process in the system. d. Asynchronous events – Events that are not associated with any process. 3. Determine Audit Policy implementation and options. a. Public – Public objects are no longer audited for read-only events. b. Perzone – A separate audit daemon runs in each zone. c. Zonename – The name of the zone in which an audit event occurred can be included in audit records. d. Single audit service – for all zones. 4. Is the auditing system contents correctly configured for the required events for all users and root? 5. Analyze and examine the <code>/etc/security/audit_control</code> file: a. For the <code>audit_binfile.so</code> plugin and <code>p-</code> flags that creates binary audit files (the audit trail), and directory store. b. For the <code>audit_syslog.so</code> plugin and <code>p-</code> flags which filters selected audit records to the syslog 6. Analyze the IPFILTER rule sets and determine if <code>IPFILTERS</code> is installed and <code>ACTIVE</code> for logging. a. IP Filter is managed by the SMF services <code>svc:/network/ipfilter.</code> b. Examine (<code>/etc/ipf/ipf.conf</code>) for packet filtering rules that are loaded at boot time

Requirement	Checks and Procedures
	7. Examine the non-global zones and determine if per-zone auditing is implemented (i.e. customized audit configurations), determine that auditing is conducted and sufficient. 8. Interview – Who manages the selection of events to be audited by individual components of the information system? a. Is there a scheduled review to determine that auditing configurations for the OS? i. Every 365 days per organization guidance b. Identify audit setup on a system with zones – How is auditing disseminated to zones? c. Specifying the location of binary audit data: Are the audit logs stored locally on the system? d. Interview - Periodically review and update the list of auditable events.
AU-3 Content of Audit Records	1. Determine the ownership (System Administration or Security staff), and application of the auditreduce and praudit commands. (Solaris Basic Security Module). 2. Is there a procedure that enhances that capability of auditing additional events? 3. Verify that valid time-stamps for audit logs are supported. 4. Centrally manage the content of audit records generated by individual components throughout the system. a. Does Syslog include a Plugin (audit_remoteplugin) for transmission of UDP to Central Logging server? b. Is the syslog to central logging server on a dedicated/protected interface?
AU-4 Audit Storage Capacity	1. Is the audit storage capacity adequate? 2. Are there separate partitions for audit data? 3. Are their processes in place to avoid exceeding audit storage capacity? 4. What is the procedure if all the audit directories have reached the minfree threshold? 5. Ask the SA if audit logs and records are backed up onto a different system or offline media on at least a weekly basis.
AU-5 Response to Audit Processing Failures	1. Is the process in place that handles serious audit events alert/notifications, other than the console where audit capacity is being monitored? a. The audit_warn script. The script sends email to the audit_warn alias. b. Is the audit_warn script implemented? 2. Are Primary, secondary, and directory of last resort defined.
AU-6 Audit Monitoring, Analysis, and Reporting	1. Interview and examine documentation if the audit policy collects audit records in binary format, in syslog format, or in both formats 2. Are the "dmesg (system diag messages)" reviewed, reported, analyzed, and corrected? 3. Examine the /var partition. Identify the log files stored. Interview whether syslog text logs are stored on the /var partition with the binary audit files. The auditreduce command, which reads binary audit files, assumes that all files in an audit partition are binary auditfiles. 4. Examine the Warning Levels (emerg; alert; crit) configured in syslog and the destinations for logged events 5. Is a user or are multiple users' recipients of error messages at their consoles or workstations? 6. Describe the procedures and personnel who are responsible to investigations and reporting process for escalations.

Requirement	Checks and Procedures
	7. Describe and confirm on the OS the tools and procedures in place to review audit records. a. Who reviews the audit trails (The <code>praudit</code> command enables you to view the contents of binary audit files. You can pipe the output from the <code>auditreduce</code> command). b. Output from the <code>praudit</code> command has an additional output format, XML. Implemented? c. Describe schedule and output procedures of audit reviews d. What is the procedure if further investigations are needed or approved? 8. Who inspects administrator groups on demand but no less than once every thirty (30L - 14 M - 7 H) days to ensure unauthorized administrator accounts have not been created. 9. Describe procedures for organization to review/certify administrator accounts for validity, ownership, and existence. 10. Are automated mechanisms utilized for audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities? 11. Are automated mechanisms utilized to immediately alert security personnel of the following minimal examples of inappropriate or unusual activities with security implications: threats to infrastructure, systems or assets; threats to organization sensitive data; and threats to finances, personnel, or property? 12. Are automated mechanisms utilized for audit records review? 13. Are manual methods available for review (BINARY and SYSLOG) audit trails?
AU-7 Audit Reduction and Report Generation	1. Explain the process and procedures that include audit reduction, review, and reporting tools that support after-the-fact investigations of security incidents without altering original audit records. 2. Are consolidation, correlation, and detection of audit logs the solution? 3. Are the tools in place able to define and utilize selective criteria in generating audit reports? 4. Examine the OS for active services of the audit reduction and reporting.
AU-8 Time Stamps	1. Verify if Information system clock synchronization occurs daily and at system boot. 2. Examine the <code>/etc/inet/ntp.conf</code> file. a. As a Client: Uncomment <code>multicastclient 224.0.0.1</code> in IPv4 and <code>ff02::1</code> in IPv6 and at least one ntp server in the organization b. Server - internal NTP server address 3. Service enabled on Server: <code>svc:/network/ntp:default</code> (online) 4. Examine IPFILTER for port 123 pass in/ pass out; keep state rules 5. Examine the TZ (timezone) environment (env) variable. Time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. NTP uses UTC as reference time. 6. Crontab entry (<code>/usr/sbin/ntpdate</code>) 7. Arrange to have the Global Zone server included for analysis for any/all non-global zones in scope for the assessment
AU-9 Protection of Audit Information	1. Are automated mechanisms implemented that are restricted to hardware-enforced, "write-once" media for recording audit information (e.g., CD-R, not CDRW). a. Is the audit data protected so that access to it is limited to audit and accountability roles

Requirement	Checks and Procedures
	b. Examine the <code>cron</code> permissions or utilities that handle audit logs c. Is CD-RW - DVD-RW being utilized? d. How are audit logs accessed? e. Are they transferred to other hosts for analysis? f. Is there a chain of custody procedure in place to ensure confidentiality and integrity of audit logs?
AU-10 Non-Repudiation	N/A
AU-11 Audit Record Retention	1. Describe the audit log retention Policy? 2. Interview and examine documentation to determine if the organization retains audit records for ninety (90) days and archive old records for one (1) year to provide support for after-the-fact investigations of security incidents and to meet regulatory and organization information retention requirements. 3. What is the retention period for analyzing logs in real-time? 4. What is the retention policy for analyzing historical/archived logs?
AU-12 Audit Generation	1. By default, all events (Audit all successful attempts to log in and log out, and all failed attempts to log in) are audited for the system. 2. Examine pre-selected audit classes and ensure the following exist: a. <code>as</code> - System-wide administration b. <code>am</code> - Administrative actions 3. Interview and examine the auditreduce procedure and the praudit for audit collection and review. 4. Interview if there are 3rd party security utilities utilized in the audit class collection and review.
AU-13 Monitoring for Information Disclosure	N/A
AU-14 Session Audit	N/A
AU-15 Alternate Audit Capability	N/A
AU-16 Cross-Organizational Auditing	N/A

3.4 Security Assessment and Authorization (CA)

There are no UNIX specific checks and procedures for these controls.

3.5 Configuration Management (CM)

Table 5 lists CM checks and procedures.

Table 3. Configuration Management Requirement Evaluation

Requirement	Checks and Procedures
CM-1 Configuration Management Policy and Procedure	N/A

Requirement	Checks and Procedures
CM-2 Baseline Configuration	1. Do System Administrators have any role in creating/monitoring/updating the baseline configuration and system inventory documentation for changes? 2. Does the SA create and maintain a system baseline (all device files, all sgid and suid files, and system libraries and binaries), to include cryptographic hashes of files in the baseline. 3. Is the Hardware/Software Inventory documentation include a. The inventory of the information system must be verified that it includes information allowing unique identification of the system hardware and software (for example, manufacturer, type, serial number, version number, physical location and logical location within the system architecture).
CM-3 Configuration Change Control	N/A
CM-4 Security Impact Analysis	N/A
CM-5 Access Restrictions for Change	1. Explain and identify your roles and responsibilities during change controls? 2. How is it decided that a change control has been successfully completed? 3. Are there any areas where independent contractors have access to the system and if so explain the procedure for granting access and completing the change(s)? 4. What is the procedure for removing access to contractors?
CM-6 Configuration Settings	1. Describe the process of configuring the OS security when implementing the resources that references vendors, organization, security authority's recommendations? 2. Is there a development/staging/test environment with security policy configurations applied that you can test patches- investigate performance issues – run and test security utilities? 3. How do system administrators determine that the system's security settings are configured to the most restrictive mode compatible with the system's operational requirements? 4. Are there other authorities that are screened for applicability concerning security for the OS? 5. Who is responsible for approving and monitoring the authorized security services on the servers? 6. Are there tools and procedures available to verify the current and archived versions of configuration settings for the system?
CM-7 Least Functionality	1. Have all active services been configured to operate under the least privileged account? 2. What processes or procedures are in place or followed that verifies that the information system is configured to prohibit and restrict the use of functions, ports, protocols, and/or services? 3. Has the system imposed system minimalization. 4. Excessive SUID/SGID on system
CM-8 Information System Component Inventory	1. Does the organization provided documentation depict an accurate-detailed component inventory for the system?
CM-9 Configuration Management Plan	N/A
CM-10 Software Usage Restrictions	Determine if the organization have software usage restrictions on the system?

Requirement	Checks and Procedures
CM-11 User-Installed Software	Determine if the organization has restrictions for user-installed software on the system?

3.6 Contingency Planning (CP)

Table 4 lists CP checks and procedures.

Table 4. Contingency Planning Requirement Evaluation

Requirement	Checks and Procedures
CP-1 Contingency Planning Policy and Procedures	N/A
CP-2 Contingency Plan	N/A
CP-3 Contingency Training	N/A
CP-4 Contingency Plan Testing and Exercises	N/A
CP-6 Alternate Storage Site	N/A
CP-7 Alternate Processing Site	N/A
CP-8 Telecommunications Services	N/A
CP-9 Information System Backup	1. Full weekly backups are performed. 2. Daily incremental and differential backups are performed. 3. Backups are stored offsite. 4. Onsite and off-site backup media are logged with name, date, time, and action.
CP-10 Information System Recovery and Reconstitution	N/A
CP-11 Alternate Communications Protocols	N/A
CP-12 Safe Mode	N/A
CP-13 Alternative Security Mechanisms	N/A

3.7 Identification and Authentication (IA)

Table 5 lists IA checks and procedures.

Table 5. Identification and Authentication Requirement Evaluation

Requirement	Checks and Procedures
IA-1 Identification and Authentication Policy and Procedures	N/A
IA-2 User Identification and Authentication (Organizational Users)	1. Verify if the system uses multifactor authentication for access to the servers. 2. Examine the server's system messages and <code>/etc/groups</code> for accounts and groups that bypass the multifactor authentication. These accesses most likely rely on the traditional UNIX UID/Password for authentication. 3. Examination of the <code>sudo</code> entries for user-user authentication. 4. Confirm with the SA, if shared accounts exists and what precautions are utilized to prevent accessing shared accounts 5. Identify any <code>".netrc"</code> and <code>".rhosts"</code> files 6. What are the security options for authenticating NFS mounts and subsequent accesses?
IA-3 Device Identification and Authentication	N/A
IA-4 Identifier Management	1. Are common device identifiers disabled after 365 (L), 180(M), and 90(H) days of inactivity? 2. "ifconfig" look for interfaces configurations (<code>netstat - Routing Table - TCP/IP LISTEN-Established</code> and match against <code>/etc/hosts</code>). 3. Document and verify "INACTIVE" interface(s).
IA-5 Authenticator Management	1. Are passwords protected from disclosure, leakage, or modification when stored or transmitted 2. Ensure password fields are Not Empty 3. Check for the <code>PASSREQ=YES</code> setting in <code>/etc/default/login</code> 4. Force users to select a password comprising a minimum of eight (8) alphanumeric and/or special characters a. <code>MINALPHA=8</code> (Password must contain at least this number of alpha characters.) 5. Automatically force users (including administrators) to change account and system account passwords every sixty (60) days. a. <code>MAXWEEKS= 8</code> (<code>MAXWEEKS</code> specifies the maximum time period for which a password is valid. The <code>MAXWEEKS</code> value can be overridden by entries in the <code>/etc/shadow</code> file. 6. Automatically force users to select one (1) unique password prior to reusing a previous one a. <code>MINDIFF=1</code> (The old and new passwords must differ by at least the <code>MINDIFF</code> value.) 7. Enforce password lifetime restrictions within a minimum of one (1) day and maximum of sixty (60) days. a. <code>MINWEEKS=1</code> and <code>MAXWEEKS= 8</code>. The <code>MINWEEKS</code> value can be overridden by entries in the <code>/etc/shadow</code> file. 8. Automatically force users to select six (6) unique passwords prior to reusing a previous one. a. <code>MINDIFF=6</code> 9. Dictionary word checking of passwords a. <code>DICTIONDBDIR=/var/passwd</code> (defined- If the password database does not yet exist) b. <code>DICTIONLIST=/...</code> (dictionary files) 10. PAM – Disable access using a nonpassword-based program a. Grep "pam_rhosts_auth.so.1" in the <code>/etc/pam.conf</code> file. b. Verify if <code>svc:/network/login:rlogin</code> is enabled

Requirement	Checks and Procedures
	c. Verify if <code>svc:/network/shell:default</code> is enabled d. If an entry for the client exists in both <code>/etc/hosts</code> and <code>/etc/hosts.equiv</code> - then no prompt for password. e. Removing the <code>pam_rhosts_auth.so.1</code> entry will disable the <code>/etc/hosts.equiv</code> and <code>~/.rhosts</code> authentication protocol and the user would always be forced to type the password.
IA-6 Authenticator Feedback	N/A
IA-7 Cryptographic Module Authentication	1. Verify vulnerability scan outputs 2. Verify validated cryptography implementation 3. SSH and system supported applications
IA-8 Uniquely Identify and Authenticate (Non- Organizational Users)	N/A
IA-9 Service Identification and Authentication	N/A
IA-10 Adaptive Identification and Authentication	N/A
IA-11 Re-authentication	N/A

3.8 Incident Response (IR)

There are no UNIX specific checks and procedures for these controls.

3.9 Maintenance (MA)

There are no UNIX specific checks and procedures for these controls.

3.10 Media Protection (MP)

There are no UNIX specific checks and procedures for these controls.

3.11 Physical and Environmental Protection (PE)

There are no UNIX specific checks and procedures for these controls.

3.12 Planning (PL)

There are no UNIX specific checks and procedures for these controls.

3.13 Personnel Security (PS)

There are no UNIX specific checks and procedures for these controls.

3.14 Risk Assessment (RA)

There are no UNIX specific checks and procedures for these controls.

3.15 System and Services Acquisition (SA)

There are no UNIX specific checks and procedures for these controls.

3.16 System and Communications Protection (SC)

Table 6 lists SC checks and procedures.

Table 6. System and Communications Protection Requirement Evaluation

Requirement	Checks and Procedures
SC-1 System and Communications Protection Policy and Procedures	N/A
SC-2 Application Partitioning	1. Examine documentation (network diagrams) for architecture a. Verify placement of UNIX hosts with organization compliant architecture 2. Identify Global and Non-Global zones. a. Services that are in Maintenance Mode can be the result of destructive system misconfiguration and partitions (e.g. NFS) can be in a failed state. 3. Examine IP Filters configurations a. Solaris zones IP Filter is now able to filter communication occurring over the loopback interface b. loopback interface for non-global zones
SC-3 Security Function Isolation	1. Identify hardware separation mechanisms to facilitate the isolation of security functions. a. Central SYSLOG Server/ Remote auditing services b. Solaris ZONES isolation (#dladm show-link -Z and concentrate on LINK-ZONE-CLASS-MTU-STATE-OVER information that identifies server interfaces) (HIGH) c. Security/Data/Management/Backup (Separate NICs for traffic) 2. Isolate security functions from non-security functions. a. Security dedicated interface for SSH - isolated from other traffic
SC-4 Information in Shared Resources	1. NIST Special Publication 800-88: Guidelines for Media Sanitization 2. Interview about account creation procedure – focus on the organization's avoidance of reusing the UIDs from deleted accounts. 3. If applicable, check whether Oracle/Sun provided device-clean scripts are applied to: a. cartridge tape drives (st_clean device-clean script) b. diskette drives (fd_clean script) c. CD-ROM drives (sr_clean script) d. audio devices (audio_clean script)
SC-5 Denial-of-Service Protection	1. Vulnerability scans (identify rogue ports and scan outputs) 2. Missing patches (check advisories for current vulnerabilities CVE) 3. Set the maximum number of incoming connections

Requirement	Checks and Procedures
	a. <code># ipadm set-prop -p _conn_req_max_q0=4096 tcp</code> b. Verify: <code>tcp _conn_req_max_q0 rw 4096</code> 4. IP Tunable Parameters a. <code>_respond_to_echo_broadcast</code> - Default 1 (enabled) Change to 0 (disabled)
SC-6 Resource Priority	N/A
SC-7 Boundary Protection	1. Physically allocate publicly accessible information system components with the organization reference system network diagrams a. Limit the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic. b. Are the interfaces managed and traffic flow reviewed every 365 days? 2. Scan target APP-DATA Zones servers from organization internal LAN to verify port blockage 3. Ensure that all network traffic is denied through packet screening rules, except for those hosts, ports, and services that are explicitly required. a. Examine <code>IPFILTERS</code> analysis and TCPIP services b. Are managed interfaces denying network traffic by default and allowing network traffic by exception (i.e., deny all, permit by exception)? 4. Prevention of remote connections from established non-remote connection would include an interview question concerning remote access through VPN and physical devices utilized (Example: provided hardened laptop from organization).
SC-8 Transmission Confidentiality and Integrity	1. Unnecessary administrative and monitoring Graphical User Interface (GUI) services enabled on the Solaris 10 servers. a. Solaris Management Console (SMC) b. X11 forwarding i. The Solaris password security for these servers implement a stronger crypt module than the required (<code>CRYPT_DEFAULT= unix</code>) and less secure default algorithm needed for the SMC. Therefore, authentication to the SMC cannot work with the current configuration. c. Ensure that IP forwarding and IP dynamic routing are disabled 2. IPSEC security association implementation a. <code>svc:/network/ipsec/ike</code> (IPSEC service) b. <code>svc:/network/ipsec/policy</code> (IPSEC Policy) c. <code>svc:/network/ipsec/ike:default</code> (Auto keys create) d. <code>svc:/network/ipsec/manual-key:default</code> (Manual keys create) 3. Enable IP strict destination multihoming a. <code>ndd -set /dev/ip ip_strict_dst_multihoming 1</code> 4. Serial telecommunications: Solaris PPP 4.0 implements the Point-to-Point Protocol (PPP) a. MS-CHAPv1 and MS-CHAPv2 authentication (insecure for confidentiality) b. Interview about all possible dial-(in-out), leased DSL, modem connections. 5. Solaris Network Cache and Accelerator (NCA) Procedures a. The SSL kernel proxy supports the approved TLS implementation i. device name - <code>/dev/nca</code> ii. service - <code>svc:/network/ssl/proxy</code> b. The NCA service logs web activity i. binary file - <code>/var/nca/log</code>

Requirement	Checks and Procedures
SC-10 Network Disconnect	Ensure the system is configured to terminate remote sessions after a defined level of inactivity.
SC-11 Trusted Path	N/A
SC-12 Cryptographic Key Establishment and Management	- IPSEC security association implementation - svc:/network/ipsec/ike (IPSEC service) - svc:/network/ipsec/policy (IPSEC Policy) - svc:/network/ipsec/ike:default (Auto keys create) - svc:/network/ipsec/manual-key:default (Manual keys create)
SC-13 Cryptographic Protection	- Secure Shell (OpenSSH) - SSH Version 2 (v2) defined (/etc/ssh/sshd_config) - Sun Crypto Accelerator 6000 card utilized #cryptoadm list fips-140 (displays the status of FIPS mode - output is either enabled or disabled) - Oracle Solaris 11 bundled OpenSSL, FIPS Object Module support has been added.
SC-14 Public Access Protections	Determine configurations of the following: - Uneven file permissions for the following directories/files /etc, /bin, /usr/bin, /usr/sbin, /usr/usb, /sbin, and /usr/sbin
SC-15 Collaborative Computing Devices	N/A
SC-16 Transmission of Security Parameters	N/A
SC-17 Public Key Infrastructure Certificates	N/A
SC-18 Mobile Code	N/A
SC-19 Voice Over Internet Protocol	N/A
SC-20 Secure Name /Address Resolution Service (Authoritative Source)	N/A
SC-21 Secure Name /Address Resolution Service (Recursive or Caching Resolver)	N/A
SC-22 Architecture and Provisioning for Name /Address Resolution Service	N/A
SC-23 Session Authenticity	N/A
SC-24 Fail in Known State	N/A
SC-25 Thin Nodes	N/A

Requirement	Checks and Procedures
SC-26 Honeypots	N/A
SC-27 Platform Independent Applications	N/A
SC-28 Protection of Information at Rest	If required, ensure the system is configured to encrypt data at rest.
SC-29 Heterogeneity	N/A
SC-30 Concealment and Misdirection	N/A
SC-31 Covert Channel Analysis	N/A
SC-32 Information System Partitioning	If required, ensure the system is configured to separate data from the operating system functionality.
SC-34 Non-Modifiable Executable Programs	N/A
SC-35 Honeyclients	N/A
SC-36 Distributed Processing and Storage	N/A
SC-37 Out-of-Band Channels	N/A
SC-38 Operations Security	N/A
SC-39 Process Isolation	N/A
SC-40 Wireless Link Protection	N/A
SC-41 Port and I/O Device Access	N/A
SC-42 Sensor Capability and Data	N/A
SC-43 Usage Restrictions	N/A
SC-44 Detonation Chambers	N/A

3.17 System and Information Integrity (SI)

Table 7 lists SI checks and procedures.

Table 7. System and Information Integrity Requirement Evaluation

Requirement	Checks and Procedures
SI-1	N/A

Requirement	Checks and Procedures
System and Information Integrity Policy and Procedures	
SI-2 Flaw Remediation	1. What is the process/procedure and timeframe for newly released security relevant patches, service packs, and hot fixes installs on the information system? 2. What testing is accomplished before security relevant patches, service packs, and hot fixes on a production system? 3. Describe roles and responsibilities for conducting continuous security assessments to identify vulnerabilities in the information system within its operating environment? 4. Explain the process/procedure that captures all appropriate information pertaining to discovered flaws, including the cause of the information system flaws, mitigation activities, and lessons learned to identify necessary improvements in the flaw remediation process? 5. Is there a centralized patch management program to assist system administrators in identifying, acquiring, testing, and deploying patches? 6. Are specific parties are assigned responsibility and actions defined to ensure that flaw remediation for the information system is conducted correctly? 7. Are updates to the system automatically applied through vendor supplied patches? 8. Describe the patching test and evaluation methodology for your organization? Are the patches tested in a non-production environment? Is there an evaluation (regression test) conducted to the environment with the new patches?
SI-3 Malicious Code Protection	1. Ensure an antivirus product is installed and configured for real-time protection and monitoring 2. Ensure servers are configured to obtain antivirus software updates and virus code definitions from a centralized and automated source. 3. Ensure the antivirus product is configured to perform daily system scans and at boot time.
SI-4 Information System Monitoring	1. Is there any host intrusion detection systems (HIDS) implemented on the OS? 2. Who is assigned responsibility to ensure that intrusion detection tools and techniques are employed correctly within the information system? 3. Describe and explain process on whether ADMINS and Organization is capable of immediately investigating, reporting, and responding to suspicious activity in real-time?
SI-5 Security Alerts and Advisories	1. Describe your participation and roles/responsibilities with monitoring and receipt of system security alerts/advisories on a regular basis, issuing alerts/advisories to appropriate personnel, and taking appropriate actions in response? 2. Are the SysAdmins receiving security alerts/advisories and documenting any actions that were taken to include the date/time of the action? 3. Describe the SysAdmins capabilities of immediately reacting and responding to new security alerts and advisories? 4. Are security alerts and advisories are automatically disseminated to the appropriate personnel throughout the organization?
SI-6 Security Function Verification	N/A

Requirement	Checks and Procedures
SI-7 Software and Information Integrity (Moderate) Control	1. Examine system for Tripwire-BART-Solaris Fingerprint-ASET etc. 2. Is integrity verification software utilities implemented on the information system to look for evidence of information tampering, errors, and omissions? 3. Does the information system Integrity tool detect and protect against unauthorized changes to software and information consistently and on an ongoing basis? 4. Are Specific personnel assigned responsibility and specific actions defined to ensure that the information system detects and protects against unauthorized changes to software and information?
SI-8 Spam Protection	N/A
SI-10 Information Input Validation	N/A
SI-11 Error Handling	1. Verify X11(CDE) and SYSLOG appropriate error logs a. Syslog stored /var/adm directory b. /var/adm/messages for console messages c. Check /etc/syslog.conf for "err"; "alert"; "crit" and "emerg" logging configurations 2. Check crontab for core dump jobs/rotations 3. Auxiliary Consoles and persistent auxiliary consoles a. Check the # consadm (output) and # consadm -p b. Expected output includes: /dev/term/[a,b] 4. Check Application log locations a. Check the /etc/logadm.conf file for information about application logging. 5. Check service states - Failed services (Offline, Maintenance, uninitialized) in dependency order, whether they failed as the result of administrator error, software bug, or were affected by an uncorrectable hardware error. The dependency order is defined by dependency statements. a. Check /var/svc/log - service log files for a list of errors
SI-12 Information Output Handling and Retention	N/A
SI-13 Predictable Failure Prevention	N/A
SI-14 Non-Persistence	N/A
SI-15 Information Output Filtering	N/A
SI-16 Memory Protection	N/A
SI-17 Fail-Safe Procedures	N/A

3.18 Program Management (PM)

There are no UNIX specific checks and procedures for these controls.

4. References

1. Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*.
2. FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.
3. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.
4. NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.
5. National Security Agency (NSA) Guides to Secure Configuration
6. Various Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS) and Checklists.
7. U.S. National Institute of Standards and Technology Special Publication 800-88, *Guidelines for Media Sanitization*.

5. Acronyms

Acronym	Definition
AC	Access Control
ACL	Access Control List
ASET	Automated Security Enhancement Tool
AT	Awareness and Training
AU	Audit and Accountability
BART	Basic Audit Reporting Tool
BDPU	Bridge Protocol Data Unit
BSD	Berkley Software Distribution
CA	Security Assessment and Authorization (NIST 800-53 version 3)
CDE	Common Desktop Environment
CDP	Cisco Discovery Protocol
CIS	Center for Internet Security
CM	Configuration Management
CP	Contingency Planning
crit	critical
DBA	Database Administrator
DES	Data Encryption Standard
DISA	Defense Information Systems Agency
DMZ	De-Militarized Zone
DoD	Department of Defense
Emerg	emergency
Err	error
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GUI	Graphical User Interface
HIDS	Host Intrusion Detection System
HTTP	Hyper Text Transfer Protocol
IA	Identification and Authentication
ICMP	Internet Control Message Protocol

Acronym	Definition
IP	Internet Protocol
IPSEC	IP Security
IR	Incident Response
IS	Information Security
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
M&O	Management & Operations
MA	Maintenance
MAC	Media Access Control
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MP	Media Protection
N/A	Not Applicable
NARA	National Archives and Records Administration
NCP	National Checklist Program
NDA	Non-Disclosure Agreement
NFC	Network File System
NFS	Network File Service
NIS+	Network Information Service Plus
NIST	National Institute of Standards and Technology
NSCD	Name Service Caching
NTP	Network Time Protocol
OS	Operating System
PE	Physical and Environmental Protection
PL	Planning
POC	Point of Contact
PAM	Pluggable Authentication Module
PPP	Point-to-Point Protocol
PS	Personnel Security
RA	Risk Assessment

Acronym	Definition
RBAC	Role Based Access Control
RFC	Request for Comment
RO	Read Only
RW	Read-Write
SA	System and Services Acquisition
SC	System and Communications Protection
SDD	System Design Document
SFpDB	Solaris Fingerprint Database
SI	System and Information Integrity
SNMP	Simple Network Management Protocol
SP	Special Publication
SSH	Secure Shell
SSP	System Security Plan
STIG	Security Technical Implementation Guide
SU	Super User
SysAdmins	System Administrators
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UID	User ID
UTC	Coordinated Universal Time
UUCP	UNIX-to-UNIX copy
VM	Virtual Machine
VPN	Virtual Private Network
XML	eXtensible Markup Language

Windows Security Control Assessment Guide

The views, opinions and/or findings contained in this guide are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Approved for Public Release: 19-3536.
Distribution Unlimited.

©2019 The MITRE Corporation. All rights reserved.

Author(s): Nathan Adams
Christine Brown
Jose Cintron

September 2015

McLean, VA

MITRE

This page intentionally left blank.

Table of Contents

1. Overview	1
1.1 Caveats	1
1.2 Assessment Methodology	1
1.2.1 Phase 1: Planning	2
1.2.2 Phase 2: Assessment	2
1.2.3 Phase 3: Reporting	2
2. Assessment Activities	3
2.1 Phase 1: Planning	3
2.2 Phase 2: Assessment	3
2.2.1 System Configuration Review	4
2.2.2 Network Ports and Services Review	8
2.2.3 Vulnerability Review	8
2.2.4 Interviews	8
2.2.5 Tools	9
2.3 Phase 3: Reporting	9
3. Assessing Security Controls	10
3.1 Access Control (AC)	10
3.2 Awareness and Training (AT)	13
3.3 Audit and Accountability (AU)	13
3.4 Certification, Accreditation, and Security Assessments (CA)	15
3.5 Configuration Management (CM)	15
3.6 Contingency Planning (CP)	16
3.7 Identification and Authentication (IA)	17
3.8 Incident Response (IR)	19
3.9 Maintenance (MA)	19
3.10 Media Protection (MP)	19
3.11 Physical and Environmental Protection (PE)	19
3.12 Planning (PL)	19
3.13 Personnel Security (PS)	19
3.14 Risk Assessment (RA)	19
3.15 System and Services Acquisition (SA)	20
3.16 System and Communications Protection (SC)	20
3.17 System and Information Integrity (SI)	23

3.18	Program Management (PM)	24
4.	References.....	25
5.	List of Acronyms.....	26

List of Tables

Table 1.	Access Control Requirement Evaluation	10
Table 2.	Audit and Accountability Requirement Evaluation	13
Table 3.	Configuration Management Requirement Evaluation.....	15
Table 4.	Contingency Planning Requirement Evaluation	17
Table 5.	Identification and Authentication Requirement Evaluation.....	18
Table 6.	System and Communications Protection Requirement Evaluation	20
Table 7.	System and Information Integrity Requirement Evaluation	23

This page intentionally left blank.

1. Overview

This *Microsoft Windows Control Security Assessment Guide* is intended to serve as a practical guidance for information security (IS) engineers who conduct security control assessments for systems that must meet federal guidance. This guide focuses on testing and evaluation techniques for technical controls required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* as they relate to Microsoft Windows installations. Parameters defined in this guide are considered industry best practice but may be modified by the organization as required. These controls include both technical configuration items and Management & Operations (M&O) policies and procedures. The guide also references the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) developed for the Department of Defense (DoD). Where there is no specific organization guidance for a particular parameter setting, the STIG setting will be used. The Windows operating system assessment methodology is just one portion of an overall assessment methodology that includes planning, assessment, and reporting phases.

1.1 Caveats

The controls presented here are for a Federal Information Processing Standard (FIPS) 199 Moderate Impact rated system. Thus, controls for Low and High impact rated systems may differ.

The guide focuses on the Microsoft Windows operating system (OS). The guide assumes the OS evaluator has an understanding of the operating system, is familiar with navigating the Windows registry, permissions and security settings, and generating reports of system security and group policy settings as needed.

This *Windows Security Control Assessment Guide*:

- Provides the operating system security evaluator and subject matter expert (SME), a reference for conducting operating system security control assessments
- Provides **sample** operating system configurations (Section 2.2.1) only for ease of reference and to define the testing concepts and depth of analysis required to verify the implementation of security controls

The configuration settings contained in Section 3 should not be considered an authoritative checklist as there may be more than one way to implement the intent of a particular control. In addition, there may be valid business or functional reasons for a particular device setting that deviates from what is presented here.

1.2 Assessment Methodology

The following sections define the three-phase assessment methodology.

1.2.1 Phase 1: Planning

The first phase, Planning, defines the assessment's scope, identifies goals, sets boundaries, and identifies assessment activities. This phase, as well as subsequent phases, requires the coordination of all involved parties. During this phase, the Evaluation Team reviews all security policies and procedures in accordance with the organization's security requirements. The team will then create assessment scenarios and premises and define assessment agreeable terms as approved by the organization.

1.2.2 Phase 2: Assessment

Phase 2 may have several steps depending on the assessment's objectives, scope, and goals as set forth in Planning Phase. These steps can be grouped by the nature of the activities involved. These activity groups are as follows:

- **Information Collection**—thorough research must be performed against the target system/application before any meaningful assessment can be conducted. Data gathered is analyzed as the assessment proceeds and when the assessment is complete. Prior to the assessment, pre-assessment planning requests for information/artifacts will need to be made in order to have an accurate understanding of the testing environment and to properly prepare for the assessment.
- **Enumeration**—activities that provide specific information about assessment targets. This information is often collected using appropriate software tools.
- **Testing and Review**—activities that typically involve both the automated testing of security vulnerabilities via software tools and the evaluation of particular aspects of the organization's security policies and practices by Assessment Team members.

1.2.3 Phase 3: Reporting

Phase 3, Reporting, documents the soundness of the implemented security controls and consolidates all findings into the final output. This output includes reports that provide a summary of key findings and actionable recommendations, as well as provisions for all information derived from the assessment.

2. Assessment Activities

Assessment activities are be grouped by the three phases—Planning, Assessment, and Reporting. These activities must be thoroughly developed and documented specifically for the technology and systems being implemented prior to the beginning of any assessment.

2.1 Phase 1: Planning

The OS Evaluator reviews the *Security Control Assessment Test Plan* to understand the scope of the assessment. Based on the scope and organization security policies and procedures, security requirements are reviewed. As system documentation is received, the OS Evaluator reviews the documentation to ensure that they have a full understanding of the system to be assessed and the components to be evaluated during the assessment phase. To ensure an efficient onsite assessment, the OS Evaluator will determine any technical scripts, scans, or other requests required. During this time, any special requests for testing are provided to the Lead Evaluator so that the Evaluator can deliver these to the system's point of contact (POC) and the organization facilitator. The OS Evaluator will then create assessment scenarios, update the testing strategy, and select tools to be used. To prepare for this assessment, the OS Evaluator should review the following system documentation:

- System Security Plan (SSP)
- Information System (IS) Risk Assessment (RA)
- Configuration Management (CM) policy document
- Change Management policy document
- Asset Management policy document
- Network diagrams depicting both the logical and physical network architecture
- Baseline configuration documents for each type of device
- Management and Operation (M&O)-related policy documents that may not be contained in the SSP, such as:
 - Password change policy
 - Audit log retention and review policy
 - Backup, recovery, and data protection policy

2.2 Phase 2: Assessment

The operating system assessment activities consist of, but is not limited to, a system configuration review, network ports and services review, vulnerability review, and personnel interviews. The activities and the detailed supporting processes and procedures must be at an adequate level to determine compliance with controls at each system impact level: Low, Moderate, and High.

2.2.1 System Configuration Review

The vast majority of the work performed by the OS Evaluator is devoted to system host configuration review. The OS Evaluator must understand the intent of each control, determine if a technical implementation is required to meet the control, and then determine the necessary configuration parameters required to implement that control.

The configuration review establishes whether organizational secure baseline configurations exist and determines whether the system implements the defined baseline configurations. The secure baselines will result from applying organization and, possibly, industry best practices to securing hardware and software such as DISA STIG developed for the DoD or vendor secure configuration guidance. Some configurations should be consistent across the entire environment (e.g., authentication and audit). Review the baseline configuration documents and compare the content to actual device configurations. The assessor must establish whether the organization consistently applies the baseline configuration across the environment. The following examples illustrate the depth of review required to properly validate secure configurations.

The OS Evaluator should evaluate secure operating system configurations. The evaluator should obtain detailed system configuration information. The control assessment procedure needs to be detailed enough to ascertain compliance with specific controls.

Organization environments may use several versions of Windows operating systems, including Windows Server 2008, 2012, and Windows 7/8/10. Deprecated or obsolete OS versions, such as Windows NT, XP, Vista, or products that have reached end-of-life/end-of-support, such as Windows 2003, should not be present in an organization production network.

Group or local policies are used to configure security settings across the Windows OS platform. For example, auditable events configured for the Audit and Accountability (AU)-2 security control are found within the “Local Policies” segment of the configuration. Generally, the recommended audit settings include the following.

Account Logon	Success, Failure
Account Management	Success, Failure
Directory Service Access	No auditing (Success, Failure on domain controllers)
Logon	Success, Failure
Object Access	Failure (may cause excess log entries)
Policy Change	Success, Failure
Privilege Use	Failure
Process Tracking	No auditing
System	Success, Failure

And for AU-6, if an external log server does not exist, verify that the automatic log archive feature is enabled using the following registry settings.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Ap
plication\AutoBackupLogFiles REG_DWORD, 0x00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Sec
urity\AutoBackupLogFiles REG_DWORD, 0x00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Sys
tem\AutoBackupLogFiles REG_DWORD, 0x00000001
```

Another example of an Access Control (AC) requirement includes Least Privilege (AC-6). An important factor for Windows is to ensure that User Rights assigned to the system are the most restrictive needed for the system to function or as authorized by the organization. The following are typical recommended Windows User Rights settings for a non-domain server, but can vary depending on the Windows OS version and the system purpose:

Access this computer from the network	BUILTIN\Backup Operators BUILTIN\Power Users BUILTIN\Users BUILTIN\Administrators
Act as part of the operating system	None
Add workstations to domain	BUILTIN\Administrators
Adjust memory quotas for a process	None
Allow logon through Terminal Services	None
Back up files and directories	BUILTIN\Backup Operators BUILTIN\Administrators
Bypass traverse checking	BUILTIN\Backup Operators BUILTIN\Power Users BUILTIN\Users BUILTIN\Administrators
Change the system time	BUILTIN\Administrators NT AUTHORITY\LOCAL SERVICE
Create a pagefile	BUILTIN\Administrators
Create a token object	None
Create permanent shared objects	None
Debug programs	BUILTIN\Administrators
Deny access to this computer from the network	None
Deny logon as a batch job	None
Deny logon as a service	None
Deny logon locally	None
Deny logon through Terminal Services	None

Enable computer and user accounts to be trusted for delegation	None
Force shutdown from a remote system	BUILTIN\Administrators
Generate security audits	None
Increase scheduling priority	BUILTIN\Administrators
Load and unload device drivers	BUILTIN\Administrators
Lock pages in memory	
Log on as a batch job	NT AUTHORITY\LOCAL SERVICE
Log on as a service	NT AUTHORITY\NETWORK SERVICE
Log on locally	BUILTIN\Administrators
Manage auditing and security log	BUILTIN\Administrators
Modify firmware environment variables	BUILTIN\Administrators
Perform volume maintenance tasks	None
Profile single process	BUILTIN\Administrators
Profile system performance	BUILTIN\Administrators
Remove computer from docking station	None
Replace a process level token	NT AUTHORITY\NETWORK SERVICE NT AUTHORITY\LOCAL SERVICE
Restore files and directories	BUILTIN\Backup Operators BUILTIN\Administrators
Shut down the system	BUILTIN\Administrators
Synchronize directory service data	None
Take ownership of files or other objects	BUILTIN\Administrators

An example of a Configuration Management (CM) control includes CM-7 (Least Functionality). For CM-7 on Windows 2012 ensure that services are minimized. Depending on the system's purpose, services that typically are not required may include:

- Alerter (Alerter)
- Client Service for NetWare (NWCWorkstation)
- Clipboard (ClipSrv)
- Error reporting
- Fax Service (Fax)
- File Replication (NtFrs)
- File Server for Macintosh (MacFile)

FTP Publishing Service (MSFtpsvc)
Help and Support (helpsvc)
HTTP SSL (HTTPFilter)
IIS Admin Service (IISADMIN)
Indexing Service (cisvc)
License Logging Service (LicenseService)
Messenger (Messenger)
Microsoft POP3 Service
NetMeeting Remote Desktop Sharing (mnmsrvc)
Network Connections
Network News Transport Protocol (NNTP) (NntpSvc)
Print Server for Macintosh (MacPrint)
Print Spooler (Spooler)
Remote Access Auto Connection Manager (RasAuto)
Remote Access Connection Manager (RasMan)
Remote Administration Service
Remote Desktop Help Session Manager (RDSessMgr)
Remote Installation (BINLSVC)
Remote Procedure Call (RPC) Locator (RpcLocator)
Remote Registry Service (RemoteRegistry)
Remote Server Manager (AppMgr)
Remote Server Monitor (Appmon)
Remote Storage Notification (Remote_Storage_User_Link)
Remote Storage Server (Remote_Storage_Server)
Simple Mail Transfer Protocol (SMTP) (SMTPSVC)
SNMP Service (SNMP)
SNMP Trap Service (SNMPTRAP)
Telnet (TlntSvr)
Terminal Services (TermService)
Trivial FTP Daemon (tftpd)
Wireless Configuration (WZCSVC)
World Wide Web Publishing Services (W3SVC)

For System and Communications Protection (SC), a number of different configurations can help secure the host. For SC-5 (Denial of Service), several parameters can be set to protect the TCP/IP stack including:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect=0
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=0
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\nonamereleaseondemand=1

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=300,000 (5 mins)
```

Finally, for SC-8 (Transmission Confidentiality and Integrity) Server Message Block (SMB) communications should be signed using the following settings:

```
Require message integrity  
Require message confidentiality  
Require NTLMv2 session security  
Require 128-bit encryption
```

As previously stated, these are examples of the level of detail required to evaluate a Windows host. They are not all inclusive and the OS evaluator must ensure that enough detail is collected to allow assessment of each applicable control.

2.2.2 Network Ports and Services Review

The OS Evaluator should be prepared to conduct multiple levels of network scans of the hosts using approved types of tools similar to those described in section 2.2.5. Scans should identify all ports and protocols offered by the host. The OS Evaluator should determine the ports and services required for proper system operation.

2.2.3 Vulnerability Review

The OS Evaluator should perform a review of the system for known vulnerabilities. Software tools can be used to identify most known vulnerabilities. Since most software tools are not 100% accurate, care must be taken to eliminate any false positives. There are various vendors and community forums that list or publish OS vulnerabilities. The OS Evaluator should perform specific OS testing to validate the system is not susceptible to these vulnerabilities.

2.2.4 Interviews

Compliance with a number of M&O-related controls is determined through interviews with the system administrators and other personnel. The assessment team's M&O interviewer will address the majority of the M&O controls. The following questions help supplement and corroborate the responses obtained by the M&O interviewer. They also serve to provide more in-depth analysis for certain controls requiring additional scrutiny. Questions serve as a starting point only and based on the interview responses may lead to additional or more in-depth questions. Questions should be tailored to the system environment and its implementations. The following example questions are not meant to limit the interview, but rather serve to illustrate the types of questions that should be asked.

- Describe the Change/Configuration Management (CM) process, gauging how well personnel know and understand the process
- Describe the process to periodically review secure configurations, gauging how well personnel know and understand the process

- Describe the process to periodically store and review audit information, gauging how well personnel know and understand the process
- Describe how and how often authentication credentials updated, gauging how well personnel know and understand the process
- Describe how personnel stay aware of the security patches, fixes, and bug announcements, gauging how well personnel know and understand the process

2.2.5 Tools

The following is a sample of the types of software tools used to perform an OS assessment. The list is by no-means exhaustive. Assessors may have their individual tool preferences and the testing environment may dictate the use of certain tools over others. Familiarity with these types of software tools will provide a baseline approach for testing and should be included as a minimum in the assessor's tool kit for any OS assessment.

- **Automated Data Collection Scripts**—scripts developed by the assessment team to collect configuration information for a specific host operating system, software, or appliance
- **Cryptographic Protocol and Cipher Analysis**—assesses cryptographic protocols in use, strength of ciphers supported, and validity of digital certificates
- **Network Port Mapper/Scanner**—network exploration or security auditing through User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) port scanning
- **Network Protocol Analyzer**—intercepts and logs traffic passing over a network as well as decodes and analyzes the contents according to the appropriate protocol specifications
- **Network Vulnerability Scanner**—system scanner for security vulnerabilities found via services, ports, and system patch levels
- **Web Server Vulnerability Scanner**—software scanner that identifies vulnerabilities in Web server configurations and patch levels

2.3 Phase 3: Reporting

The OS Evaluator must document all weaknesses following the organization reporting procedures and forward to the Lead Evaluator for consolidation and discussion during out-briefs. The OS Evaluator should discuss any Moderate or High findings with support staff so that the out-brief is not the first time staff are exposed to the finding and the supporting evidence.

It is during this phase that the OS Evaluator also reviews any closure evidence if provided. While the finding is not removed from the report, the finding can be closed based on the OS Evaluator determining that the evidence provided is adequate to close the finding. The reporting phase includes documentation of the soundness of the implemented security controls and the actual findings are consolidated into a final report.

3. Assessing Security Controls

This section outlines a list of the security controls specified in NIST 800-53 and the corresponding checks and procedures used to verify Windows operating systems are in compliance. Checks and procedures entries of 'N/A' indicate the security control does not have an applicable technical test to be conducted due to the scope of controls. These controls will be tested in other areas of the assessment by other members of the Evaluation Team.

3.1 Access Control (AC)

Table 1 lists AC checks and procedures.

Table 1. Access Control Requirement Evaluation

Requirement	Checks and Procedures
AC-1 Access Control Policy and Procedures	N/A
AC-2 Account Management	1. Ensure unnecessary administrator accounts are removed. 2. Ensure the built-in Administrator and Guest accounts are renamed and disabled. 3. Ensure the renamed Guest account and the built-in Microsoft support account (SUPPORT_388945a0) is disabled. 4. Ensure anonymous Security Identifier (SID) /Name translation is disabled. 5. Ensure anonymous enumeration of SAM accounts and shares are disabled. 6. Ensure anonymous access to Named Pipes and Shares are restricted. 7. Ensure "Everyone" permissions apply to anonymous users is disabled. 8. Ensure the sharing and security model for local accounts is set to Classic (i.e. local users authenticate as themselves). 9. Ensure automatic administrative logon to the recovery console is disabled. 10. Ensure the default owner for objects created by members of the Administrators group is set to the Administrators Group. 11. Ensure a policy for reviewing administrator account activities, Administrators group membership, administrator accounts and the use of other system related accounts exists.
AC-3 Access Enforcement	1. Ensure all non-removable disk volumes are configured to use New Technology File System (NTFS). 2. Ensure Access Control Lists (ACL) used to protect files, directories, processes and programs from unauthorized access. 3. Ensure proper authentication methods are used (e.g. two-factor) based on the appropriate e-authentication standard. 4. Ensure the CTRL+ALT+Delete sequence is enabled for Logon. 5. Ensure the system shut down without having to logon is disabled.

Requirement	Checks and Procedures
	6. Ensure Domain Controller authentication to unlock workstation is enabled (Active Directory domains only). 7. Ensure passwords are not stored using reversible encryption. 8. Ensure unsigned driver and non-driver installation behavior is set to "Warn but allow installation" or "Do not allow installation".
AC-4 Information Flow Enforcement	Validate if host-based firewalls exist and they are appropriately configured to restrict access to authorized ports protocols, and services.
AC-5 Separation of Duties	1. Ensure System Administrators are not members of any Network Security/Monitoring groups. 2. Ensure developer accounts/groups do not have access to production systems.
AC-6 Least Privilege	1. Ensure access to user-created shares is limited to the users/groups requiring access and the most restrictive rights are assigned. 2. Ensure User Rights assigned by the system are the most restrictive needed for function or authorized by the organization. 3. Ensure the Everyone group is removed and/or replaced by the Authenticated Users group where appropriate. 4. Ensure restricted rights are assigned to Guest user and group (deny logon over the network and locally). 5. Ensure no account has the Synchronize directory service data rights (Active Directory only). 6. Ensure no Administrator accounts (other than the built-in domain administrator) have persistent access to the Enterprise Admins and Schema Admins groups (Active Directory only). 7. Ensure anonymous connections are restricted.
AC-7 Unsuccessful Log-on Attempts	1. Ensure account lock-outs are performed after the organizationally defined failed logon attempts. 2. Ensure account lockout duration is set to the organizationally defined timeframe.
AC-8 System Use Notification	Ensure warning banners are configured and require acknowledgement before granting user access. The banner should notify users that: • They are accessing a <organization> information system • The <organization> maintains ownership and responsibility for its computer systems • Users must adhere to <organization> Information Security Policies, Standards, and Procedures • Their usage may be monitored, recorded, and audited • Unauthorized use is prohibited and subject to criminal and civil penalties • The use of the information system establishes their consent to any and all monitoring and recording of their activities
AC-9 Previous Logon (Access) Notification	Ensure for systems with a "High" FIPS impact level, the date and time of previous logon is recorded and displayed.

Requirement	Checks and Procedures
AC-10 Concurrent Session Control	Ensure the number of remote logins [e.g. Remote Desktop Protocol (RDP) or Terminal Service (TS)] is limited to the organizationally defined value.
AC-11 Session Lock	1. Ensure a screensaver is configured to lock the desktop automatically after a defined level of inactivity. 2. Ensure the screensaver is password protected.
AC-12 Session Termination	Ensure the system is configured to terminate remote sessions after a defined level of inactivity.
AC-14 Permitted Actions without Identification or Authentication	Ensure only publicly available systems allow user access without requiring authentication. Such systems may not provide unauthenticated access to sensitive information.
AC-16 Security Attributes	N/A
AC-17 Remote Access	1. Ensure all remote management of the servers over un-trusted medium (e.g., the Internet) is performed over a Virtual Private Network (VPN). 2. Ensure VPN connections are protected by FIPS 140-2 compliant and NIST validated encryption algorithms.
AC-18 Wireless Access	Ensure the Wireless Configuration service is not enabled and running on production servers. If wireless access is explicitly approved, the following wireless access controls are implemented: • Service set identifier (SSID) broadcasting is disabled • Encryption protection is enabled • Access points are placed in secure areas • Access points are shut down when not in use (i.e., nights, weekends) • A firewall is implemented between the wireless network and the wired infrastructure • MAC address authentication is utilized • Static IP addresses, not DHCP, is utilized • Personal firewalls are utilized on all wireless clients • File sharing is disabled on all wireless clients • Intrusion detection agents are deployed on the wireless side of the firewall Wireless activity is monitored and recorded, and the records are reviewed on a regular basis
AC-19 Access Control for Mobile Devices	1. Ensure only approved, organization-controlled portable and mobile devices are attached to systems and the network, if authorized. 2. Ensure portable/mobile systems (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity) must use an approved encryption method.

Requirement	Checks and Procedures
AC-20 Use of External Information Systems	Ensure any external system (e.g., personal desktop computers, laptops, tablet personal computers, portable/handheld devices, and cellular telephones) used to access, process or store PII or sensitive information is organization-owned.
AC-21 Information Sharing	N/A
AC-22 Publicly Accessible Content	N/A
AC-23 Data Mining Protection	N/A
AC-24 Access Control Decisions	N/A
AC-25 Reference Monitor	N/A

3.2 Awareness and Training (AT)

There are no operating system checks and procedures in this section.

3.3 Audit and Accountability (AU)

Table 2 lists AU checks and procedures.

Table 2. Audit and Accountability Requirement Evaluation

Requirement	Checks and Procedures
AU-1 Audit and Accountability Policy and Procedures	N/A
AU-2 Auditable Events	1. Ensure audit logging is enabled. 2. Ensure the following minimum recommended audit baseline is configured.
AU-3 Content of Audit Records	1. Auditing is enabled for shares, files, and directories containing sensitive information, including protected health information and financial information. 2. Audit record captures date, time, event type, user identity, and source/destination.
AU-4 Audit Storage Capacity	1. Ensure the combined sizes of all event logs do not exceed a defined storage capacity. 2. If an audit server does not exist, ensure minimum audit log sizes are configured.

Requirement	Checks and Procedures
AU-5 Response to Audit Processing Failures	Determine if a procedure is established for identifying audit processing failures in a timely manner.
AU-6 Audit Monitoring, Analysis, and Reporting	1. Ensure a policy for reviewing administrator account activities, administrator group membership, administrator accounts and the use of other system related accounts exists. 2. Ensure filters and alerts are configured for critical events. 3. If an external log server does not exist, verify that the automatic log archive feature is enabled.
AU-7 Audit Reduction and Report Generation	Ensure auditing is automated across the enterprise and facilitates reporting.
AU-8 Time Stamps	1. Ensure timestamps are synchronized system-wide through the use of common Network Time Protocol (NTP) primary and secondary servers located within the network. 2. For Active Directory (AD) domains, follow the AD NTP hierarchy. 3. Ensure servers do not synchronize with external NTP servers (e.g., time.microsoft.com)
AU-9 Protection of Audit Information	Ensure audit records (e.g., AppEvent .Evt, SecEvent .Evt, and SysEvent .Evt) are protected from access and modification by inappropriate users/groups, including Administrators who are responsible for everyday system maintenance.
AU-10 Non-Repudiation	N/A
AU-11 Audit Record Retention	1. Ensure audit logs are retained for an organizationally defined period and old records archived. 2. Ensure record archives are retained for one (1) year, or according to the applicable records control schedule.
AU-12 Audit Generation	1. Ensure the system generates audit records as defined in AU-2 with the content defined in AU-3. 2. Ensure log data is sent to a centralized audit server (e.g., syslogserver). 3. If an audit server does not exist, a local archival process exists. 4. If an audit server does not exist, the security event log is configured to generate a warning when it reaches a defined threshold.
AU-13 Monitoring for Information Disclosure	N/A
AU-14 Session Audit	N/A
AU-15 Alternate Audit Capability	N/A
AU-16	N/A

Requirement	Checks and Procedures
Cross-Organizational Auditing	

3.4 Certification, Accreditation, and Security Assessments (CA)

There are no operating system checks and procedures in this section.

3.5 Configuration Management (CM)

Table 3 lists CM checks and procedures.

Table 3. Configuration Management Requirement Evaluation

Requirement	Checks and Procedures
CM-1 Configuration Management Policy and Procedures	N/A
CM-2 Baseline Configuration	Ensure a system baseline document exists for all servers and installed software.
CM-3 Configuration Change Control	Ensure system changes follow approved CM procedures.
CM-4 Security Impact Analysis	Ensure procedures for monitoring configuration changes to the information system exist.
CM-5 Access Restrictions for Change	Ensure configuration changes are restricted to authorized personnel.
CM-6 Configuration Settings	Ensure mandatory configuration settings are applied to all systems.
CM-7 Least Functionality	1. Ensure security settings are the most restrictive that allow for functionality (e.g., unnecessary services are disabled). 2. Ensure permissions for system services to give Administrators 'Full Control' and the System 'Read' and 'Start, Stop, and Pause' rights. 3. Ensure unnecessary applications are uninstalled. 4. Ensure unnecessary system components/functionality is disabled. 5. Ensure media auto play is disabled for all drives. 6. Ensure the ability to create and access floppy and CD-ROM remote shares is disabled. 7. The list of registry keys that can be accessed remotely is cleared or restricted to an organizational defined set.

Requirement	Checks and Procedures
	8. The list of named pipes that can be accessed anonymously is cleared or restricted to an organizational defined set. 9. Restrict access to clients using a null session. 10. Prevent the LAN Manager (LM) hash from being stored in the SAM or AD.
CM-8 Information System Component Inventory	System component inventory is maintained and reflects the current state of the system.
CM-9 Configuration Management Plan	N/A
CM-10 Software Usage Restrictions	1. Examine policies for software usage restrictions.
CM-11 User-Installed Software	1. Examine policies for user-installed software.

3.6 Contingency Planning (CP)

Table 4 lists CM checks and procedures.

Table 4. Contingency Planning Requirement Evaluation

Requirement	Checks and Procedures
CP-1 Contingency Planning Policy and Procedures	N/A
CP-2 Contingency Plan	N/A
CP-3 Contingency Training	N/A
CP-4 Contingency Plan Testing and Exercises	N/A
CP-6 Alternate Storage Site	N/A
CP-7 Alternate Processing Site	N/A
CP-8 Telecommunication s Services	N/A
CP-9 Information System Backup	1. Full weekly backups are performed. 2. Daily incremental and differential backups are performed. 3. Backups are stored offsite. 4. Onsite and off-site backup media are logged with name, date, time, and action.
CP-10 Information System Recovery and Reconstitution	Ensure automated recovery procedures and capabilities exist.
CP-11 Alternate Communications Protocols	N/A
C-12 Safe Mode	N/A
CP-13 Alternative Security Mechanisms	N/A

3.7 Identification and Authentication (IA)

Table 5 lists IA checks and procedures.

Table 5. Identification and Authentication Requirement Evaluation

Requirement	Checks and Procedures
IA-1 Identification and Authentication Policy and Procedures	Ensure a compliant Identification and Authentication policy is defined.
IA-2 User Identification and Authentication (Organizational Users)	1. Ensure organizational users and administrators have unique system accounts. Organizational users (i.e., organizational information system users) include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). 2. Ensure multifactor authentication is implemented using the following criteria; • Network access to privileged and non-privileged accounts (High only). • Local access to privileged and non-privileged accounts (High only). 3. Ensure the information system uses replay resistant authentication mechanisms for network access to privileged and non-privileged accounts that include protocols using nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators (High only).
IA-3 Device Identification and Authentication	N/A
IA-4 Identifier Management	1. Ensure procedures for reviewing and validating system accounts is defined. 2. Ensure user identifiers are disabled after a pre-defined period of inactivity. 3. Ensure disabled accounts are deleted during annual recertification process. 4. Ensure system administrators maintain separate user accounts: one for standard user functions (e.g., Internet, email, etc.) and one for system administration activities.
IA-5 Authenticator Management	1. Ensure the organizational password policy (min/max age, minimum length, history, and complexity) is defined and automatically enforced. 2. Ensure caching of logon credentials is disabled, or the number of credentials that are cached is limited. 3. Ensure the exposure of authorized user accounts is prevented by not displaying the last user that authenticated to the host. 4. Ensure default Simple Network Management Protocol (SNMP) community strings are changed.
IA-6 Authenticator Feedback	Ensure passwords are not displayed when entered.
IA-7 Cryptographic Module Authentication	Ensure authentication methods use FIPS 140-2 compliant encryption modules.

Requirement	Checks and Procedures
IA-8 Identification and Authentication (Non-Organizational Users)	1. Ensure non-organizational users (those not covered under IA-2) have unique system accounts. 2. Ensure multifactor authentication is used for remote system access.
IA-9 Service Identification and Authentication	N/A
IA-10 Adaptive Identification and Authentication	N/A
IA-11 Re-authentication	N/A

3.8 Incident Response (IR)

There are no operating system checks and procedures in this section.

3.9 Maintenance (MA)

There are no operating system checks and procedures in this section.

3.10 Media Protection (MP)

There are no operating system checks and procedures in this section.

3.11 Physical and Environmental Protection (PE)

There are no operating system checks and procedures in this section.

3.12 Planning (PL)

There are no operating system checks and procedures in this section.

3.13 Personnel Security (PS)

There are no operating system checks and procedures in this section.

3.14 Risk Assessment (RA)

There are no operating system checks and procedures in this section.

3.15 System and Services Acquisition (SA)

There are no operating system checks and procedures in this section.

3.16 System and Communications Protection (SC)

Table 6 lists SC checks and procedures.

Table 6. System and Communications Protection Requirement Evaluation

Requirement	Checks and Procedures
SC-1 System and Communications Protection Policy and Procedures	N/A
SC-2 Application Partitioning	1. Ensure interactive user services (e.g., Web servers) are not co-located with data services (e.g., database servers). 2. Ensure application services are not run under user accounts (i.e., non-interactive dedicated system accounts are used).
SC-3 Security Function Isolation	Ensure Security functions are isolated from non-security functions (i.e., authentication servers are dedicated to that role).
SC-4 Information in Shared Resources	Information contained with shared resources (e.g., Windows shares) is protected from unintended transfer.
SC-5 Denial-of-Service Protection	Ensure denial-of-service protection is configured using TCP stack parameters.
SC-6 Resource Priority	N/A
SC-7 Boundary Protection	N/A
SC-8 Transmission Confidentiality and Integrity	1. Ensure strong encryption keys are computed when using secure channels. 2. Ensure sending unencrypted password to connect to third-party SMB servers is disabled. 3. Ensure the system is configured to terminate remote sessions after a defined level of inactivity. Ensure SMB communications are signed. 4. Ensure NTLMv2 is used for challenge and response authentication and deprecated hash methods are refused. Note: Both clients and servers will need to be configured to support or accept the same authentication level to avoid compatibility issues. If there is an application dependency for the current configuration this exception should be documented. 5. Ensure a strong session key required (Windows 2000 or later). 6. Ensure that a minimum session security for NTLM SSP based (including secure RPC) servers is enabled.
SC-10 Network Disconnect	N/A

Requirement	Checks and Procedures
SC-11 Trusted Path	N/A
SC-12 Cryptographic Key Establishment and Management	N/A
SC-13 Cryptographic Protection	1. Ensure encryption that is used to protect stored sensitive information is FIPS 140-2 compliant and NIST validated modules 2. Ensure FIPS compliant algorithms are used for encryption, hashing, and signing.
SC-14 Public Access Protections	N/A
SC-15 Collaborative Computing Devices	N/A
SC-16 Transmission of Security Parameters	N/A
SC-17 Public Key Infrastructure Certificates	N/A
SC-18 Mobile Code	N/A
SC-19 Voice Over Internet Protocol	N/A
SC-20 Secure Name /Address Resolution Service (Authoritative Source)	1. Ensure authoritative DNS servers provide name resolution only for the zones for which they have authoritative information (Active Directory (AD)-integrated DNS). 2. Ensure recursion is disabled on authoritative DNS servers (AD-integrated DNS). 3. Ensure forwarding and recursion is disabled on AD-integrated DNS servers. 4. Ensure zone integrity checking is enabled (AD-integrated DNS). 5. Ensure DNS transactions are restricted to trusted hostnames/IPs. 6. If multiple network adapters are installed, DNS is bound to the interface providing this service.
SC-21 Secure Name /Address Resolution Service (Recursive or Caching Resolver)	For systems with a "High" FIPS impact level, ensure caching DNS servers perform data origin authentication and integrity verification for resolution services (DNS security extensions [DNSSEC], or hash-based message authentication codes [HMAC] or Transaction Signature Key [TSIG]).
SC-22 Architecture and Provisioning for Name /Address Resolution Service	1. Ensure primary and secondary DNS servers are securely deployed (AD-integrated DNS). 2. Ensure split-DNS is implemented to isolate and protect internal and external resource records (AD-integrated DNS).

Requirement	Checks and Procedures
	3. Ensure separate internal and external DNS namespaces are used 4. Ensure internal name servers are not accessible from outside and provide naming services exclusively to internal clients. 5. Ensure external names servers are located within a DMZ and serve resource records for hosts with public services.
SC-23 Session Authenticity	N/A
SC-24 Fail in Known State	N/A
SC-25 Thin Nodes	N/A
SC-26 Honeypots	N/A
SC-27 Operating System- Independent Applications	N/A
SC-28 Protection of Information at Rest	Bit Locker can be installed and configured as needed.
SC-29 Heterogeneity	N/A
SC-30 Virtualization Techniques	N/A
SC-31 Covert Channel Analysis	N/A
SC-32 Information System Partitioning	Ensure the information system is segmented into components residing in separate physical domains (or environments) as deemed necessary.
SC-33 Transmission Preparation Integrity	N/A
SC-34 Non-Modifiable Executable Programs	N/A
SC-35 Honeyclients	N/A
SC-36 Distributed Processing and Storage	N/A
SC-37 Out-of-Band Channels	N/A
SC-38 Operations Security	N/A

Requirement	Checks and Procedures
SC-39 Process Isolation	N/A
SC-40 Wireless Link Protection	N/A
SC-41 Port and I/O Device Access	N/A
SC-42 Sensor Capability and Data	N/A
SC-43 Usage Restrictions	N/A
SC-44 Detonation Chambers	N/A

3.17 System and Information Integrity (SI)

Table 7 lists SI checks and procedures.

Table 7. System and Information Integrity Requirement Evaluation

Requirement	Checks and Procedures
SI-1 System and Information Integrity Policy and Procedures	N/A
SI-2 Flaw Remediation	1. Ensure a software update agent or service is installed. 2. Ensure the latest OS and software patches, service packs, and hot fixes are installed. 3. Ensure servers are configured to obtain OS and software patches, service packs, and hot fixes from a centralized and automated source.
SI-3 Malicious Code Protection	1. Ensure an antivirus product is installed and configured for real-time protection and monitoring 2. Ensure servers are configured to obtain antivirus software updates and virus code definitions from a centralized and automated source. 3. Ensure the antivirus product is configured to perform daily system scans and at boot time.
SI-4 Information System Monitoring	Ensure a monitoring agent is installed or the server is otherwise monitored for unusual or unauthorized activities or conditions.
SI-5 Security Alerts, Advisories, and Directives	N/A

Requirement	Checks and Procedures
SI-6 Security Function Verification	N/A
SI-7 Software, Firmware, and Information Integrity	Ensure an integrity checking tool is installed (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and is configured to automatically monitor system and applications for evidence of information tampering, errors, and omissions.
SI-8 Spam Protection	N/A
SI-10 Information Input Validation	N/A
SI-11 Error Handling	N/A
SI-12 Information Output Handling and Retention	N/A
SI-13 Predictable Failure Prevention	N/A
SI-14 Non-Persistence	N/A
SI-15 Information Output Filtering	N/A
SI-16 Memory Protection	N/A
SI-17 Fail-Safe Procedures	N/A

3.18 Program Management (PM)

There are no operating system checks and procedures in this section.

4. References

1. Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*.
2. FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.
3. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.
4. NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.
5. NIST SP 800-81 Revision 1, *Secure Domain Name System (DNS) Deployment Guide*.
6. Various Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS) and Checklists.
7. Various Microsoft Windows Security Guides.

5. List of Acronyms

Acronym	Definition
AC	Access Control
ACL	Access Control List
AD	Active Directory
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization (NIST 800-53 version 3)
CM	Configuration Management
CP	Contingency Planning
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DMZ	De-Militarized Zone
DNS	Domain Name System
DNSSEC	DNS Security
DoD	Department of Defense
DoS	Denial-of-Service
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
HMAC	Hash-based Message Authentication Code
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IA	Identification and Authentication
ICMP	Internet Control Message Protocol
IIS	Internet Information Services
IP	Internet Protocol
IR	Incident Response
IS	Information Security
LAN	Local Area Network
LM	LAN Manager

Acronym	Definition
M&O	Management & Operations
MA	Maintenance
MAC	Media Access Control
MP	Media Protection
MS	Microsoft
N/A	Not Applicable
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTFS	New Technology File System
NTLM	NT LAN Manager
NTP	Network Time Protocol
PE	Physical and Environmental Protection
PII	Personally Identifiable Information
PL	Planning
POC	Point of Contact
PS	Personnel Security
OS	Operating System
RA	Risk Assessment
RDP	Remote Desktop Protocol
RO	Read-Only
RPC	Remote Procedure Call
RW	Read-Write
SA	System and Services Acquisition
SAM	Security Account Manager
SC	System and Communications Protection
SCA	Security Control Assessment
SI	System and Information Integrity
SMB	Server Message Block
SME	Subject Matter Expert
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SP	Special Publication

Acronym	Definition
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
SSP	System Security Plan
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TS	Terminal Services
TSIG	Transaction Signature Key
UDP	User Datagram Protocol
VPN	Virtual Private Network