NIST Special Publication
NIST SP 800-171Ar3 ipd

Assessing Security Requirements for Controlled Unclassified Information

Initial Public Draft

Ron Ross
Victoria Pillitteri

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171Ar3.ipd

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800-171Ar3 ipd

Assessing Security Requirements for Controlled Unclassified Information

Initial Public Draft

Ron Ross
Victoria Pillitteri
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171Ar3.ipd

November 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283 [1]. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130 [2].

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

How to Cite this NIST Technical Series Publication:

Ross R, Pillitteri V (2023) Assessing Security Requirements for Controlled Unclassified Information and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-171Ar3 ipd. https://doi.org/10.6028/NIST.SP.800-171Ar3.ipd

Author ORCID iDs

Ron Ross: 0000-0002-1099-9757
Victoria Pillitteri: 0000-0002-7446-7506

Public Comment Period

November 9, 2023 – January 12, 2024

Submit Comments

800-171comments@list.nist.gov
National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the Federal Government to successfully conduct its essential missions and functions. This publication provides federal and nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the security requirements in NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. The assessment procedures are flexible and can be customized to the needs of organizations and assessors. Security assessments can be conducted as independent, third-party assessments or as government-sponsored assessments. The assessments can also be applied with various degrees of rigor based on customer-defined depth and coverage attributes. The findings and evidence produced during the assessments can facilitate risk-based decisions by organizations related to the security requirements.

Keywords

assessment; assessment method; assessment object; assessment procedure; assurance; basic security requirement; controlled unclassified information; coverage; CUI registry; depth; Executive Order 13556; FISMA; NIST Special Publication 800-171; NIST Special Publication 800-53A; nonfederal organization; nonfederal system; security assessment; security control.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Audience

This publication serves a diverse group of individuals and organizations in the public and private sectors, including individuals with:

- System development life cycle responsibilities (e.g., program managers, mission/business owners, information owners/stewards, system designers and developers, system/security engineers, systems integrators)
- Acquisition or procurement responsibilities (e.g., contracting officers)
- System, security, or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, system owners, information security managers)
- Security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, independent verifiers/validators, analysts)

The above roles and responsibilities can be viewed from two perspectives:

- *Federal perspective*: The entity establishing and conveying security assessment requirements in contractual vehicles or other types of agreements
- *Nonfederal perspective*: The entity responding to and complying with security assessment requirements set forth in contracts or agreements

Note to Reviewers

This update to NIST Special Publication (SP) 800-171A represents over one year of data collection, technical analysis, customer interaction, redesign, and development of the procedures for assessing the security requirements for Controlled Unclassified Information (CUI). Many trade-offs have been made to ensure that the assessment procedures have been stated clearly and concisely while also recognizing the specific needs of both federal and nonfederal organizations. The following significant changes have been made in the initial public draft (ipd) of NIST SP 800-171A, Revision 3:

- The restructuring of the assessment procedure syntax to align with NIST SP 800-53A [5].
- The addition of a references section to provide source assessment procedures from NIST SP 800-53A [5].

There has also been a one-time change to the publication version number to align with NIST SP 800-171, Revision 3 [3].

NIST is specifically interested in comments, feedback, and recommendations for the following topics:

- The alignment of the assessment procedures to NIST SP 800-53A [5].
- The use of organization-defined parameters (ODPs) in the assessment procedures.
- The ease-of-use of the assessment procedures in conducting assessments of the CUI security requirements.

Reviewers are encouraged to comment on all or parts of NIST SP 800-171A, Revision 3 ipd. NIST requests that all comments be submitted to 800-171comments@list.nist.gov by 11:59 p.m. Eastern Standard Time (EST) on **January 12, 2024**. Commenters are encouraged to use the comment template provided with the document announcement.

Comments received in response to this request will be posted on the Protecting CUI project site after the due date. Submitters' names and affiliations (when provided) will be included, while contact information will be removed.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

    i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

    ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: 800-171comments@list.nist.gov

Table of Contents

List of Tables

Acknowledgments

The authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors whose constructive comments improved the overall quality, thoroughness, and usefulness of this publication. The authors also wish to thank the NIST technical editing and production staff – Jim Foti, Jeff Brewer, Eduardo Takamura, Isabel Van Wyk, and Cristina Ritfeld – for their outstanding support in preparing this document for publication.

Historical Contributions

The authors wish to acknowledge the following individuals for their historic contributions to this publication: Jon Boyens, Devin Casey, Chris Enloe, Ned Goren, Gary Guissanie, Jody Jacobs, Jeff Marron, Vicki Michetti, Mark Riddle, Mary Thomas, Gary Stoneburner, Patricia Toth, and Patrick Viscuso.

1. Introduction

The security assessment process gathers information and produces evidence to determine the effectiveness of security requirements by:

- Identifying potential problems or shortfalls in security and risk management programs;
- Identifying security weaknesses and deficiencies in systems and the environments in which those systems operate;
- Prioritizing risk mitigation decisions and activities;
- Confirming that identified security weaknesses and deficiencies in the system and environment of operation have been addressed; and
- Supporting continuous monitoring activities and providing information security situational awareness.

1.1. Purpose and Applicability

The purpose of this publication is to provide procedures for assessing the security requirements in NIST Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations* [3]. Organizations can use the assessment procedures to generate evidence to support the assertion that the security requirements have been satisfied. The scope of the security assessments conducted using the procedures described in this publication are guided and informed by the system security plans for systems that process, store, or transmit CUI. The assessment procedures offer the flexibility to customize assessments based on organizational policies and requirements, known threat and vulnerability information, system and platform dependencies, operational considerations, and tolerance for risk.[1]

1.2. Organization of This Publication

The remainder of this special publication is organized as follows:

- Section 2 describes the fundamental concepts associated with assessments of security requirements, including assessment procedures, methods, objects, and assurance cases that can be created using evidence produced during assessments.
- Section 3 provides assessment procedures for the security requirements in NIST SP 800-171, including assessment objectives and potential assessment methods and objects for each procedure.

The following sections provide additional information to support the protection of CUI in nonfederal systems and organizations:

- References
- Appendix A: Acronyms

[1] The term *risk* refers to risks to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. See NIST SP 800-39 [4] for additional information on organizational risk management and risk tolerance.

- Appendix B: Glossary
- Appendix C: Change Log

The contents of this publication can be used for many different assessment-related purposes to determine organizational compliance with the security requirements. The broad range of potential assessment methods and objects listed in this publication does not necessarily reflect and should not be directly associated with actual compliance or noncompliance. Rather, the selection of specific assessment methods and objects from the list provided can help generate a picture of overall compliance with the security requirements. There is no expectation about the number of methods or objects needed to determine compliance with the security requirements. Moreover, the entire list of potential assessment objects should not be viewed as required artifacts needed to determine compliance. Organizations have the flexibility to determine the specific methods and objects sufficient to obtain the needed evidence to support any claims of compliance.

2. The Fundamentals

The process used by organizations and assessors to assess the security requirements in NIST SP 800-171 includes (1) preparing for the assessment, (2) developing a security assessment plan, (3) conducting the assessment, and (4) documenting, analyzing, and reporting the assessment results.[2] The remainder of this section describes the structure and content of the procedures used to assess the security requirements and the importance of assurance cases in providing the evidence necessary to determine compliance with the requirements.

2.1. Assessment Procedures

The security requirements in NIST SP 800-171 are organized into 17 families, as illustrated in Table 1. The assessment procedures in Section 3 are grouped by similar family designations to ensure the completeness and consistency of assessments. The procedures have been derived from the assessment procedures in NIST SP 800-53A [5].

Table 1. Security requirement families

Access Control	Maintenance	Security Assessment and Monitoring
Awareness and Training	Media Protection	System and Communications Protection
Audit and Accountability	Personnel Security	System and Information Integrity
Configuration Management	Physical Protection	Planning
Identification and Authentication	Risk Assessment	System and Services Acquisition
Incident Response		Supply Chain Risk Management

An assessment procedure consists of an assessment *objective* and a set of potential assessment *methods* and *objects* that can be used to conduct the assessment. Each potential assessment objective includes a determination statement related to the security requirement. If there is an organization-defined parameter (ODP) in the security requirement, then the assessment objective begins with a determination statement related to the definition of the ODP. The determination statements are linked to the content of the security requirements to help ensure traceability of the assessment results to the requirements.

Assessment objects identify the specific items being assessed and can include specifications, mechanisms, activities, and individuals. Specifications are the documented artifacts[3] (e.g., plans, policies, procedures, requirements, functional and assurance specifications, architectures, and design documentation) associated with a system. Mechanisms are the hardware, software, and firmware safeguards implemented within a system. Activities are the protection-related actions supporting a system that involve people (e.g., conducting system backup operations, exercising an incident response plan, and monitoring network traffic). Individuals are the people applying the specifications, mechanisms, or activities described above.

[2] NIST SP 800-53A [5] provides additional information on the assessment process and the individuals steps listed above.

[3] Artifacts may be in formats other than documents (e.g., databases, Governance, Risk, and Compliance [GRC] tools, or Open Security Controls Assessment Language [OSCAL])

Assessment methods define the nature and extent of the assessor's actions and are used to facilitate understanding, achieve clarification, or obtain evidence. The potential assessment methods include *examine*, *interview*, and *test*. The examine method is the process of reviewing, studying, inspecting, observing, or analyzing assessment objects. The interview method is the process of holding discussions with individuals or groups about assessment objects. The test method is the process of exercising assessment objects (i.e., activities, mechanisms) under specified conditions to compare actual with expected behavior. Assessment methods include attributes of *depth* and *coverage*, which define the rigor, scope, and level of effort for the assessment as well as the degree of assurance that the security requirements have been satisfied.

The structure and content of a typical assessment procedure are provided in the example below:

3.1.8 Unsuccessful Logon Attempts

Security Requirement Name

REQUIREMENT: 03.01.08

ASSESSMENT OBJECTIVE

Determine if:

Multi-Part Determination Statement for Security Requirement and ODPs

A.03.01.08.ODP[01]: ***the number of consecutive invalid logon attempts by a user allowed during a time period is defined.***

A.03.01.08.ODP[02]: ***the time period to which the number of consecutive invalid logon attempts by a user is limited is defined.***

A.03.01.08: the number of consecutive invalid logon attempts by a user during ***<03.01.08.ODP[02]: time period>*** is limited to ***<A.03.01.08.ODP[01]: number>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for unsuccessful logon attempts; system design documentation; system audit records; system configuration settings; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms implementing access control policy for unsuccessful logon attempts]

REFERENCES

Source Assessment Procedure: AC-07

Determination statements have alphanumeric identifiers. Each determination statement begins with the letter "**A**" to indicate that it is part of an assessment procedure. The next sequence of numbers and/or letters (e.g., **03.01.01.e** or **03.01.01.f.02**) indicates the security requirement identifier from SP 800-171 (and the specific control item if it is a multi-part requirement) that is the target of the assessment. Organization-defined parameters are indicated by the letters "**ODP**." If there are multiple ODPs in the determination statement, the ODP number is indicated in a square bracket (e.g., **A.03.01.08.ODP[01]**). Square brackets are also used to denote when an assessment procedure further decomposes a requirement into more granular determination statements (e.g., **A.03.01.12.a[01]**, **A.03.01.12.a[02]**, **A.03.01.12.a[03]**).

The application of an assessment procedure to a security requirement produces assessment results or *findings*. The findings are compiled and used as evidence to determine whether the security requirement has been *satisfied* or *other than satisfied*. A finding of satisfied indicates that the assessment objective has been met, producing a fully acceptable result. A finding of other than satisfied indicates that there are potential anomalies that may need to be addressed by the organization. A finding of other than satisfied may also indicate that the assessor was unable to obtain sufficient information to make the determination called for in the determination statement.

For assessment findings that are other than satisfied, organizations may define subcategories of findings to indicate the severity or criticality of the weaknesses or deficiencies discovered and the potential adverse effects of those weaknesses or deficiencies on the missions and/or business functions of the organization. Defining such subcategories can help to establish priorities for needed risk mitigation actions.

2.2. Assurance Cases

Building an effective assurance case to determine compliance with security requirements is a process that involves compiling evidence from a variety of sources and conducting different types of activities during an assessment. An *assurance case* is a body of evidence organized into an argument demonstrating that some claim about a system is true. For assessments conducted using the procedures in this publication, that claim is compliance with the security requirements in NIST SP 800-171. Assessors obtain evidence during security assessments to allow designated officials[4] to make objective determinations about compliance with the security requirements. The evidence needed to make such determinations can be obtained from various sources, including independent, third-party assessments or other types of assessments, depending on the needs of the organization establishing the requirements and the organization conducting the assessments.

For example, many technical security requirements are satisfied by security capabilities that are built into commercial information technology products and systems. Product assessments are typically conducted by independent, third-party testing organizations.[5] These assessments examine the security functions of products and established configuration settings. Assessments can also be conducted to demonstrate compliance with industry, national, or international security standards as well as developer and vendor claims. Since many information technology products are assessed by commercial testing organizations and then subsequently deployed in hundreds of thousands of systems, these types of assessments can be carried out at a greater level of depth and provide deeper insights into the security capabilities of the products.

The evidence needed to determine compliance comes from assessing the implementation of the safeguards and countermeasure selected to satisfy the security requirements. Assessors can build on previously developed materials that started with the specification of the information security

[4] A *designated official* is an official, either internal or external to a nonfederal organization, with the responsibility to determine organizational compliance with the security requirements.

[5] Examples of third-party testing organizations include Common Criteria Testing Laboratories that evaluate IT products in accordance with ISO/IEC 15408 [6] and Cryptographic Module Validation Program Testing Laboratories that evaluate cryptographic modules in accordance with Federal Information Processing Standard (FIPS) 140 [7].

needs of the organization and were further improved during the design, development, and implementation of the system. These materials provide the initial evidence for an assurance case. Assessments can be conducted by system developers, system integrators, auditors, system owners, or the security staffs of organizations. The assessors or assessment teams bring together available information about the system, such as the results of component product assessments. The assessors can conduct additional system-level assessments using the assessment methods and procedures contained in this publication and based on the implementation information provided by the nonfederal organization in its system security plan. Assessments can be used to compile and evaluate the evidence needed by organizations to help determine the effectiveness of the safeguards implemented to protect CUI, the actions needed to mitigate security risks to the organization, and compliance with the security requirements.

3. The Procedures

This section provides assessment procedures for the security requirements defined in NIST SP 800-171. Organizations that conduct security requirement assessments can develop their security assessment plans by using the information provided in the assessment procedures and selecting the specific assessment methods and objects that meet the organization's needs. Organizations also have flexibility in defining the level of rigor and detail associated with the assessment based on the assurance requirements of the organization.

3.1. Access Control

3.1.1. Account Management

REQUIREMENT: 03.01.01

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.01.ODP[01]: ***time period for account inactivity before disabling is defined*.**

A.03.01.01.a[01]: system account types allowed are defined.

A.03.01.01.a[02]: system account types prohibited are defined.

A.03.01.01.b[01]: system accounts are created in accordance with organizational policy, procedures, prerequisites, and criteria.

A.03.01.01.b[02]: system accounts are enabled in accordance with organizational policy, procedures, prerequisites, and criteria.

A.03.01.01.b[03]: system accounts are modified in accordance with organizational policy, procedures, prerequisites, and criteria.

A.03.01.01.b[04]: system accounts are disabled in accordance with organizational policy, procedures, prerequisites, and criteria.

A.03.01.01.b[05]: system accounts are removed in accordance with organizational policy, procedures, prerequisites, and criteria.

A.03.01.01.c[01]: authorized users of the system are specified.

A.03.01.01.c[02]: group and role membership are specified.

A.03.01.01.c[03]: access authorizations (i.e., privileges) are specified.

A.03.01.01.d[01]: access to the system is authorized based on a valid access authorization.

A.03.01.01.d[02]: access to the system is authorized based on intended system usage.

A.03.01.01.e: the use of system accounts is monitored.

A.03.01.01.f.01: system accounts are disabled when the accounts have expired.

A.03.01.01.f.02: system accounts are disabled when the accounts have been inactive for ***<A.03.01.01.ODP[01] time period>***.

A.03.01.01.f.03: system accounts are disabled when the accounts are no longer associated with a user or individual.

A.03.01.01.f.04: system accounts are disabled when the accounts violate organizational policy.

A.03.01.01.f.05: system accounts are disabled when significant risks associated with individuals are discovered.

A.03.01.01.g.01: organizational personnel or roles are notified when accounts are no longer required.

A.03.01.01.g.02: organizational personnel or roles are notified when users are terminated or transferred.

A.03.01.01.g.03: organizational personnel or roles are notified when system usage or the need-to-know changes for an individual.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; personnel termination/transfer policies and procedures; procedures for account management; system design documentation; system configuration settings; list of active system accounts and the name of the individual associated with each account; notifications of recent transfers, separations, or terminations of employees; list of conditions for group and role membership; list of recently disabled system accounts and the name of the individual associated with each account; list of user activities that pose significant organizational risks; access authorization records; account management compliance reviews; system monitoring and audit records; system security plan; system-generated list of accounts removed; system-generated list of emergency accounts disabled; system-generated list of disabled accounts; other relevant documents and records]

Interview

[SELECT FROM: personnel with account management responsibilities; system administrators; personnel with information security responsibilities; system developers]

Test

[SELECT FROM: processes for account management on the system; mechanisms for implementing account management]

REFERENCES

Source Assessment Procedures: AC-02, AC-02(03), AC-02(13)

3.1.2. Access Enforcement

REQUIREMENT: 03.01.02

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.02: approved authorizations for logical access to CUI and system resources are enforced.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for access enforcement; system design documentation; system configuration settings; list of approved authorizations (i.e., user privileges); system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with access enforcement responsibilities; system administrators; personnel with information security responsibilities; system developers]

Test

[SELECT FROM: mechanisms for implementing the access control policy]

REFERENCES

Source Assessment Procedure: AC-03

3.1.3. Information Flow Enforcement

REQUIREMENT: 03.01.03

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.03: approved authorizations are enforced for controlling the flow of CUI within the system and between connected systems.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; information flow control policies; procedures for information flow enforcement; security architecture and design documentation; system configuration settings; system baseline configuration; system audit records; list of information flow authorizations; system security plan; other relevant documents or records]

Interview

[SELECT FROM: system administrators; personnel with security architecture responsibilities; personnel with information security responsibilities; system developers]

Test

[SELECT FROM: mechanisms for implementing the information flow enforcement policy]

REFERENCES

Source Assessment Procedure: AC-04

3.1.4. Separation of Duties

REQUIREMENT: 03.01.04

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.04.a: duties of individuals requiring separation are identified.

A.03.01.04.b: system access authorizations to support separation of duties are defined.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for the separation of duties and the division of responsibilities; system configuration settings; system audit records; system access authorizations; list of divisions of responsibility and separation of duties; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for defining the separation of duties and the division of responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: mechanisms for implementing the separation of duties policy]

REFERENCES0

Source Assessment Procedure: AC-05

3.1.5. Least Privilege

REQUIREMENT: 03.01.05

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.05.ODP[01]: ***security functions for authorized access are defined.***

A.03.01.05.ODP[02]: ***security-relevant information for authorized access is defined.***

A.03.01.05.a: system access for users (or processes acting on behalf of users) is authorized only when necessary to accomplish assigned organizational tasks.

A.03.01.05.b[01]: access to ***<A.03.01.05.ODP[01] security functions>*** is authorized.

A.03.01.05.b[02]: access to ***<A.03.01.05.ODP[01] security-relevant information>*** is authorized.

A.03.01.05.c: the privileges assigned to roles or classes of users are periodically reviewed to validate the need for such privileges.

A.03.01.05.d: privileges are reassigned or removed, as necessary.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for least privilege; list of assigned access authorizations (i.e., privileges); system configuration settings; system audit records; list of security functions (deployed in hardware, software, and firmware); security-relevant information for which access must be explicitly authorized; list of system-generated roles or classes of users and assigned privileges; validation reviews of privileges assigned to roles or classes or users; records of privilege removals or reassignments for roles or classes of users; system design documentation; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for defining least privileges; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: mechanisms for implementing least privilege functions; mechanisms for implementing reviews of user privileges]

REFERENCES

Source Assessment Procedures: AC-06, AC-06(01), AC-06(07), AU-09(04)

3.1.6. Least Privilege – Privileged Accounts

REQUIREMENT: 03.01.06

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.06.ODP[01]: ***personnel or roles to which privileged accounts on the system are to be restricted are defined***.

A.03.01.06.a: privileged accounts on the system are restricted to ***<A.03.01.06.ODP[01]: personnel or roles>***.

A.03.01.06.b: users (or roles) with privileged accounts are required to use non-privileged accounts when accessing nonsecurity functions or nonsecurity information.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for least privilege; list of system-generated privileged accounts; list of system administration personnel; system audit records; system configuration settings; system security plan; list of system-generated security functions or security-relevant information assigned to system accounts or roles; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for defining least privileges; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: mechanisms for implementing least privilege functions]

REFERENCES

Source Assessment Procedures: AC-06(02), AC-06(05)

3.1.7. Least Privilege – Privileged Functions

REQUIREMENT: 03.01.07

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.07.a: non-privileged users are prevented from executing privileged functions.

A.03.01.07.b: the execution of privileged functions is logged.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for least privilege; system design documentation; system configuration settings; system audit records; list of audited events; list of privileged functions to be audited and associated user account assignments; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for reviewing least privileges; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for auditing the execution of least privilege functions; mechanisms for implementing least privilege functions for non-privileged users]

REFERENCES

Source Assessment Procedures: AC-06(09), AC-06(10)

3.1.8. Unsuccessful Logon Attempts

REQUIREMENT: 03.01.08

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.08.ODP[01]: ***the number of consecutive invalid logon attempts by a user allowed during a time period is defined***.

A.03.01.08.ODP[02]: ***the time period to which the number of consecutive invalid logon attempts by a user is limited is defined***.

A.03.01.08: the number of consecutive invalid logon attempts by a user during ***<03.01.08.ODP[02]: time period>*** is limited to ***<A.03.01.08.ODP[01]: number>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for unsuccessful logon attempts; system design documentation; system audit records; system configuration settings; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for implementing the access control policy for unsuccessful logon attempts]

REFERENCES

Source Assessment Procedure: AC-07

3.1.9. System Use Notification

REQUIREMENT: 03.01.09

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.09: a system use notification message with privacy and security notices consistent with applicable CUI rules is displayed before granting access to the system.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; privacy and security policies, procedures for system use notification; documented approval of system use notification messages; system audit records; user acknowledgements of system use notification messages; system design documentation; system configuration settings; system use notification messages; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with information security responsibilities; legal counsel; system developers; system administrators]

Test

[SELECT FROM: mechanisms for implementing system use notifications]

REFERENCES

Source Assessment Procedure: AC-08

3.1.10. Device Lock

REQUIREMENT: 03.01.10

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.10.ODP[01]: ***one or more of the following parameter values is/are selected: {initiating a device lock after <A.03.01.10.ODP[02] time period> of inactivity; requiring the user to initiate a device lock before leaving the system unattended}***.

A.03.01.10.ODP[02]: ***time period of inactivity after which a device lock is initiated is defined (if selected)***.

A.03.01.10.a: access to the system is prevented by ***<A.03.01.10.ODP[01]: selected parameter value(s)>***.

A.03.01.10.b: the device lock is retained until the user reestablishes access using established identification and authentication procedures.

A.03.01.10.c: information previously visible on the display is concealed via device lock with a publicly viewable image.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for session lock and identification and authentication; system design documentation; system configuration settings; display screen with session lock activated; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for implementing the access control policy for session lock; session lock mechanisms]

REFERENCES

Source Assessment Procedures: AC-11, AC-11(01)

3.1.11. Session Termination

REQUIREMENT: 03.01.11

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.11.ODP[01]: ***conditions or trigger events that require session disconnect are defined***.

A.03.01.11: a user session is automatically terminated after ***<A.03.01.11.ODP[01]: conditions or trigger events>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for session termination; system design documentation; system configuration settings; list of conditions or trigger events requiring session disconnect; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: automated mechanisms for implementing user session termination]

REFERENCES

Source Assessment Procedure: AC-12

3.1.12. Remote Access

REQUIREMENT: 03.01.12

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.12.a[01]: types of allowable remote system access are defined.

A.03.01.12.a[02]: usage restrictions are established for each type of allowable remote system access.

A.03.01.12.a[03]: configuration requirements are established for each type of allowable remote system access.

A.03.01.12.a[04]: connection requirements are established for each type of allowable remote system access.

A.03.01.12.b: each type of remote system access is authorized prior to establishing such connections.

A.03.01.12.c: remote access to the system is routed through managed access control points.

A.03.01.12.d[1]: remote execution of privileged commands is authorized.

A.03.01.12.d[2]: remote access to security-relevant information is authorized.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for remote system access; remote system access configuration and connection requirements; configuration management plan; system configuration settings; remote access authorizations; system audit records; system design documentation; procedures for remote access to the system; system monitoring records; list of managed network access control points; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for managing remote access connections; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: mechanisms for monitoring and controlling remote access methods; mechanisms for routing remote accesses through managed access control points; remote access management capability for the system]

REFERENCES

Source Assessment Procedures: AC-17, AC-17(03), AC-17(04)

3.1.13. Withdrawn

Incorporated into 03.01.12.

3.1.14. Withdrawn

Incorporated into 03.01.12.

3.1.15. Withdrawn

Incorporated into 03.01.12.

3.1.16. Wireless Access

REQUIREMENT: 03.01.16

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.16.a[01]: each type of wireless access to the system is defined.

A.03.01.16.a[02]: usage restrictions are established for each type of wireless access to the system.

A.03.01.16.a[03]: configuration requirements are established for each type of wireless access to the system.

A.03.01.16.a[04]: connection requirements are established for each type of wireless access to the system.

A.03.01.16.b: each type of wireless access to the system is authorized prior to establishing such connections.

A.03.01.16.c: wireless networking capabilities not intended for use are disabled prior to issuance and deployment.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for wireless system access; wireless system access configuration and connection requirements; configuration management plan; system configuration settings; wireless access authorizations; system audit records; system design documentation; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for managing wireless access connections; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: wireless access management capability for the system; mechanisms for implementing wireless access protections to the system; mechanisms for managing the disabling of wireless networking capabilities]

REFERENCES

Source Assessment Procedures: AC-18, AC-18(03)

3.1.17. Withdrawn

Incorporated into 03.01.16.

3.1.18. Access Control for Mobile Devices

REQUIREMENT: 03.01.18

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.18.a[01]: usage restrictions are established for mobile devices.

A.03.01.18.a[02]: configuration requirements are established for mobile devices.

A.03.01.18.a[03]: connection requirements are established for mobile devices.

A.03.01.18.b: the connection of mobile devices to the system is authorized.

A.03.01.18.c: full-device or container-based encryption is implemented to protect the confidentiality of CUI on mobile devices.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for mobile device access control; system design documentation; configuration management plan; system configuration settings; authorizations for mobile device connections to organizational systems; system audit records; encryption mechanisms and associated configuration documentation; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with access control responsibilities for mobile devices; personnel using mobile devices to access organizational systems; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: access control capability for mobile device connections to organizational systems; encryption mechanisms for protecting the confidentiality of CUI on mobile devices; configurations of mobile devices]

REFERENCES

Source Assessment Procedures: AC-19, AC-19(05)

3.1.19. Withdrawn

Incorporated into 03.01.18.

3.1.20. Use of External Systems

REQUIREMENT: 03.01.20

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.20.ODP[01]: ***terms and conditions to be satisfied on external systems prior to allowing the use of or access to those systems by authorized individuals are defined***.

A.03.01.20.ODP[02]: ***security requirements to be satisfied on external systems prior to allowing the use of or access to those systems by authorized individuals are defined***.

A.03.01.20.a: the use of external systems is prohibited unless the systems are specifically authorized.

A.03.01.20.b[01]: the following terms and conditions to be satisfied on external systems prior to allowing the use of or access to those systems by authorized individuals are established: ***<A.03.01.20.ODP[01]: terms and conditions>***.

A.03.01.20.b[02]: the following security requirements to be satisfied on external systems prior to allowing the use of or access to those systems by authorized individuals are established: ***<A.03.01.20.ODP[02]: security requirements>***.

A.03.01.20.c.01: authorized individuals are permitted to use an external system to access the organizational system or to process, store, or transmit CUI only after verification of the implementation of security requirements on the external system as specified in the organization's security plans.

A.03.01.20.c.02: authorized individuals are permitted to use an external system to access the organizational system or to process, store, or transmit CUI only after the retention of approved system connection or processing agreements with the organizational entity hosting the external system.

A.03.01.20.d: the use of organization-controlled portable storage devices by authorized individuals on external systems is restricted.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for the use of external systems; terms and conditions for the use of external systems; external systems security requirements; list of types of applications accessible from external systems; system configuration settings; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for defining terms, conditions, and security requirements for the use of external systems; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: mechanisms for implementing and/or enforcing terms, conditions, and security requirements for the use of external systems]

REFERENCES

Source Assessment Procedures: AC-20, AC-20(01), AC-20(02)

3.1.21. Withdrawn

Incorporated into 03.01.20.

3.1.22. Publicly Accessible Content

REQUIREMENT: 03.01.22

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.22.a: authorized individuals are trained to ensure that publicly accessible information does not contain CUI.

A.03.01.22.b[01]: the content on publicly accessible systems is periodically reviewed for CUI.

A.03.01.22.b[02]: CUI is removed from publicly accessible systems if discovered.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for publicly accessible content; list of users authorized to post publicly accessible content on organizational systems; training materials and/or records; records of publicly accessible information reviews; records of response to CUI discovered on public websites; system audit logs; security awareness training records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for managing publicly accessible information posted on organizational systems; personnel with information security responsibilities]

Test

[SELECT FROM: mechanisms for implementing the management of publicly accessible content]

REFERENCES

Source Assessment Procedure: AC-22

3.2. Awareness and Training

3.2.1. Literacy Training and Awareness

REQUIREMENT: 03.02.01

ASSESSMENT OBJECTIVE

Determine if:

A.03.02.01.ODP[01]: ***events that require role-based security training are defined***.

A.03.02.01.a.01[01]: security literacy training is provided to system users as part of initial training for new users.

A.03.02.01.a.01[02]: security literacy training is provided to system users periodically after initial training.

A.03.02.01.a.02: security literacy training is provided to system users when required by system changes or following ***<A.03.02.01.ODP[01] events>***.

A.03.02.01.a.03[01]: security literacy training on recognizing indicators of insider threat is provided.

A.03.02.01.a.03[02]: security literacy training on reporting indicators of insider threat is provided.

A.03.02.01.a.03[03]: security literacy training on recognizing indicators of social engineering is provided.

A.03.02.01.a.03[04]: security literacy training on reporting indicators of social engineering is provided.

A.03.02.01.a.03[05]: security literacy training on recognizing indicators of social mining is provided.

A.03.02.01.a.03[06]: security literacy training on reporting indicators of social mining is provided.

A.03.02.01.b[01]: security literacy training content is updated periodically.

A.03.02.01.b[02]: security literacy training content is updated following ***<A.03.02.01.ODP[01] events>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: security literacy training and awareness policy and procedures; procedures for security literacy training and awareness implementation; codes of federal regulations; security literacy and awareness training curriculum; security literacy and awareness training materials; training records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for security literacy training and awareness; personnel comprising the general system user community; personnel with information security responsibilities]

Test

[SELECT FROM: mechanisms for managing information security literacy training and awareness]

REFERENCES

Source Assessment Procedures: AT-02, AT-02(02), AT-02(03)

3.2.2. Role-Based Training

REQUIREMENT: 03.02.02

ASSESSMENT OBJECTIVE

Determine if:

A.03.02.02.ODP[01]: ***events that require role-based security training are defined***.

A.03.02.02.a.01[01]: role-based security training is provided to organizational personnel before authorizing access to the system or CUI.

A.03.02.02.a.01[02]: role-based security training is provided to organizational personnel before performing assigned duties.

A.03.02.02.a.01[03]: role-based security training is provided to organizational personnel periodically after initial access.

A.03.02.02.a.02: role-based security training is provided to organizational personnel when required by system changes or following ***<A.03.02.02.ODP[01] events>***.

A.03.02.02.b[01]: role-based training content is updated periodically.

A.03.02.02.b[02]: role-based training content is updated following ***<A.03.02.02.ODP[01] events>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: security awareness and training policy and procedures; procedures for security training implementation; codes of federal regulations; security training curriculum; security training materials; training records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for role-based security training; personnel with assigned system security roles and responsibilities]

Test

[SELECT FROM: mechanisms for managing role-based security training and awareness]

REFERENCES

Source Assessment Procedure: AT-03

3.2.3. Withdrawn

Incorporated into 03.02.01.

3.3. Audit and Accountability

3.3.1. Event Logging

REQUIREMENT: 03.03.01

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.01.ODP[01]: ***the event types selected for logging within the system are defined***.

A.03.03.01.a: the following event types are specified for logging within the system: ***<A.03.03.01.ODP[01] event types>***.

A.03.03.01.b[01]: the event types selected for logging are reviewed periodically.

A.03.03.01.b[02]: the event types selected for logging are updated periodically.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: audit and accountability policy and procedures; procedures for auditable events; system design documentation; system configuration settings; system audit records; system auditable events; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with audit and accountability responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: mechanisms for implementing system auditing]

REFERENCES

Source Assessment Procedure: AU-02

3.3.2. Audit Record Content

REQUIREMENT: 03.03.02

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.02.a.01: audit records contain information that establishes what type of event occurred.

A.03.03.02.a.02: audit records contain information that establishes when the event occurred.

A.03.03.02.a.03: audit records contain information that establishes where the event occurred.

A.03.03.02.a.04: audit records contain information that establishes the source of the event.

A.03.03.02.a.05: audit records contain information that establishes the outcome of the event.

A.03.03.02.a.06: audit records contain information that establishes the identity of the individuals, subjects, objects, or entities associated with the event.

A.03.03.02.b: additional information for audit records is provided, as needed.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: audit and accountability policy and procedures; procedures for the content of audit records; list of organization-defined auditable events; system design documentation; system configuration settings; system audit records; system incident reports; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with audit and accountability responsibilities; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for implementing system auditing of auditable events; system audit capability]

REFERENCES

Source Assessment Procedures: AU-03, AU-03(01)

3.3.3. Audit Record Generation

REQUIREMENT: 03.03.03

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.03.a: audit records for the selected event types and audit record content specified in 3.3.1 and 3.3.2 are generated.

A.03.03.03.b: audit records are retained for a time period consistent with records retention policy.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: audit and accountability policy and procedures; procedures for audit record generation; system design documentation; list of auditable events; audit records; audit record retention policy and procedures; organization-defined retention period for audit records; audit record archives; system configuration settings; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with audit record generation responsibilities; personnel with audit record retention responsibilities; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for implementing the audit record generation capability]

REFERENCES

Source Assessment Procedures: AU-11, AU-12

3.3.4. Response to Audit Logging Process Failures

REQUIREMENT: 03.03.04

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.04.ODP[01]: ***time period for organizational personnel or roles receiving audit logging process failure alerts is defined***.

A.03.03.04.ODP[02]: ***additional actions to be taken in the event of an audit logging process failure are defined***.

A.03.03.04.a: organizational personnel or roles are alerted in the event of an audit logging process failure within ***<A.03.03.04.ODP[01] time period>***.

A.03.03.04.b: the following additional actions are taken in the event of an audit logging process failure: ***<A.03.03.04.ODP[02] additional actions>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: audit and accountability policy and procedures; procedures for responding to audit processing failures; system design documentation; system configuration settings; list of personnel to be notified in case of an audit processing failure; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with audit and accountability responsibilities; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for implementing system response to audit processing failures]

REFERENCES

Source Assessment Procedure: AU-05

3.3.5. Audit Record Review, Analysis, and Reporting

REQUIREMENT: 03.03.05

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.05.a: system audit records are reviewed and analyzed periodically for indications and potential impacts of inappropriate or unusual activity.

A.03.03.05.b: findings are reported to organizational personnel or roles.

A.03.03.05.c: audit records across different repositories are analyzed and correlated to gain organization-wide situational awareness.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: audit and accountability policy and procedures; procedures for audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews and analyses of audit records; system design documentation; system audit records across different repositories; system configuration settings; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with audit review, analysis, and reporting responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: mechanisms for supporting the analysis and correlation of audit records]

REFERENCES

Source Assessment Procedures: AU-06, AU-06(03)

3.3.6. Audit Record Reduction and Report Generation

REQUIREMENT: 03.03.06

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.05.a: an audit record reduction and report generation capability that supports audit record review, analysis, reporting requirements, and after-the-fact investigations of incidents is implemented.

A.03.03.05.b: the original content and time ordering of audit records are preserved.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: audit and accountability policy and procedures; procedures for audit reduction and report generation; system design documentation; system configuration settings; system audit records; audit reduction, review, analysis, and reporting tools; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with audit reduction and report generation responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: audit reduction and report generation capability]

REFERENCES

Source Assessment Procedure: AU-07

3.3.7. Time Stamps

REQUIREMENT: 03.03.07

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.07.ODP[01]: ***the granularity of time measurement for audit record time stamps is defined***.

A.03.03.07.a: internal system clocks are used to generate time stamps for audit records.

A.03.03.07.b[01]: time stamps for audit records meet ***<A.03.03.07.ODP[01] granularity of time measurement>***.

A.03.03.07.b[02]: time stamps for audit records use Coordinated Universal Time (UTC), have a fixed local time offset from UTC, or include the local time offset as part of the time stamp are recorded.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: audit and accountability policy and procedures; procedures for timestamp generation; system design documentation; system configuration settings; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for implementing timestamp generation]

REFERENCES

Source Assessment Procedure: AU-08

3.3.8. Protection of Audit Information

REQUIREMENT: 03.03.08

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.08.a: audit information and audit logging tools are protected from unauthorized access, modification, and deletion.

A.03.03.08.b: access to the management of audit logging functionality is authorized to only a subset of privileged users or roles.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: audit and accountability policy and procedures; access control policy and procedures; procedures for the protection of audit information; system configuration settings; system audit records; audit tools; system-generated list of privileged users with access to the management of audit functionality; access authorizations; access control list; system design documentation; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with audit and accountability responsibilities; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for implementing audit information protection; mechanisms for managing access to audit functionality]

REFERENCES

Source Assessment Procedures: AU-09, AU-09(04)

3.3.9. Withdrawn

Incorporated into 03.03.08.

3.4. Configuration Management

3.4.1. Baseline Configuration

REQUIREMENT: 03.04.01

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.01.a[01]: a current baseline configuration of the system is developed.

A.03.04.01.a[02]: a current baseline configuration of the system is maintained under configuration control.

A.03.04.01.b[01]: the baseline configuration of the system is reviewed periodically.

A.03.04.01.b[02]: the baseline configuration of the system is reviewed when system components are installed or modified.

A.03.04.01.b[03]: the baseline configuration of the system is updated periodically.

A.03.04.01.b[04]: the baseline configuration of the system is updated when system components are installed or modified.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: configuration management policy and procedures; procedures for the baseline system configuration; configuration management plan; enterprise architecture; system design documentation; system architecture; system configuration settings; system component inventory; change control records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with configuration management responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for managing baseline configurations; mechanisms for supporting configuration control of the baseline configuration]

REFERENCES

Source Assessment Procedure: CM-02

3.4.2. Configuration Settings

REQUIREMENT: 03.04.02

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.02.ODP[01]: ***configuration settings for the system that reflect the most restrictive mode consistent with operational requirements are defined***.

A.03.04.02.a[01]: the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements are established and documented: ***<A.03.04.02.ODP[01] configuration settings>***.

A.03.04.02.a[02]: the following configuration settings for the system are implemented: ***<A.03.04.02.ODP[01] configuration settings>***.

A.03.04.02.b[01]: any deviations from established configuration settings are identified and documented.

A.03.04.02.b[02]: any deviations from established configuration settings are approved.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: configuration management policy and procedures; procedures for system configuration settings; configuration management plan; system design documentation; system configuration settings; common secure configuration checklists; system component inventory; evidence supporting approved deviations from established configuration settings; change control records; system data processing and retention permissions; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with security configuration management responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for managing configuration settings; mechanisms that implement, monitor, and/or control system configuration settings; mechanisms that identify and/or document deviations from established configuration settings]

REFERENCES

Source Assessment Procedure: CM-06

3.4.3. Configuration Change Control

REQUIREMENT: 03.04.03

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.03.a: the types of changes to the system that are configuration-controlled are defined.

A.03.04.03.b[01]: proposed configuration-controlled changes to the system are reviewed.

A.03.04.03.b[02]: proposed configuration-controlled changes to the system are approved or disapproved with explicit consideration for security impacts.

A.03.04.03.c[01]: approved configuration-controlled changes to the system are implemented.

A.03.04.03.c[02]: approved configuration-controlled changes to the system are documented.

A.03.04.03.d[01]: activities associated with configuration-controlled changes to the system are monitored.

A.03.04.03.d[02]: activities associated with configuration-controlled changes to the system are reviewed.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: configuration management policy and procedures; procedures for system configuration change control; configuration management plan; system architecture; configuration settings; change control records; system audit records; change control audit and review reports; agenda, minutes, and documentation from configuration change control oversight meetings; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with configuration change control responsibilities; personnel with information security responsibilities; members of change control board or similar; system administrators]

Test

[SELECT FROM: processes for configuration change control; mechanisms that implement configuration change control]

REFERENCES

Source Assessment Procedure: CM-03

3.4.4. Impact Analyses

REQUIREMENT: 03.04.04

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.04: changes to the system are analyzed for security impact prior to implementation.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: configuration management policy and procedures; procedures for security impact analyses for system changes; configuration management plan; security impact analysis documentation; system design documentation; analysis tools and outputs; change control records; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with security impact analysis responsibilities; personnel with information security responsibilities; members of change control board; system developers; system administrators]

Test

[SELECT FROM: processes for security impact analyses]

REFERENCES

Source Assessment Procedure: CM-04

3.4.5. Access Restrictions for Change

REQUIREMENT: 03.04.05

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.05[01]: physical access restrictions associated with changes to the system are defined and documented.

A.03.04.05[02]: physical access restrictions associated with changes to the system are approved.

A.03.04.05[03]: physical access restrictions associated with changes to the system are enforced.

A.03.04.05[04]: logical access restrictions associated with changes to the system are defined and documented.

A.03.04.05[05]: logical access restrictions associated with changes to the system are approved.

A.03.04.05[06]: logical access restrictions associated with changes to the system are enforced.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: configuration management policy and procedures; procedures for access restrictions for system changes; configuration management plan; system design documentation; system architecture; system configuration settings; logical access approvals; physical access approvals; access credentials; change control records; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with logical access control responsibilities; personnel with physical access control responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for managing access restrictions for system changes; mechanisms for supporting, implementing, or enforcing access restrictions associated with system changes]

REFERENCES

Source Assessment Procedure: CM-05

3.4.6. Least Functionality

REQUIREMENT: 03.04.06

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.06.ODP[01]: ***functions to be prohibited or restricted are defined***.

A.03.04.06.ODP[02]: ***ports to be prohibited or restricted are defined***.

A.03.04.06.ODP[03]: ***protocols to be prohibited or restricted are defined***.

A.03.04.06.ODP[04]: ***connections to be prohibited or restricted are defined***.

A.03.04.06.ODP[05]: ***services to be prohibited or restricted are defined***.

A.03.04.06.ODP[06]: ***functions deemed unnecessary or non-secure are defined***.

A.03.04.06.ODP[07]: ***ports deemed unnecessary or non-secure are defined***.

A.03.04.06.ODP[08]: ***protocols deemed unnecessary or non-secure are defined***.

A.03.04.06.ODP[09]: ***connections deemed unnecessary or non-secure are defined***.

A.03.04.06.ODP[10]: ***services deemed unnecessary or non-secure are defined***.

A.03.04.06.a: the system is configured to provide only mission-essential capabilities.

A.03.04.06.b[01]: the use of the following functions is prohibited or restricted: ***<A.03.04.06.ODP[01]: functions>***.

A.03.04.06.b[02]: the use of the following ports is prohibited or restricted: ***<A.03.04.06.ODP[02]: ports>***.

A.03.04.06.b[03]: the use of the following protocols is prohibited or restricted: ***<A.03.04.06.ODP[03]: protocols>***.

A.03.04.06.b[04]: the use of the following connections is prohibited or restricted: ***<A.03.04.06.ODP[04]: connections>***.

A.03.04.06.b[05]: the use of the following services is prohibited or restricted: ***<A.03.04.06.ODP[05]: services>***.

A.03.04.06.c: the system is reviewed periodically to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.

A.03.04.06.d[01]: the following unnecessary or nonsecure functions are disabled or removed: ***<A.03.04.06.ODP[06]: functions>***.

A.03.04.06.d[02]: the following unnecessary or nonsecure ports are disabled or removed: ***<A.03.04.06.ODP[07]: ports>***.

A.03.04.06.d[03]: the following unnecessary or nonsecure protocols are disabled or removed: ***<A.03.04.06.ODP[08]: protocols>***.

A.03.04.06.d[04]: the following unnecessary or nonsecure connections are disabled or removed: ***<A.03.04.06.ODP[09]: connections>***.

A.03.04.06.d[05]: the following unnecessary or nonsecure services are disabled or removed: ***<A.03.04.06.ODP[10]: services>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: configuration management policy and procedures; procedures for least functionality in the system; configuration management plan; system design documentation; system configuration settings; system component inventory; common secure configuration checklists; documented reviews of functions, ports, protocols, and services; change control records; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with configuration management responsibilities; personnel with responsibilities for reviewing functions, ports, protocols, and services; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: processes for prohibiting or restricting functions, ports, protocols, and services; processes for reviewing or disabling functions, ports, protocols, and services; mechanisms for implementing the review and disabling of functions, ports, protocols, and services; mechanisms for implementing restrictions on or the prohibition of functions, ports, protocols, and services]

REFERENCES

Source Assessment Procedures: CM-07, CM-07(01)

3.4.7. Withdrawn

Incorporated into 03.04.06.

3.4.8. Authorized Software – Allow by Exception

REQUIREMENT: 03.04.08

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.08.a: software programs authorized to execute on the system are identified.

A.03.04.08.b: a deny-all, allow-by-exception policy for the execution of software programs on the system is implemented.

A.03.04.08.c[01]: the list of authorized software programs is reviewed periodically.

A.03.04.08.c[02]: the list of authorized software programs is updated periodically.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: configuration management policy and procedures; procedures for least functionality in the system; configuration management plan; system design documentation; system configuration settings; list of software programs authorized to execute on the system;

system component inventory; common secure configuration checklists; review and update records associated with list of authorized software programs; change control records; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for identifying software authorized to execute on the system; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for identifying, reviewing, and updating programs authorized to execute on the system; processes for implementing authorized software policy; mechanisms for supporting and/or implementing authorized software policy]

REFERENCES

Source Assessment Procedure: CM-07(05)

3.4.9. Withdrawn

Addressed by 03.01.05, 03.01.06, 03.01.07, and 03.04.08.

3.4.10. System Component Inventory

REQUIREMENT: 03.04.10

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.10.a: an inventory of system components is developed and documented.

A.03.04.10.b[01]: the system component inventory is reviewed periodically.

A.03.04.10.b[02]: the system component inventory is updated periodically.

A.03.04.10.c[01]: the system component inventory is updated as part of component installations.

A.03.04.10.c[02]: the system component inventory is updated as part of component removals.

A.03.04.10.c[03]: the system component inventory is updated as part of system updates.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: configuration management policy and procedures; procedures for system component inventory; configuration management plan; system design documentation; system component inventory; inventory reviews and update records; component installation records; change control records; component removal records; system change records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with component inventory management responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for managing the system component inventory; mechanisms for supporting and/or implementing the system component inventory; processes for updating the system component inventory; mechanisms for supporting and/or implementing the system component inventory updates]

REFERENCES

Source Assessment Procedures: CM-08, CM-08(01)

3.4.11. Information Location

REQUIREMENT: 03.04.11

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.11.a[01]: the location of CUI is identified and documented.

A.03.04.11.a[02]: the system components on which CUI is processed are identified and documented.

A.03.04.11.a[03]: the system components on which CUI is stored are identified and documented.

A.03.04.11.b[01]: users who have access to the system and system components where CUI is processed are identified and documented.

A.03.04.11.b[02]: users who have access to the system and system components where CUI is stored are identified and documented.

A.03.04.11.c[01]: changes to the location (i.e., system or system components) where CUI is processed are documented.

A.03.04.11.c[02]: changes to the location (i.e., system or system components) where CUI is stored are documented.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: configuration management policy and procedures; configuration management plan; procedures for identification and documentation of information location; system; audit records; architecture documentation; system design documentation; list of users with system and system component access; change control records; system component inventory; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for managing information location and user access; personnel with responsibilities for operating, using, and/or maintaining the system; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: processes governing information location; mechanisms for enforcing policies and methods for governing information location]

REFERENCES

Source Assessment Procedure: CM-12

3.4.12. System and Component Configuration for High-Risk Areas

REQUIREMENT: 03.04.12

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.12.ODP[01]: ***configurations for systems or system components to be issued to individuals traveling to high-risk locations are defined***.

A.03.04.12.ODP[02]: ***the security requirements to be applied to the system or system components when individuals return from travel are defined***.

A.03.04.12.a: systems or system components with the following configurations are issued to individuals traveling to high-risk locations: ***<A.03.04.12.ODP[01]: configurations>***.

A.03.04.12.b: the following security requirements are applied to the system or system components when the individuals return from travel: ***<A.03.04.12.ODP[02]: requirements>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: configuration management policy and procedures; configuration management plan; procedures for the baseline configuration of the system; procedures for system component installations and upgrades; system component inventory; system component installations or upgrades and associated records; records of system baseline configuration reviews and updates; system configuration settings; system architecture; change control records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with configuration management responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for managing baseline configurations]

REFERENCES

Source Assessment Procedure: CM-02(07)

3.5. Identification and Authentication

3.5.1. User Identification, Authentication, and Re-Authentication

REQUIREMENT: 03.05.01

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.01.ODP[01]: ***circumstances or situations that require re-authentication are defined***.

A.03.05.01.a[01]: system users are uniquely identified and authenticated.

A.03.05.01.a[02]: the unique identification of authenticated system users is associated with processes acting on behalf of those users.

A.03.05.01.b: users are reauthenticated when ***<A.03.05.01.ODP[01]: circumstances or situations>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: identification and authentication policy and procedures; list of circumstances or situations requiring re-authentication; system design documentation; system configuration settings; system audit records; list of system accounts; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with identification and authentication responsibilities; personnel with system operations responsibilities; personnel with account management responsibilities; system developers; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for uniquely identifying and authenticating users; mechanisms for supporting and/or implementing identification and authentication capabilities]

REFERENCES

Source Assessment Procedures: IA-02, IA-11

3.5.2. Device Identification and Authentication

REQUIREMENT: 03.05.02

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.02: devices are uniquely identified and authenticated before establishing a system connection.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: identification and authentication policy and procedures; procedures for device identification and authentication; system design documentation; list of devices requiring unique identification and authentication; device connection reports; system configuration settings; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for device identification and authentication; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for supporting and/or implementing device identification and authentication capabilities]

REFERENCES

Source Assessment Procedure: IA-03

3.5.3. Multi-Factor Authentication

REQUIREMENT: 03.05.03

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.03: multi-factor authentication for access to system accounts is implemented.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: identification and authentication policy and procedures; system design documentation; list of system accounts; system configuration settings; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with system operations responsibilities; personnel with account management responsibilities; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for supporting and/or implementing a multi-factor authentication capability]

REFERENCES

Source Assessment Procedures: IA-02(01), IA-02(02)

3.5.4. Replay-Resistant Authentication

REQUIREMENT: 03.05.04

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.04: replay-resistant authentication mechanisms for access to system accounts are implemented.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: identification and authentication policy and procedures; system design documentation; system audit records; system configuration settings; list of privileged system accounts; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with system operations responsibilities; personnel with account management responsibilities; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for supporting and/or implementing identification and authentication capabilities; mechanisms for supporting and/or implementing replay-resistance]

REFERENCES

Source Assessment Procedure: IA-02(08)

3.5.5. Identifier Management

REQUIREMENT: 03.05.05

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.05.ODP[01]: ***personnel or roles from whom authorization must be received to assign an identifier are defined***.

A.03.05.05.ODP[02]: ***a time period for preventing the reuse of identifiers is defined***.

A.03.05.05.a: authorization is received from ***<A.03.05.05.ODP[01]: personnel or roles>*** to assign an individual, group, role, service, or device identifier.

A.03.05.05.b[01]: an identifier that identifies an individual, group, role, service, or device is selected.

A.03.05.05.b[02]: an identifier that identifies an individual, group, role, service, or device is assigned.

A.03.05.05.c: the reuse of identifiers for ***<A.03.05.05.ODP[02]: time period>*** is prevented.

A.03.05.05.d: the status of each individual is uniquely identified with an identifying characteristic.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: identification and authentication policy and procedures; procedures for identifier management; procedures for account management; system design documentation; list of system accounts; list of characteristics identifying individual status; system configuration settings; list of identifiers generated from physical access control devices; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with identifier management responsibilities; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for supporting and/or implementing identifier management]

REFERENCES

Source Assessment Procedures: IA-04, IA-04(04)

3.5.6. Withdrawn

3.5.7. Password Management

REQUIREMENT: 03.05.07

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.07.ODP[01]: ***password composition and complexity rules are defined***.

A.03.05.07.a[01]: a list of commonly used, expected, or compromised passwords is maintained.

A.03.05.07.a[02]: a list of commonly used, expected, or compromised passwords is updated periodically.

A.03.05.07.a[03]: a list of commonly used, expected, or compromised passwords is updated when organizational passwords are suspected to have been compromised.

A.03.05.07.b: passwords are verified not to be found on the list of commonly used, expected, or compromised passwords when they are created or updated by users.

A.03.05.07.c: passwords are only transmitted over cryptographically protected channels.

A.03.05.07.d: passwords are stored in a cryptographically protected form.

A.03.05.07.e: a new password is selected upon first use after account recovery.

A.03.05.07.f: the following composition and complexity rules are enforced: ***<A.03.05.07.ODP[01]: rules>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: identification and authentication policy and procedures; password policy; procedures for authenticator management; system design documentation; system configuration settings; password configurations; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with authenticator management responsibilities; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for supporting and/or implementing a password-based authenticator management capability]

REFERENCES

Source Assessment Procedure: IA-05(01)

3.5.8. Withdrawn

3.5.9. Withdrawn

Incorporated into 03.05.07.

3.5.10. Withdrawn

Incorporated into 03.05.07.

3.5.11. Authentication Feedback

REQUIREMENT: 03.05.11

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.11: feedback of authentication information during the authentication process is obscured.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: identification and authentication policy and procedures; procedures for authenticator feedback; system design documentation; system configuration settings; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for supporting and/or implementing the obscuring of feedback of authentication information during authentication]

REFERENCES

Source Assessment Procedure: IA-06

3.5.12. Authenticator Management

REQUIREMENT: 03.05.12

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.12.ODP[01]: ***events that trigger the change or refreshment of authenticators are defined***.

A.03.05.12.a: the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution is verified.

A.03.05.12.b: initial authenticator content for any authenticators issued by the organization is established.

A.03.05.12.c[01]: administrative procedures for initial authenticator distribution are established and implemented.

A.03.05.12.c[02]: administrative procedures for lost, compromised, or damaged authenticators are established and implemented.

A.03.05.12.c[03]: administrative procedures for revoking authenticators are established and implemented.

A.03.05.12.d: default authenticators are changed at first use.

A.03.05.12.e: authenticators are changed and refreshed periodically or when the following events occur: ***<A.03.05.12.ODP[01]: events>***.

A.03.05.12.f[01]: authenticator content is protected from unauthorized disclosure.

A.03.05.12.f[01]: authenticator content is protected from unauthorized modification.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: identification and authentication policy and procedures; procedures for authenticator management; system configuration settings; list of system authenticator types; system design documentation; system audit records; change control records associated with managing system authenticators; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with authenticator management responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: mechanisms for supporting and/or implementing the authenticator management capability]

REFERENCES

Source Assessment Procedure: IA-05

3.6. Incident Response

3.6.1. Incident Response Plan and Handling

REQUIREMENT: 03.06.01

ASSESSMENT OBJECTIVE

Determine if:

A.03.06.01.a: an incident response plan that provides the organization with a roadmap for implementing its incident response capability is developed.

A.03.06.01.b[01]: an incident-handling capability for incidents that is consistent with the incident response plan is implemented.

A.03.06.01.b[02]: the incident handling capability for incidents includes preparation.

A.03.06.01.b[03]: the incident handling capability for incidents includes detection and analysis.

A.03.06.01.b[04]: the incident handling capability for incidents includes containment.

A.03.06.01.b[05]: the incident handling capability for incidents includes eradication.

A.03.06.01.b[06]: the incident handling capability for incidents includes recovery.

A.03.06.01.c: the incident response plan is updated to address system and organizational changes or problems encountered during plan implementation, execution, or testing.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: incident response policy and procedures; contingency planning policy and procedures; procedures for incident handling; procedures for incident response planning; incident response plan; contingency plan; records of incident response plan reviews and approvals; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with incident handling responsibilities; personnel with incident response planning responsibilities; personnel with contingency planning responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: incident handling capability for the organization; incident response plan]

REFERENCES

Source Assessment Procedures: IR-04, IR-08

3.6.2. Incident Monitoring, Reporting, and Response Assistance

REQUIREMENT: 03.06.02

ASSESSMENT OBJECTIVE

Determine if:

A.03.06.02.ODP[01]: ***the time period to report suspected incidents to the organizational incident response capability is defined***.

A.03.06.02.ODP[02]: ***authorities to whom incident information is to be reported are defined***.

A.03.06.02.a[01]: system security incidents are tracked.

A.03.06.02.a[02]: system security incidents are documented.

A.03.06.02.b: suspected incidents are reported to the organizational incident response capability within ***<A.03.06.02.ODP[01]: time period>***.

A.03.06.02.c: incident information is reported to ***<A.03.06.02.ODP[02]: authorities>***.

A.03.06.02.d: an incident response support resource that offers advice and assistance to users of the system for the handling and reporting of incidents is provided.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: incident response policy and procedures; procedures for incident monitoring; procedures for incident response assistance; incident response records and documentation; incident response plan; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with incident monitoring responsibilities; personnel with incident response assistance and support responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: processes for incident reporting; incident monitoring capability; mechanisms for supporting and/or implementing the tracking and documenting of system security incidents; mechanisms for supporting and/or implementing incident reporting; mechanisms for supporting and/or implementing incident response assistance; processes for incident response assistance]

REFERENCES

Source Assessment Procedures: IR-05, IR-06, IR-07

3.6.3. Incident Response Testing

REQUIREMENT: 03.06.03

ASSESSMENT OBJECTIVE

Determine if:

A.03.06.03: the effectiveness of the incident response capability is tested periodically.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: incident response policy and procedures; contingency planning policy and procedures; procedures for incident response testing; procedures for contingency plan testing; incident response testing material; incident response test results; incident response test plan; incident response plan; contingency plan; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with incident response testing responsibilities; personnel with information security responsibilities]

REFERENCES

Source Assessment Procedure: IR-03

3.6.4. Incident Response Training

REQUIREMENT: 03.06.04

ASSESSMENT OBJECTIVE

Determine if:

A.03.06.04.ODP[01]: ***a time period within which incident response training is to be provided to system users is defined***.

A.03.06.04.ODP[02]: ***events that initiate a review of the incident response training content are defined***.

A.03.06.04.a.01: incident response training for system users consistent with assigned roles and responsibilities is provided within ***<A.03.06.04.ODP[01]: time period>*** of assuming an incident response role or responsibility or acquiring system access.

A.03.06.04.a.02: incident response training for system users consistent with assigned roles and responsibilities is provided when required by system changes.

A.03.06.04.a.03: incident response training for system users consistent with assigned roles and responsibilities is provided periodically after initial and event-driven training.

A.03.06.04.b[01]: incident response training content is reviewed periodically.

A.03.06.04.b[02]: incident response training content is reviewed following ***<A.03.06.04.ODP[02]: events>***.

A.03.06.04.b[03]: incident response training content is updated periodically.

A.03.06.04.b[04]: incident response training content is updated following ***<A.03.06.04.ODP[02]: events>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: incident response policy and procedures; procedures for incident response training; incident response training curriculum; incident response training materials; incident response plan; incident response training records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with incident response training and operational responsibilities; personnel with information security responsibilities]

REFERENCES

Source Assessment Procedure: IR-02

3.7. Maintenance

3.7.1. Withdrawn

Recategorized as NCO**.**

3.7.2. Withdrawn

Incorporated into 03.07.04 and 03.07.06.

3.7.3. Withdrawn

Incorporated into 03.08.03.

3.7.4. Maintenance Tools

REQUIREMENT: 03.07.04

ASSESSMENT OBJECTIVE

Determine if:

A.03.07.04.a[01]: the use of system maintenance tools is approved.

A.03.07.04.a[02]: the use of system maintenance tools is controlled.

A.03.07.04.a[03]: the use of system maintenance tools is monitored.

A.03.07.04.b: maintenance tools are inspected for improper or unauthorized modifications.

A.03.07.04.c: media that contain diagnostic and test programs are checked for malicious code before being used in the system.

A.03.07.04.d: the removal of system maintenance equipment containing CUI is prevented by verifying that there is no CUI on the equipment; sanitizing or destroying the equipment; or retaining the equipment within the facility.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: maintenance policy and procedures; procedures for system maintenance tools; system maintenance tools; maintenance tool inspection records; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with system maintenance responsibilities; personnel responsible for media sanitization; personnel with information security responsibilities]

Test

[SELECT FROM: processes for approving, controlling, and monitoring maintenance tools; mechanisms for supporting and/or implementing the approval, control, and/or monitoring of maintenance tools; processes for preventing the unauthorized removal of information; processes for inspecting media for malicious code; mechanisms for supporting media sanitization or the destruction of equipment; mechanisms for supporting the verification of media sanitization; processes for inspecting maintenance tools; mechanisms for supporting and/or implementing the inspection of maintenance tools; mechanisms for supporting and/or implementing the inspection of media used for maintenance]

REFERENCES

Source Assessment Procedures: MA-03, MA-03(01), MA-03(02), MA-03(03)

3.7.5. Nonlocal Maintenance

REQUIREMENT: 03.07.05

ASSESSMENT OBJECTIVE

Determine if:

A.03.07.05.a[01]: nonlocal maintenance and diagnostic activities are approved.

A.03.07.05.a[02]: nonlocal maintenance and diagnostic activities are monitored.

A.03.07.05.b: multi-factor authentication and replay resistance are implemented in the establishment of nonlocal maintenance and diagnostic sessions.

A.03.07.05.c[01]: session connections are terminated when nonlocal maintenance is completed.

A.03.07.05.c[02]: network connections are terminated when nonlocal maintenance is completed.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: maintenance policy and procedures; remote access policy and procedures; procedures for nonlocal system maintenance; records of remote access; maintenance records; diagnostic records; system design documentation; system configuration settings; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with system maintenance responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for managing nonlocal maintenance; mechanisms for implementing, supporting, and/or managing nonlocal maintenance; mechanisms for implementing multi-factor authentication and replay resistance; mechanisms for terminating nonlocal maintenance sessions and network connections]

REFERENCES

Source Assessment Procedure: MA-04

3.7.6. Maintenance Personnel

REQUIREMENT: 03.07.06

ASSESSMENT OBJECTIVE

Determine if:

A.03.07.06.a: a process for maintenance personnel authorization is established.

A.03.07.06.b: a list of authorized maintenance organizations or personnel is maintained.

A.03.07.06.c: verification is performed that non-escorted personnel who perform maintenance on the system possess the required access authorizations.

A.03.07.06.d: organizational personnel with required access authorizations and technical competence are designated to supervise the maintenance activities of personnel who do not possess the required access authorizations.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: maintenance policy and procedures; service provider contracts; service-level agreements; list of authorized personnel; maintenance records; access control records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with system maintenance responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: processes for authorizing and managing maintenance personnel; mechanisms for supporting and/or implementing the authorization of maintenance personnel]

REFERENCES

Source Assessment Procedure: MA-05

3.8. Media Protection

3.8.1. Media Storage

REQUIREMENT: 03.08.01

ASSESSMENT OBJECTIVE

Determine if:

A.03.08.01[01]: system media that contain CUI are physically controlled until the media are sanitized or destroyed using approved equipment, techniques, and procedures.

A.03.08.01[02]: system media that contain CUI are securely stored until the media are sanitized or destroyed using approved equipment, techniques, and procedures.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: physical protection policy and procedures; media protection policy and procedures; procedures for media storage; access control policy and procedures; system media; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with system media protection and storage responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: processes for storing information media; mechanisms for supporting and/or implementing secure media storage/media protection]

REFERENCES

Source Assessment Procedure: MP-04

3.8.2. Media Access

REQUIREMENT: 03.08.02

ASSESSMENT OBJECTIVE

Determine if:

A.03.08.02: access to CUI on system media is restricted.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: physical protection policy and procedures; media protection policy and procedures; procedures for media access restrictions; access control policy and procedures; media storage facilities; access control records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with system media protection responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for restricting information on media; mechanisms supporting and/or implementing media access restrictions]

REFERENCES

Source Assessment Procedure: MP-02

3.8.3. Media Sanitization

REQUIREMENT: 03.08.03

ASSESSMENT OBJECTIVE

Determine if:

A.03.08.03: system media that contain CUI are sanitized prior to disposal, release out of organizational control, or release for reuse.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: media protection policy and procedures; procedures for media sanitization and disposal; applicable standards and policies that address media sanitization policy; system audit records; media sanitization records; system design documentation; system configuration settings; records retention and disposition policy; records retention and disposition procedures; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with media sanitization responsibilities; personnel with records retention and disposition responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for media sanitization; mechanisms for supporting and/or implementing media sanitization]

REFERENCES

Source Assessment Procedure: MP-06

3.8.4. Media Marking

REQUIREMENT: 03.08.04

ASSESSMENT OBJECTIVE

Determine if:

A.03.08.04[01]: system media that contain CUI are marked to indicate distribution limitations.

A.03.08.04[02]: system media that contain CUI are marked to indicate handling caveats.

A.03.08.04[03]: system media that contain CUI are marked to indicate security markings.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: physical protection policy and procedures; media protection policy and procedures; procedures for media marking; list of system media marking security attributes; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with system media protection and marking responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: processes for marking information media; mechanisms for supporting and/or implementing media marking]

REFERENCES

Source Assessment Procedure: MP-03

3.8.5. Media Transport

REQUIREMENT: 03.08.05

ASSESSMENT OBJECTIVE

Determine if:

A.03.08.05.a[01]: system media that contain CUI are protected during transport outside of controlled areas.

A.03.08.05.a[02]: system media that contain CUI are controlled during transport outside of controlled areas.

A.03.08.05.b: the accountability of system media that contain CUI is maintained during transport outside of controlled areas.

A.03.08.05.c: cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI stored on digital media during transport.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: physical protection policy and procedures; media protection policy and procedures; procedures for media storage; access control policy and procedures; authorized personnel list; system media; designated controlled areas; system and communications protection policy and procedures; cryptographic mechanisms and configuration documentation; procedures for the protection of information at rest; system design documentation; system configuration settings; list of information at rest requiring confidentiality protections; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with system media protection and storage responsibilities; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: processes for storing information media; mechanisms for supporting and/or implementing media storage/media protection; mechanisms for supporting and/or implementing confidentiality protections for information at rest]

REFERENCES

Source Assessment Procedures: MP-05, SC-28, SC-28(01)

3.8.6. Withdrawn

Incorporated into 03.08.05.

3.8.7. Media Use

REQUIREMENT: 03.08.07

ASSESSMENT OBJECTIVE

Determine if:

A.03.08.07.ODP[01]: ***the types of system media with usage restrictions or that are prohibited from use are defined***.

A.03.08.07.a: the use of the following types of system media is restricted or prohibited: ***<A.03.08.07.ODP[01]: types of system media>***.

A.03.08.07.b: the use of removable system media without an identifiable owner is prohibited.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system media protection policy and procedures; system use policy; procedures for media usage restrictions; rules of behavior; system design documentation; audit records; system configuration settings; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with system media use responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for media use; mechanisms for restricting or prohibiting the use of system media on systems or system components]

REFERENCES

Source Assessment Procedure: MP-07

3.8.8. Withdrawn

Incorporated into 03.08.07.

3.8.9. System Backup – Cryptographic Protection

REQUIREMENT: 03.08.09

ASSESSMENT OBJECTIVE

Determine if:

A.03.08.09: cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI at backup storage locations.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: contingency planning policy and procedures; procedures for system backup; contingency plan; system design documentation; system configuration settings; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with system backup responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: mechanisms for supporting and/or implementing the cryptographic protection of backup information]

REFERENCES

Source Assessment Procedure: CP-09(08)

3.9. Personnel Security

3.9.1. Personnel Screening

REQUIREMENT: 03.09.01

ASSESSMENT OBJECTIVE

Determine if:

A.03.09.01.ODP[01]: ***the conditions that require the rescreening of individuals are defined***.

A.03.09.01.a: individuals are screened prior to authorizing access to the system.

A.03.09.01.b: individuals are rescreened in accordance with the following conditions: ***<A.03.09.01.ODP[01]: conditions>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: personnel security policy and procedures; procedures for personnel screening; records of screened personnel; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with personnel security responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: processes for personnel screening]

REFERENCES

Source Assessment Procedure: PS-03

3.9.2. Personnel Termination and Transfer

REQUIREMENT: 03.09.02

ASSESSMENT OBJECTIVE

Determine if:

A.03.09.02.ODP[01]: ***the time period within which to disable system access is defined***.

A.03.09.02.ODP[02]: ***the time period within which transfer or reassignment actions must occur following an individual transfer or reassignment is defined***.

A.03.09.02.ODP[03]: ***the transfer or reassignment actions to be initiated following transfer or reassignment are defined***.

A.03.09.02.a.01: upon the termination of individual employment, system access is disabled within ***<A.03.09.02.ODP[01]: time period>***.

A.03.09.02.a.02: upon the termination of individual employment, authenticators and credentials associated with the individual are terminated or revoked.

A.03.09.02.a.03: upon the termination of individual employment, security-related system property is retrieved.

A.03.09.02.b.01: upon individual reassignment or transfer to other positions in the organization, the ongoing operational need for current logical and physical access authorizations to the system and facility are reviewed and confirmed.

A.03.09.02.b.02: upon individual reassignment or transfer to other positions in the organization, the following transfer or reassignment actions are initiated within ***<A.03.09.02.ODP[02]: time period>***: ***<A.03.09.02.ODP[03]: transfer or reassignment actions>***.

A.03.09.02.b.03: upon individual reassignment or transfer to other positions in the organization, access authorization is modified to correspond with any changes in operational need.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: personnel security policy and procedures; procedures for personnel termination; records of personnel transfer actions; procedures for personnel transfer; list of system and facility access authorizations; records of personnel termination actions; records of terminated or revoked authenticators or credentials; list of system accounts; records of exit interviews; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with personnel security responsibilities; personnel with account management responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for personnel termination; processes for personnel transfer; mechanisms for supporting and/or implementing personnel transfer notifications; mechanisms for supporting and/or implementing personnel termination notifications; mechanisms for disabling system access and revoking authenticators]

REFERENCES

Source Assessment Procedures: PS-04, PS-05

3.10. Physical Protection

3.10.1. Physical Access Authorizations

REQUIREMENT: 03.10.01

ASSESSMENT OBJECTIVE

Determine if:

A.03.10.01.a[01]: a list of individuals with authorized access to the physical location where the system resides is developed.

A.03.10.01.a[02]: a list of individuals with authorized access to the physical location where the system resides is approved.

A.03.10.01.a[03]: a list of individuals with authorized access to the physical location where the system resides is maintained.

A.03.10.01.b: authorization credentials are issued for facility access.

A.03.10.01.c: the physical access list is reviewed periodically.

A.03.10.01.d: individuals from the physical access list are removed when access is no longer required.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: physical protection policy and procedures; procedures for physical access authorizations; authorized personnel access list; physical access list reviews; physical access termination records; authorization credentials; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with physical access authorization responsibilities; personnel with physical access to the facility where the system resides; personnel with information security responsibilities]

Test

[SELECT FROM: processes for physical access authorizations; mechanisms for supporting and/or implementing physical access authorizations]

REFERENCES

Source Assessment Procedure: PE-02

3.10.2. Monitoring Physical Access

REQUIREMENT: 03.10.02

ASSESSMENT OBJECTIVE

Determine if:

A.03.10.02.a[01]: physical access to the location where the system resides is monitored to detect physical security incidents.

A.03.10.02.a[02]: physical access to the location where the system resides is monitored to respond to physical security incidents.

A.03.10.02.b: physical access logs are reviewed periodically.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: physical protection policy and procedures; procedures for physical access monitoring; physical access logs or records; physical access monitoring records; physical access log reviews; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with physical access monitoring responsibilities; personnel with incident response responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: processes for monitoring physical access; mechanisms supporting and/or implementing physical access monitoring; mechanisms supporting and/or implementing the review of physical access logs]

REFERENCES

Source Assessment Procedure: PE-06

3.10.3. Withdrawn

Incorporated into 03.10.07.

3.10.4. Withdrawn

Incorporated into 03.10.07.

3.10.5. Withdrawn

Incorporated into 03.10.07.

3.10.6. Alternate Work Site

REQUIREMENT: 03.10.06

ASSESSMENT OBJECTIVE

Determine if:

A.03.10.06.ODP[01]: ***the security requirements to be employed at alternate work sites are defined***.

A.03.10.06.a: alternate work sites allowed for use by employees are defined.

A.03.10.06.b: the following security requirements are employed at alternate work sites: ***<A.03.10.06.ODP[01]: security requirements>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: physical protection policy and procedures; procedures for alternate work sites for personnel; list of security requirements for alternate work sites; assessments of security requirements at alternate work sites; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel approving the use of alternate work sites; personnel using alternate work sites; personnel assessing security requirements at alternate work sites; personnel with information security responsibilities]

Test

[SELECT FROM: processes for security at alternate work sites; mechanisms for supporting alternate work sites; security requirements employed at alternate work sites; means of communication between personnel at alternate work sites and security personnel]

REFERENCES

Source Assessment Procedure: PE-17

3.10.7. Physical Access Control

REQUIREMENT: 03.10.07

ASSESSMENT OBJECTIVE

Determine if:

A.03.10.07.ODP[01]: ***the circumstances requiring visitor escorts and control of visitor activity are defined***.

A.03.10.07.a.01: physical access is controlled at the location where the system resides by verifying individual physical access authorizations before granting access.

A.03.10.07.a.02: physical access is controlled at the location where the system resides by controlling ingress and egress with physical access control systems/devices or guards.

A.03.10.07.b: physical access audit logs for entry or exit points are maintained.

A.03.10.07.c[01]: visitors are escorted.

A.03.10.07.c[02]: visitor activity is controlled under the following circumstances: ***<A.03.10.07.ODP[01]: circumstances>***.

A.03.10.07.d[01]: keys are secured.

A.03.10.07.d[02]: combinations are secured.

A.03.10.07.d[03]: other physical access devices are secured.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: physical protection policy and procedures; procedures for physical access control; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with physical access control responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: processes for physical access control; mechanisms for supporting and/or implementing physical access control; physical access control devices]

REFERENCES

Source Assessment Procedure: PE-03

3.10.8. Access Control for Transmission and Output Devices

REQUIREMENT: 03.10.08

ASSESSMENT OBJECTIVE

Determine if:

A.03.10.08.a: physical access to system distribution and transmission lines in organizational facilities is controlled.

A.03.10.08.b: physical access to output devices is controlled to prevent unauthorized individuals from obtaining access to CUI.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: physical protection policy and procedures; procedures for access control for transmission mediums; system design documentation; facility communications and wiring diagrams; list of physical security safeguards applied to system distribution and transmission lines; procedures for access control for display medium; facility layout of system components; actual displays from system components; list of output devices and associated outputs that require physical access controls; physical access control logs or records for areas containing output devices and related outputs; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with physical access control responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: processes for access control for distribution and transmission lines; mechanisms for supporting and/or implementing access control for distribution and transmission lines; processes for access control to output devices; mechanisms for supporting and/or implementing access control for output devices]

REFERENCES

Source Assessment Procedures: PE-04, PE-05

3.11. Risk Assessment

3.11.1. Risk Assessment

REQUIREMENT: 03.11.01

ASSESSMENT OBJECTIVE

Determine if:

A.03.11.01.a: the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI is assessed.

A.03.11.01.b: risk assessments are updated periodically.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: risk assessment policy and procedures; security planning policy and procedures; procedures for organizational assessments of risk; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; SCRM policy and procedures; inventory of critical systems, system components, and system services; procedures for organizational assessments of supply chain risk; acquisition policy; SCRM plan; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with risk assessment responsibilities; personnel with SCRM responsibilities; personnel with security responsibilities]

Test

[SELECT FROM: processes for organizational risk assessments; mechanisms for supporting and/or conducting, documenting, reviewing, disseminating, and updating risk assessments; mechanisms supporting and/or conducting, documenting, reviewing, disseminating, and updating supply chain risk assessments]

REFERENCES

Source Assessment Procedures: RA-03, RA-03(01), SR-06

3.11.2. Vulnerability Monitoring and Scanning

REQUIREMENT: 03.11.02

ASSESSMENT OBJECTIVE

Determine if:

A.03.11.02.ODP[01]: ***response times to remediate system vulnerabilities are defined***.

A.03.11.02.a[01]: the system is monitored for vulnerabilities periodically.

A.03.11.02.a[02]: the system is monitored for vulnerabilities when new vulnerabilities that affect the system are identified.

A.03.11.02.a[03]: the system is scanned for vulnerabilities periodically.

A.03.11.02.a[04]: the system is scanned for vulnerabilities when new vulnerabilities that affect the system are identified.

A.03.11.02.b: system vulnerabilities are remediated ***<A.03.11.02.ODP[01]: response times>***.

A.03.11.02.c[01]: system vulnerabilities to be scanned are updated periodically.

A.03.11.02.c[02]: system vulnerabilities to be scanned are updated when new vulnerabilities are identified.

A.03.11.02.c[03]: system vulnerabilities to be scanned are updated when new vulnerabilities are reported.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: risk assessment policy and procedures; procedures for vulnerability scanning; patch and vulnerability management records; vulnerability scanning tools and configuration documentation; vulnerability scanning results; risk assessment; risk assessment report; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with risk assessment and vulnerability scanning responsibilities; personnel with vulnerability scan analysis responsibilities; personnel with vulnerability remediation responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for vulnerability scanning, analysis, and remediation; mechanisms for supporting and/or implementing vulnerability scanning, analysis, and remediation]

REFERENCES

Source Assessment Procedures: RA-05, RA-05(02)

3.11.3. Withdrawn

Incorporated into 03.11.02.

3.12. Security Assessment and Monitoring

3.12.1. Security Assessment

REQUIREMENT: 03.12.01

ASSESSMENT OBJECTIVE

Determine if:

A.03.12.01: the security requirements for the system and its environment of operation are assessed periodically to determine if the requirements have been satisfied.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: security assessment and monitoring policy and procedures; procedures for security assessment planning; security assessment plan; security assessment report; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with security assessment responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: mechanisms supporting security assessments, processes for security assessment plan development and/or security assessment reporting]

REFERENCES

Source Assessment Procedure: CA-02

3.12.2. Plan of Action and Milestones

REQUIREMENT: 03.12.02

ASSESSMENT OBJECTIVE

Determine if:

A.03.12.02.a.01: a plan of action and milestones for the system is developed to document the planned remediation actions for correcting weaknesses or deficiencies noted during security assessments.

A.03.12.02.a.02: a plan of action and milestones for the system is developed to reduce or eliminate known system vulnerabilities.

A.03.12.02.b[01]: the existing plan of action and milestones is updated periodically based on the findings from security assessments.

A.03.12.02.b[02]: the existing plan of action and milestones is updated periodically based on the findings from independent audits or reviews.

A.03.12.02.b[03]: the existing plan of action and milestones is updated periodically based on the findings from continuous monitoring activities.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: security assessment and monitoring policy and procedures; procedures for plans of action and milestones; security assessment plan; security assessment report; security assessment evidence; plan of action and milestones; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with plans of action and milestones development and implementation responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: mechanisms for developing, implementing, and maintaining plans of action and milestones]

REFERENCES

Source Assessment Procedure: CA-05

3.12.3. Continuous Monitoring

REQUIREMENT: 03.12.03

ASSESSMENT OBJECTIVE

Determine if:

A.03.12.03[01]: a system-level continuous monitoring strategy is developed and implemented.

A.03.12.03[02]: ongoing monitoring is included in the continuous monitoring strategy.

A.03.12.03[03]: security assessments are included the continuous monitoring strategy.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: security assessment and monitoring policy and procedures; organizational continuous monitoring strategy; system-level continuous monitoring strategy; procedures for continuous monitoring of the system; procedures for configuration management; security assessment report; plan of action and milestones; system monitoring records; configuration management records; impact analyses; status reports; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with continuous monitoring responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: mechanisms for implementing continuous monitoring; mechanisms supporting response actions for assessment and monitoring results; mechanisms for supporting security status reporting]

REFERENCES

Source Assessment Procedure: CA-07

3.12.4. Withdrawn

Incorporated into 03.15.02.

3.12.5. Information Exchange

REQUIREMENT: 03.12.05

ASSESSMENT OBJECTIVE

Determine if:

A.03.12.05.ODP[01]: ***one or more of the following parameter values is/are selected: {interconnection security agreements; information exchange security agreements;***

memoranda of understanding or agreement; service-level agreements; user agreements; non-disclosure agreements}.

A.03.12.05.a: the exchange of CUI between the system and other systems is approved and managed using ***<A.03.12.05.ODP[01]: selected parameter value(s)>***.

A.03.12.05.b[01]: interface characteristics are documented as part of the exchange agreements.

A.03.12.05.b[02]: security requirements are documented as part of the exchange agreements.

A.03.12.05.b[03]: responsibilities for each system are documented as part of the exchange agreements.

A.03.12.05.c[01]: exchange agreements are reviewed periodically.

A.03.12.05.c[02]: exchange agreements are updated periodically.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; procedures for system connections; system and communications protection policy and procedures; system interconnection security agreements; information exchange security agreements; service-level agreements; memoranda of understanding or agreements; non-disclosure agreements; system design documentation; enterprise architecture; security architecture; system configuration settings; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with development, implementation, and approval responsibilities for system interconnection agreements; personnel who manage systems to which the exchange agreements apply; personnel with information security responsibilities]

REFERENCES

Source Assessment Procedure: CA-03

3.13. System and Communications Protection

3.13.1. Boundary Protection

REQUIREMENT: 03.13.01

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.01.a[01]: communications at external managed interfaces to the system are monitored.

A.03.13.01.a[02]: communications at external managed interfaces to the system are controlled.

A.03.13.01.a[03]: communications at key internal managed interfaces within the system are monitored.

A.03.13.01.a[04]: communications at key internal managed interfaces within the system are controlled.

A.03.13.01.b: subnetworks are implemented for publicly accessible system components that are physically or logically separated from internal networks.

A.03.13.01.c: external system connections are only made through managed interfaces that consist of boundary protection devices arranged in accordance with an organizational security architecture.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and communications protection policy and procedures; procedures for boundary protection; list of key internal boundaries within the system; boundary protection hardware and software; system configuration settings; security architecture; system audit records; system design documentation; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with boundary protection responsibilities; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for implementing boundary protection capabilities]

REFERENCES

Source Assessment Procedure: SC-07

3.13.2. Withdrawn

Recategorized as NCO.

3.13.3. Withdrawn

Addressed by 03.01.04, 03.01.05, 03.01.06, and 03.01.07.

3.13.4. Information in Shared System Resources

REQUIREMENT: 03.13.04

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.04[01]: unauthorized information transfer via shared system resources is prevented.

A.03.13.04[02]: unintended information transfer via shared system resources is prevented.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and communications protection policy and procedures; procedures for information protection in shared system resources; system configuration settings; system audit records; system design documentation; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for preventing the unauthorized and unintended transfer of information via shared system resources]

REFERENCES

Source Assessment Procedure: SC-04

3.13.5. Withdrawn

Incorporated into 03.13.01.

3.13.6. Network Communications – Deny by Default – Allow by Exception

REQUIREMENT: 03.13.06

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.06[01]: network communications traffic is denied by default.

A.03.13.06[02]: network communications traffic is allowed by exception.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and communications protection policy and procedures; procedures for boundary protection; system design documentation; system configuration settings; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with boundary protection responsibilities; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for implementing traffic management at managed interfaces]

REFERENCES

Source Assessment Procedure: SC-07(05)

3.13.7. Withdrawn

Addressed by 03.01.12, 03.04.02 and 03.04.06.

3.13.8. Transmission and Storage Confidentiality

REQUIREMENT: 03.13.08

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.08[01]: cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI during transmission.

A.03.13.08[02]: cryptographic mechanisms are implemented to prevent the unauthorized disclosure of CUI while in storage.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and communications protection policy and procedures; procedures for transmission confidentiality; procedures for the protection of information at rest; system design documentation; system configuration settings; cryptographic mechanisms and associated configuration documentation; information in storage requiring confidentiality protection; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for supporting and/or implementing transmission confidentiality; cryptographic mechanisms for supporting and/or implementing transmission confidentiality; mechanisms for supporting and/or implementing confidentiality protection for information in storage; cryptographic mechanisms implementing confidentiality protections for information in storage]

REFERENCES

Source Assessment Procedures: SC-08, SC-08(01), SC-28, SC-28(01)

3.13.9. Network Disconnect

REQUIREMENT: 03.13.09

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.09: network connections associated with communications sessions are terminated at the end of the sessions or after periods of inactivity.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and communications protection policy and procedures; procedures for network disconnect; system design documentation; system configuration settings; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for supporting and/or implementing a network disconnect capability]

REFERENCES

Source Assessment Procedure: SC-10

3.13.10. Cryptographic Key Establishment and Management

REQUIREMENT: 03.13.10

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.10.ODP[01]: ***requirements for key establishment and management are defined***.

A.03.13.10[01]: cryptographic keys are established in the system in accordance with the following key management requirements: ***<A.03.13.10.ODP[01]: requirements>***.

A.03.13.10[02]: cryptographic keys are managed in the system in accordance with the following key management requirements: ***<A.03.13.10.ODP[01]: requirements>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and communications protection policy and procedures; procedures for cryptographic key establishment and management; system design documentation; system configuration settings; cryptographic mechanisms; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for cryptographic key establishment and/or management; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: mechanisms for supporting and/or implementing cryptographic key establishment and management]

REFERENCES

Source Assessment Procedure: SC-12

3.13.11. Cryptographic Protection

REQUIREMENT: 03.13.11

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.11.ODP[01]: ***the types of cryptography for protecting the confidentiality of CUI are defined***.

A.03.13.11: the following types of cryptography are implemented when used to protect the confidentiality of CUI: ***<A.03.13.11.ODP[01]: types of cryptography>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and communications protection policy and procedures; procedures for cryptographic protection; system design documentation; system configuration settings; cryptographic module validation certificates; list of FIPS-validated cryptographic modules; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for cryptographic protection; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms for supporting and/or implementing cryptographic protection]

REFERENCES

Source Assessment Procedure: SC-13

3.13.12. Collaborative Computing Devices and Applications

REQUIREMENT: 03.13.12

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.12.a: remote activation of collaborative computing devices and applications is prohibited.

A.03.13.12.b: an explicit indication of use is provided to users who are physically present at the devices.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and communications protection policy and procedures; procedures for collaborative computing; access control policy and procedures; system configuration settings; system design documentation; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for managing collaborative computing devices; personnel with information security responsibilities; system developers; system administrators]

Test

[SELECT FROM: mechanisms supporting and/or implementing the management of remote activation of collaborative computing devices; mechanisms for providing an indication of use of collaborative computing devices]

REFERENCES

Source Assessment Procedure: SC-15

3.13.13. Mobile Code

REQUIREMENT: 03.13.13

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.13.a[01]: acceptable mobile code is defined.

A.03.13.13.a[02]: acceptable mobile code technologies are defined.

A.03.13.13.b[01]: the use of mobile code is authorized.

A.03.13.13.b[02]: the use of mobile code is monitored.

A.03.13.13.b[03]: the use of mobile code is controlled.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and communications protection policy and procedures; procedures for mobile code; mobile code implementation policy and procedures; list of acceptable mobile code and mobile code technologies; authorization records; system monitoring records; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for managing mobile code; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for authorizing, monitoring, and controlling mobile code; mechanisms for supporting and/or implementing the management of mobile code; mechanisms for supporting and/or implementing mobile code monitoring]

REFERENCES

Source Assessment Procedure: SC-18

3.13.14. Withdrawn

Technology-specific.

3.13.15. Session Authenticity

REQUIREMENT: 03.13.15

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.15: the authenticity of communications sessions is protected.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and communications protection policy and procedures; procedures for session authenticity; system design documentation; system configuration settings; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: mechanisms for supporting and/or implementing session authenticity]

REFERENCES

Source Assessment Procedure: SC-23

3.13.16. Withdrawn

Incorporated into 03.13.08.

3.14. System and Information Integrity

3.14.1. Flaw Remediation

REQUIREMENT: 03.14.01

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.01.ODP[01]: ***time period within which to install security-relevant software updates after the release of the updates is defined***.

A.03.14.01.ODP[02]: ***time period within which to install security-relevant firmware updates after the release of the updates is defined***.

A.03.14.01.a[01]: system flaws are identified.

A.03.14.01.a[02]: system flaws are reported.

A.03.14.01.a[03]: system flaws are corrected.

A.03.14.01.b[01]: security-relevant software updates are installed within ***<A.03.14.01.ODP[01]: time period>*** of the release of the updates.

A.03.14.01.b[02]: security-relevant firmware updates are installed within ***<A.03.14.01.ODP[02]: time period>*** of the release of the updates.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and information integrity policy and procedures; procedures for flaw remediation; procedures for configuration management; list of recent security flaw remediation actions performed on the system; list of flaws and vulnerabilities that may potentially affect the system; test results from the installation of software and firmware updates to correct system flaws; installation and change control records for security-relevant software and firmware updates; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel responsible for installing, configuring, and/or maintaining the system; personnel responsible for flaw remediation; personnel with configuration management responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for identifying, reporting, and correcting system flaws; processes for installing software and firmware updates; mechanisms for supporting and/or implementing the reporting and correction of system flaws; mechanisms for supporting and/or implementing the testing software and firmware updates]

REFERENCES

Source Assessment Procedure: SI-02

3.14.2. Malicious Code Protection

REQUIREMENT: 03.14.02

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.02.ODP[01]: ***the frequency at which malicious code protection mechanisms perform scans is defined***.

A.03.14.02.a[01]: malicious code protection mechanisms are implemented at designated locations within the system to detect malicious code.

A.03.14.02.a[02]: malicious code protection mechanisms are implemented at designated locations within the system to eradicate malicious code.

A.03.14.02.b: malicious code protection mechanisms are updated as new releases are available in accordance with configuration management policy and procedures.

A.03.14.02.c.01[01]: malicious code protection mechanisms are configured to perform scans of the system ***<A.03.14.02.ODP[01]: the frequency>***.

A.03.14.02.c.01[02]: malicious code protection mechanisms are configured to perform real-time scans of files from external sources at endpoints or network entry and exit points as the files are downloaded, opened, or executed.

A.03.14.02.c.02: malicious code protection mechanisms are configured to block malicious code, quarantine malicious code, or take other actions in response to malicious code detection.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and information integrity policy and procedures; configuration management policy and procedures; procedures for malicious code protection; records of malicious code protection updates; system design documentation; system configuration settings; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel responsible for malicious code protection; personnel with system installation, configuration, and/or maintenance responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for employing, updating, and configuring malicious code protection mechanisms; processes for addressing the detection of false positives and resulting potential impacts; mechanisms for supporting and/or implementing, employing, updating, and configuring malicious code protection mechanisms; mechanisms for supporting and/or implementing malicious code scanning and the execution of subsequent actions]

REFERENCES

Source Assessment Procedure: SI-03

3.14.3. Security Alerts, Advisories, and Directives

REQUIREMENT: 03.14.03

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.03.a: system security alerts, advisories, and directives from external organizations are received on an ongoing basis.

A.03.14.03.b[01]: internal security alerts, advisories, and directives are generated, as necessary.

A.03.14.03.b[02]: internal security alerts, advisories, and directives are disseminated, as necessary.

A.03.14.03.c: security directives are implemented in accordance with established time frames.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and information integrity policy and procedures; procedures for security alerts, advisories, and directives; records of security alerts and advisories; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with security alert and advisory responsibilities; personnel implementing, operating, maintaining, and using the system; personnel, organizational elements, and/or external organizations to whom alerts, advisories, and directives are to be disseminated; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives; mechanisms for supporting and/or implementing security directives; mechanisms for supporting and/or implementing the definition, receipt, generation, and dissemination of security alerts, advisories, and directives]

REFERENCES

Source Assessment Procedure: SI-05

3.14.4. Withdrawn

Incorporated into 03.14.02.

3.14.5. Withdrawn

Addressed by 03.14.02.

3.14.6. System Monitoring

REQUIREMENT: 03.14.06

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.06.a.01: the system is monitored to detect attacks and indicators of potential attacks.

A.03.14.06.a.02: the system is monitored to detect unauthorized connections.

A.03.14.06.b: unauthorized use of the system is identified.

A.03.14.06.c[01]: inbound communications traffic is monitored to detect unusual or unauthorized activities or conditions.

A.03.14.06.c[02]: outbound communications traffic is monitored to detect unusual or unauthorized activities or conditions.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and information integrity policy and procedures; procedures for system monitoring tools and techniques; continuous monitoring strategy; facility diagram or layout; system design documentation; locations within the system where monitoring devices are deployed; system configuration settings; system protocols; system audit records; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with responsibilities for installing, configuring, and/or maintaining the system; personnel with system monitoring responsibilities; personnel with intrusion detection responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing system monitoring capabilities; mechanisms for supporting and/or implementing intrusion detection and system monitoring capabilities; mechanisms supporting and/or implementing the monitoring of inbound and outbound communications traffic]

REFERENCES

Source Assessment Procedures: SI-04, SI-04(04)

3.14.7. Withdrawn

Incorporated into 03.14.06.

3.14.8. Information Management and Retention

REQUIREMENT: 03.14.08

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.08[01]: CUI within the system is managed in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.

A.03.14.08[02]: CUI within the system is retained in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.

A.03.14.08[03]: CUI output from the system is managed in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.

A.03.14.08[04]: CUI output from the system is retained in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and information integrity policy and procedures; laws, Executive Orders, directives, policies, regulations, standards, and operational requirements applicable to information management and retention; records retention and disposition policy; records retention and disposition procedures; media protection policy; media protection procedures; audit findings; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with information and records management, retention, and disposition responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for information management, retention, and disposition; mechanisms for supporting and/or implementing information management, retention, and disposition]

REFERENCES

Source Assessment Procedure: SI-12

3.15. Planning

3.15.1. Policy and Procedures

REQUIREMENT: 03.15.01

ASSESSMENT OBJECTIVE

Determine if:

A.03.15.01.a[01]: policies for implementing security requirements are developed and documented.

A.03.15.01.a[02]: policies for implementing security requirements are disseminated to organizational personnel or roles.

A.03.15.01.a[03]: procedures needed to implement security requirements are developed and documented.

A.03.15.01.a[04]: procedures needed to implement security requirements are disseminated to organizational personnel or roles.

A.03.15.01.b[01]: policies and procedures are reviewed periodically.

A.03.15.01.b[02]: policies and procedures are updated periodically.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: security policies and procedures associated with the protection of CUI; audit findings; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with information security responsibilities]

REFERENCES

Source Assessment Procedures: AC-01, AT-01, AU-01, CA-01, CM-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PS-01, RA-01, SA-01, SC-01, SI-01, SR-01

3.15.2. System Security Plan

REQUIREMENT: 03.15.02

ASSESSMENT OBJECTIVE

Determine if:

A.03.15.02.a.01: a system security plan that defines the constituent system components is developed.

A.03.15.02.a.02: a system security plan that describes the system operating environment is developed.

A.03.15.02.a.03: a system security plan that describes any specific threats to the system that are of concern to the organization is developed.

A.03.15.02.a.04: a system security plan that provides an overview of the security requirements for the system is developed.

A.03.15.02.a.05: a system security plan that identifies connections to other systems is developed.

A.03.15.02.a.06: a system security plan that identifies individuals who fulfill system roles and responsibilities is developed.

A.03.15.02.a.07: a system security plan that includes other relevant information necessary for the protection of CUI is developed.

A.03.15.02.b[01]: the system security plan is reviewed periodically.

A.03.15.02.b[02]: the system security plan is updated periodically.

A.03.15.02.c: the system security plan is protected from unauthorized disclosure.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: security planning policy and procedures; procedures for system security plan development and implementation; procedures for security plan reviews and updates; enterprise architecture; system security plan; records of system security plan reviews and updates; risk assessments; risk assessment results; security architecture and design documentation; other relevant documents or records]

Interview

[SELECT FROM: personnel with system security planning and plan implementation responsibilities; system developers; personnel with information security responsibilities]

Test

[SELECT FROM: processes for system security plan development, review, update, and approval]

REFERENCES

Source Assessment Procedure: PL-02

3.15.3. Rules of Behavior

REQUIREMENT: 03.15.03

ASSESSMENT OBJECTIVE

Determine if:

A.03.15.03.a[01]: rules that describe responsibilities and expected behavior for handling CUI and system usage are established.

A.03.15.03.a[02]: rules of behavior for handling CUI and system usage are provided to individuals who require access to the system.

A.03.15.03.b: a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior is received before authorizing access to CUI and the system.

A.03.15.03.c[01]: the rules of behavior are reviewed periodically.

A.03.15.03.c[02]: the rules of behavior are updated periodically.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: security planning policy and procedures; rules of behavior for system users; signed acknowledgements of rules of behavior; records for rules of behavior reviews and updates; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with rules of behavior establishment, review, and update responsibilities; personnel with literacy training and awareness responsibilities; personnel with role-based training responsibilities; authorized users of the system who have signed rules of behavior; personnel with information security responsibilities]

Test

[SELECT FROM: processes for establishing, reviewing, disseminating, and updating rules of behavior; mechanisms for supporting and/or implementing the establishment, dissemination, review, and update of rules of behavior]

REFERENCES

Source Assessment Procedure: PL-04

3.16. System and Services Acquisition

3.16.1. Acquisition Process

REQUIREMENT: 03.16.01

ASSESSMENT OBJECTIVE

Determine if:

A.03.16.01.ODP[01]: ***the security requirements for the system, system component, or system service are defined***.

A.03.16.01: the following security requirements are included in the acquisition contract for the system, system component, or system service: ***<A.03.16.01.ODP[01]: security requirements>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and services acquisition policy and procedures; procedures for the integration of information security and SCRM into the acquisition process; configuration management plan; acquisition contracts for the system, system component, or system service; system design documentation; SCRM plan; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with acquisition/contracting responsibilities; personnel with SCRM responsibilities; personnel with information security responsibilities; system administrators]

Test

[SELECT FROM: processes for determining system security requirements; processes for developing acquisition contracts; mechanisms for supporting and/or implementing acquisitions and the inclusion of security requirements in contracts]

REFERENCES

Source Assessment Procedure: SA-04

3.16.2. Unsupported System Components

REQUIREMENT: 03.16.02

ASSESSMENT OBJECTIVE

Determine if:

A.03.16.02.a: system components are replaced when support for the components is no longer available from the developer, vendor, or manufacturer.

A.03.16.02.b: options for risk mitigation or alternative sources for continued support for unsupported components are provided if components cannot be replaced.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and services acquisition policy and procedures; procedures for the replacement or continued use of unsupported system components; documented evidence of replacing unsupported system components; documented approvals (including justification) for the continued use of unsupported system components; SCRM plan; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with system and service acquisition responsibilities; personnel responsible for component replacement; personnel with system development life cycle responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: processes for replacing unsupported system components; mechanisms for supporting and/or implementing the replacement of unsupported system components]

REFERENCES

Source Assessment Procedure: SA-22

3.16.3. External System Services

REQUIREMENT: 03.16.03

ASSESSMENT OBJECTIVE

Determine if:

A.03.16.03.ODP[01]: ***the security requirements to be employed by external system service providers are defined***.

A.03.16.03.a: the providers of external system services used for the processing, storage, or transmission of CUI comply with the following security requirements: ***<A.03.16.03.ODP[01]: security requirements>***.

A.03.16.03.b: user roles and responsibilities with regard to external system services, including shared responsibilities with external providers, are defined and documented.

A.03.16.03.c: processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis are implemented.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and services acquisition policy and procedures; procedures for monitoring security requirement compliance by external service providers; acquisition documentation; contracts; service-level agreements; interagency agreements; licensing agreements; list of security requirements for external provider services; assessment results or reports from external service providers; SCRM plan; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with acquisition responsibilities; external providers of system services; personnel with SCRM responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: organizational processes for monitoring security and privacy control compliance by external service providers on an ongoing basis; mechanisms for monitoring security and privacy control compliance by external service providers on an ongoing basis]

REFERENCES

Source Assessment Procedure: SA-09

3.17. Supply Chain Risk Management

3.17.1. Supply Chain Risk Management Plan

REQUIREMENT: 03.17.01

ASSESSMENT OBJECTIVE

Determine if:

A.03.17.01.a[01]: a plan for managing supply chain risks is developed.

A.03.17.01.a[02]: the SCRM plan addresses risks associated with the research and development of the system, system components, or system services.

A.03.17.01.a[03]: the SCRM plan addresses risks associated with the design of the system, system components, or system services.

A.03.17.01.a[04]: the SCRM plan addresses risks associated with the manufacturing of the system, system components, or system services.

A.03.17.01.a[05]: the SCRM plan addresses risks associated with the acquisition of the system, system components, or system services.

A.03.17.01.a[06]: the SCRM plan addresses risks associated with the delivery of the system, system components, or system services.

A.03.17.01.a[07]: the SCRM plan addresses risks associated with the integration of the system, system components, or system services.

A.03.17.01.a[08]: the SCRM plan addresses risks associated with the operations and maintenance of the system, system components, or system services.

A.03.17.01.a[09]: the SCRM plan addresses risks associated with the disposal of the system, system components, or system services.

A.03.17.01.b[01]: the SCRM plan is reviewed periodically.

A.03.17.01.b[02]: the SCRM plan is updated periodically.

A.03.17.01.c: the SCRM plan is protected from unauthorized disclosure.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: SCRM policy and procedures; SCRM plan; system and services acquisition policy and procedures; system and services acquisition procedures; procedures for supply chain protection; procedures for protecting the SCRM plan from unauthorized disclosure; system development life cycle procedures; procedures for the integration of information security requirements into the acquisition process; acquisition documentation; service-level agreements; acquisition contracts for the system, system components, or system services; list of supply chain threats; list of safeguards for supply chain threats; system life cycle documentation; inter-organizational agreements and procedures; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with acquisition responsibilities; personnel with SCRM responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: organizational processes for defining and documenting the system development life cycle (SDLC); organizational processes for identifying SDLC roles and responsibilities; organizational processes for integrating SCRM into the SDLC; mechanisms for supporting and/or implementing the SDLC]

REFERENCES

Source Assessment Procedure: SR-02

3.17.2. Acquisition Strategies, Tools, and Methods

REQUIREMENT: 03.17.02

ASSESSMENT OBJECTIVE

Determine if:

A.03.17.02[01]: acquisition strategies, contract tools, and procurement methods are developed and implemented to identify supply chain risks.

A.03.17.02[02]: acquisition strategies, contract tools, and procurement methods are developed and implemented to protect against supply chain risks.

A.03.17.02[03]: acquisition strategies, contract tools, and procurement methods are developed and implemented to mitigate supply chain risks.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: SCRM policy and procedures; SCRM plan; system and services acquisition policy and procedures; procedures for supply chain protection; procedures for the integration of information security requirements into the acquisition process; solicitation documentation; acquisition documentation (including purchase orders); service-level agreements; acquisition contracts for the system, system components, or services; documentation of training, education, and awareness programs for personnel regarding supply chain risk; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with acquisition responsibilities; personnel with SCRM responsibilities; personnel with information security responsibilities]

Test

[SELECT FROM: processes for defining and employing tailored acquisition strategies, contract tools, and procurement methods; mechanisms for supporting and/or implementing the definition and employment of tailored acquisition strategies, contract tools, and procurement methods]

REFERENCES

Source Assessment Procedure: SR-05

3.17.3. Supply Chain Requirements and Processes

REQUIREMENT: 03.17.03

ASSESSMENT OBJECTIVE

Determine if:

A.03.17.03.ODP[01]: ***the security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events are defined***.

A.03.17.03.a: a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes is established.

A.03.17.03.b: the following security requirements are enforced to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences of supply chain-related events: ***<A.03.17.03.ODP[01]: security requirements>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: SCRM policy and procedures; SCRM strategy; SCRM plan; systems and critical system components inventory documentation; system and services acquisition policy and procedures; procedures for the integration of security requirements into the acquisition process; solicitation documentation; acquisition documentation (including purchase orders); acquisition contracts for systems or services; service-level agreements; risk register documentation; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with acquisition responsibilities; personnel with information security responsibilities; personnel with SCRM responsibilities]

Test

[SELECT FROM: processes for identifying and addressing supply chain element and process deficiencies]

REFERENCES

Source Assessment Procedure: SR-03

References

[1] Federal Information Security Modernization Act (P.L. 113-283), December 2014. Available at https://www.govinfo.gov/app/details/PLAW-113publ283

[2] Office of Management and Budget Memorandum Circular A-130, Managing Information as a Strategic Resource, July 2016. Available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

[3] Ross RS, Pillitteri VY (2023) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-171r3 ipd, initial public draft. https://doi.org/10.6028/NIST.SP.800-171r3.ipd

[4] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[5] Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53Ar5

[6] International Organization for Standardization/International Electrotechnical Commission 15408-3:2017, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements, April 2017. https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

[7] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

[8] Committee on National Security Systems (2022) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS Instruction 4009. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[9] Executive Order 13556 (2010) Controlled Unclassified Information. (The White House, 2340 Washington, DC), DCPD-201000942, November 4, 2010. Available at https://www.govinfo.gov/app/details/DCPD-201000942

Appendix A. Acronyms

CNSS
Committee on National Security Systems

CUI
Controlled Unclassified Information

FIPS
Federal Information Processing Standards

FISMA
Federal Information Security Modernization Act

GRC
Governance, Risk, and Compliance

ODP
Organization-Defined Parameter

OMB
Office of Management and Budget

OSCAL
Open Security Controls Assessment Language

SCRM
Supply Chain Risk Management

SDLC
System Development Life Cycle

SP
Special Publication

Appendix B. Glossary

Appendix B provides definitions for the terminology used in NIST SP 800-171A. The definitions are consistent with the definitions contained in the Committee on National Security Systems (CNSS) Glossary [8] unless otherwise noted.

agency
Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency. [2]

assessment
See *security control assessment*.

assessor
See *security control assessor*.

controlled unclassified information
Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. [9]

information
Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. [2]

nonfederal organization
An entity that owns, operates, or maintains a nonfederal system.

nonfederal system
A system that does not meet the criteria for a federal system.

risk
A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [2]

security
A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach. [8]

security assessment
See *security control assessment*.

security control
The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information. [2]

security control assessment
The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization. [2]

system

See *information system*.

system security plan

A document that describes how an organization meets the security requirements for a system or plans to meet the requirements. In particular, the system security plan describes the system boundary, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other systems.

Appendix C. Change Log

This publication incorporates the following changes from the original edition (June 2018):

- Assessment procedures have been updated to be consistent with NIST SP 800-171, Revision 3 [3].
- Organization-defined parameters (ODPs) have been added to determination statements.
- A references section has been added to each assessment procedure providing a hyperlink to the source assessment procedure in NIST SP 800-53A [5].

Table 2 shows the changes incorporated into this publication. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either *editorial* or *substantive* in nature. Any potential updates to this document that are not yet published in an errata update or a formal revision, including additional issues and potential corrections, will be posted as they are identified. See the publication details for this report. The current release of this publication does not include any errata updates.

Table 2. Change Log

Publication ID	Date	Type of Edit	Change	Location