NIST Special Publication 800
NIST SP 800-171Ar3

Assessing Security Requirements for Controlled Unclassified Information

Ron Ross
Victoria Pillitteri

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

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

NIST Special Publication
NIST SP 800-171Ar3

Assessing Security Requirements for Controlled Unclassified Information

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

May 2024

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 equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified 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.

Publication History
Approved by the NIST Editorial Review Board on 2024-04-23
Supersedes NIST Special Publication 800-171A (June 2018) https://doi.org/10.6028/NIST.SP.800-171A

How to Cite this NIST Technical Series Publication:
Ross R, Pillitteri V (2024) 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. https://doi.org/10.6028/NIST.SP.800-171Ar3

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

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

Additional Information

Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/171/a/r3/final, including related content, potential updates, and document history.

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

Abstract

The protection of Controlled Unclassified Information (CUI) 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 organizations with assessment procedures and a methodology that can be used 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. Assessments can be conducted as independent, third-party assessments or as government-sponsored assessments. The assessments can be applied with various degrees of rigor based on customer-defined depth and coverage attributes.

Keywords

assessment; assessment method; assessment object; assessment procedure; assurance; Controlled Unclassified Information; coverage; FISMA; NIST Special Publication 800-171; NIST Special Publication 800-53A; nonfederal organization; nonfederal system; security assessment; security requirement.

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 the security assessment requirements set forth in contracts or agreements

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

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, Cristina Ritfeld, Derek Sappington, and Chris Enloe – 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, 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
- 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 that the security requirements have been satisfied. The scope of the security assessments conducted using the procedures described in this publication is 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 the evidence produced during assessments.
- Section 3 provides assessment procedures for the security requirements in SP 800-171, including assessment objectives and potential assessment methods and objects for each procedure.

[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 SP 800-39 [4] for additional information on organizational risk management and risk tolerance.

The following sections provide additional information to support the protection of CUI:

- References
- Appendix A: Acronyms
- Appendix B: Glossary
- Appendix C: Security Requirement Assessments
- Appendix D: Organization-Defined Parameters
- Appendix E: 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 SP 800-171 [3] 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 SP 800-171 are organized into 17 families, as illustrated in Table 1. The assessment procedures in Sec. 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 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, design documentation, and architectures) 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

[2] 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]).

operations, exercising an incident response plan, and monitoring network traffic). Individuals are the people applying the specifications, mechanisms, or activities described above.

Assessment methods define the nature and extent of the assessor's actions and are used to facilitate understanding, achieve clarification, or obtain evidence. The assessment methods include *examine*, *interview*, and *test*. The examine method is the process of reviewing, studying, inspecting, 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. See SP 800-53A, Appendix C, *Assessment Method Descriptions* [5].

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

03.01.06 Least Privilege – Privileged Accounts **Security Requirement Name**

ASSESSMENT OBJECTIVE **Multi-Part Determination Statement and ODP for Security Requirement**

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 non-security functions or non-security 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)

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 or letters (e.g., 03.01.01.e or 03.01.01.f.02) indicates the security requirement identifier from NIST 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.

2.2. Assurance Cases

Building an effective assurance case to determine compliance with security requirements 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 security assessments conducted using the procedures in this publication, that claim is "compliance" with the security requirements in 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

[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].

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 with the security requirements is obtained by assessing the implementation of the safeguards and countermeasures selected to satisfy the requirements. Assessors can build on previously developed materials that started with the specification of the information security 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 available information about the system together, 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 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.

The assessment procedures in this publication are based on and sourced to the assessment procedures in SP 800-53A [5]. For additional information and guidance on preparing for security assessments, developing assessment plans, conducting assessments, and analyzing assessment report results, consult SP 800-53A [5].

3. The Procedures

This section provides assessment procedures for the security requirements defined in NIST SP 800-171 [3]. 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

03.01.01 Account Management

ASSESSMENT OBJECTIVE

Determine if:

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

A.03.01.01.ODP[02]: ***the time period within which to notify account managers and designated personnel or roles when accounts are no longer required is defined*****.**

A.03.01.01.ODP[03]: ***the time period within which to notify account managers and designated personnel or roles when users are terminated or transferred is defined*****.**

A.03.01.01.ODP[04]: ***the time period within which to notify account managers and designated personnel or roles when system usage or the need-to-know changes for an individual is defined*****.**

A.03.01.01.ODP[05]: ***the time period of expected inactivity requiring users to log out of the system is defined*****.**

A.03.01.01.ODP[06]: ***circumstances requiring users to log out of the system are 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 memberships are specified.

A.03.01.01.c.03: access authorizations (i.e., privileges) for each account 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: account managers and designated personnel or roles are notified within ***<A.03.01.01.ODP[02]: time period>*** when accounts are no longer required.

A.03.01.01.g.02: account managers and designated personnel or roles are notified within ***<A.03.01.01.ODP[03]: time period>*** when users are terminated or transferred.

A.03.01.01.g.03: account managers and designated personnel or roles are notified within ***<A.03.01.01.ODP[04]: time period>*** when system usage or the need-to-know changes for an individual.

A.03.01.01.h: users are required to log out of the system after ***<A.03.01.01.ODP[05]: time period>*** of expected inactivity or when the following circumstances occur: ***<A.03.01.01.ODP[06]: circumstances>***.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: access control policy and procedures; personnel termination or transfer policies and procedures; procedures for account management; list of active system accounts and the name of the individual associated with each account;

system design documentation; list of conditions for group and role membership; system configuration settings; notifications of recent transfers, separations, or terminations of employees; 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(05), AC-02(13)

03.01.02 Access Enforcement

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.02[01]: approved authorizations for logical access to CUI are enforced in accordance with applicable access control policies.

A.03.01.02[02]: approved authorizations for logical access to system resources are enforced in accordance with applicable access control policies.

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

03.01.03 Information Flow Enforcement

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.03[01]: approved authorizations are enforced for controlling the flow of CUI within the system.

A.03.01.03[02]: approved authorizations are enforced for controlling the flow of CUI 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

03.01.04 Separation of Duties

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]

REFERENCES

Source Assessment Procedure: AC-05

03.01.05 Least Privilege

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.ODP[03]: ***the frequency at which to review the privileges assigned to roles or classes of users 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[02]: security-relevant information>*** is authorized.

A.03.01.05.c: the privileges assigned to roles or classes of users are reviewed ***<A.03.01.05.ODP[03]: frequency>*** 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 (implemented 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 of users; records of privilege removals or reassignments for roles or classes of users; system security plan; system design documentation; 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)

03.01.06 Least Privilege – Privileged Accounts

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 non-security functions or non-security 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)

03.01.07 Least Privilege – Privileged Functions

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)

03.01.08 Unsuccessful Logon Attempts

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.ODP[03]: ***one or more of the following PARAMETER VALUES are selected: {the account or node is locked automatically for <A.03.01.08.ODP[04]: time period>; the account or node is locked automatically until released by an administrator; the next logon prompt is delayed automatically; the system administrator is notified automatically; other action is taken automatically}.***

A.03.01.08.ODP[04]: ***the time period for an account or node to be locked is defined (if selected)*****.**

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

A.03.01.08.b: ***<A.03.01.08.ODP[03]: SELECTED PARAMETER VALUES>*** when the maximum number of unsuccessful attempts is exceeded.

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

03.01.09 System Use Notification

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

03.01.10 Device Lock

ASSESSMENT OBJECTIVE

Determine if:

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

A.03.01.10.ODP[02]: ***the 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 VALUES>***.

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)

03.01.11 Session Termination

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 terminated automatically 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

03.01.12 Remote Access

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[01]: remote access to the system is routed through authorized access control points.

A.03.01.12.c[02]: 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)

03.01.13 Withdrawn

Addressed by 03.13.08.

03.01.14 Withdrawn

Incorporated into 03.01.12.

03.01.15 Withdrawn

Incorporated into 03.01.12.

03.01.16 Wireless Access

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.

A.03.01.16.d[01]: wireless access to the system is protected using authentication.

A.03.01.16.d[02]: wireless access to the system is protected using encryption.

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(01), AC-18(03)

03.01.17 Withdrawn

Incorporated into 03.01.16.

03.01.18 Access Control for Mobile Devices

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)

03.01.19 Withdrawn

Incorporated into 03.01.18.

03.01.20 Use of External Systems

ASSESSMENT OBJECTIVE

Determine if:

A.03.01.20.ODP[01]: ***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: 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[01]: security requirements>***.

A.03.01.20.c.01: authorized individuals are permitted to use external systems to access the organizational system or to process, store, or transmit CUI only after verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied.

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

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 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)

03.01.21 Withdrawn

Incorporated into 03.01.20.

03.01.22 Publicly Accessible Content

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 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 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

03.02.01 Literacy Training and Awareness

ASSESSMENT OBJECTIVE

Determine if:

A.03.02.01.ODP[01]: ***the frequency at which to provide security literacy training to system users after initial training is defined.***

A.03.02.01.ODP[02]: ***events that require security literacy training for system users are defined.***

A.03.02.01.ODP[03]: ***the frequency at which to update security literacy training content is defined.***

A.03.02.01.ODP[04]: ***events that require security literacy training content updates 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 ***<A.03.02.01.ODP[01]: frequency>*** 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[02]: events>***.

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

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

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

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

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

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

A.03.02.01.b[01]: security literacy training content is updated ***<A.03.02.01.ODP[03]: frequency>***.

A.03.02.01.b[02]: security literacy training content is updated following ***<A.03.02.01.ODP[04]: 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)

03.02.02 Role-Based Training

ASSESSMENT OBJECTIVE

Determine if:

A.03.02.02.ODP[01]: *the frequency at which to provide role-based security training to assigned personnel after initial training is defined*.

A.03.02.02.ODP[02]: *events that require role-based security training are defined*.

A.03.02.02.ODP[03]: *the frequency at which to update role-based security training content is defined*.

A.03.02.02.ODP[04]: *events that require role-based security training content updates 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 ***<A.03.02.02.ODP[01]: frequency>*** after initial training.

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[02]: events>***.

A.03.02.02.b[01]: role-based security training content is updated ***<A.03.02.02.ODP[03]: frequency>***.

A.03.02.02.b[02]: role-based security training content is updated following ***<A.03.02.02.ODP[04]: 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

03.02.03 Withdrawn

Incorporated into 03.02.01.

3.3. Audit and Accountability

03.03.01 Event Logging

ASSESSMENT OBJECTIVE

Determine if:

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

A.03.03.01.ODP[02]: ***the frequency of event types selected for logging are reviewed and updated.***

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 ***<A.03.03.01.ODP[02]: frequency>***.

A.03.03.01.b[02]: the event types selected for logging are updated ***<A.03.03.01.ODP[02]: frequency>***.

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

03.03.02 Audit Record Content

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)

03.03.03 Audit Record Generation

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.03.a: audit records for the selected event types and audit record content specified in 03.03.01 and 03.03.02 are generated.

A.03.03.03.b: audit records are retained for a time period consistent with the 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; system 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

03.03.04 Response to Audit Logging Process Failures

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.04.ODP[01]: *the 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: ***<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

03.03.05 Audit Record Review, Analysis, and Reporting

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.05.ODP[01]: ***the frequency at which system audit records are reviewed and analyzed is defined*.**

A.03.03.05.a: system audit records are reviewed and analyzed ***<A.03.03.05.ODP[01]: frequency>*** for indications and the potential impact of inappropriate or unusual activity.

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

A.03.03.05.c[01]: audit records across different repositories are analyzed to gain organization-wide situational awareness.

A.03.03.05.c[02]: audit records across different repositories are correlated to gain organization-wide situational awareness.

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

[SELECT FROM: personnel with audit record 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)

03.03.06 Audit Record Reduction and Report Generation

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.06.a[01]: an audit record reduction and report generation capability that supports audit record review is implemented.

A.03.03.06.a[02]: an audit record reduction and report generation capability that supports audit record analysis is implemented.

A.03.03.06.a[03]: an audit record reduction and report generation capability that supports audit record reporting requirements is implemented.

A.03.03.06.a[04]: an audit record reduction and report generation capability that supports after-the-fact investigations of incidents is implemented.

A.03.03.06.b[01]: the original content of audit records is preserved.

A.03.03.06.b[02]: the original time ordering of audit records is preserved.

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

[SELECT FROM: mechanisms for supporting audit record reduction and report generation capability]

REFERENCES

Source Assessment Procedure: AU-07

03.03.07 Time Stamps

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.07.ODP[01]: *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 are recorded for audit records that meet ***<A.03.03.07.ODP[01]: granularity of time measurement>***.

A.03.03.07.b[02]: time stamps are recorded for audit records that 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.

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

03.03.08 Protection of Audit Information

ASSESSMENT OBJECTIVE

Determine if:

A.03.03.08.a[01]: audit information is protected from unauthorized access, modification, and deletion.

A.03.03.08.a[02]: audit logging tools are protected from unauthorized access, modification, and deletion.

A.03.03.08.b: access to 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)

03.03.09 Withdrawn

Incorporated into 03.03.08.

3.4. Configuration Management

03.04.01 Baseline Configuration

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.01.ODP[01]: *the frequency of baseline configuration review and update is defined*.

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 ***<A.03.04.01.ODP[01]: frequency>***.

A.03.04.01.b[02]: the baseline configuration of the system is updated ***<A.03.04.01.ODP[01]: frequency>***.

A.03.04.01.b[03]: the baseline configuration of the system is reviewed when system components are installed or modified.

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

03.04.02 Configuration Settings

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, or control system configuration settings; mechanisms that identify or document deviations from established configuration settings]

REFERENCES

Source Assessment Procedure: CM-06

03.04.03 Configuration Change Control

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 with explicit consideration for security impacts.

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

03.04.04 Impact Analyses

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.04.a: changes to the system are analyzed to determine potential security impacts prior to change implementation.

A.03.04.04.b: the security requirements for the system continue to be satisfied after the system changes have been implemented.

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, CM-04(02)

03.04.05 Access Restrictions for Change

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

03.04.06 Least Functionality

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]: ***the frequency at which to review the system to identify unnecessary or nonsecure functions, ports, protocols, connections, or services is 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 ***<A.03.04.06.ODP[06]: frequency>*** to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.

A.03.04.06.d: unnecessary or nonsecure functions, ports, protocols, connections, and services are disabled or removed.

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)

03.04.07 Withdrawn

Incorporated into 03.04.06 and 03.04.08.

03.04.08 Authorized Software – Allow by Exception

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.08.ODP[01]: *the frequency at which to review and update the list of authorized software programs is defined*.

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 authorized software programs on the system is implemented.

A.03.04.08.c: the list of authorized software programs is reviewed and updated ***<A.03.04.08.ODP[01]: frequency>***.

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; records associated with the review and update of the list of authorized software programs; common secure configuration checklists; 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 or implementing authorized software policy]

REFERENCES

Source Assessment Procedure: CM-07(05)

03.04.09 Withdrawn

Addressed by 03.01.05, 03.01.06, 03.01.07, 03.04.08, and 03.12.03.

03.04.10 System Component Inventory

ASSESSMENT OBJECTIVE

Determine if:

A.03.04.10.ODP[01]: *the frequency at which to review and update the system component inventory is defined*.

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 ***<A.03.04.10.ODP[01]: frequency>***.

A.03.04.10.b[02]: the system component inventory is updated ***<A.03.04.10.ODP[01]: frequency>***.

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 or implementing the system component inventory; processes for updating the system component inventory; mechanisms for supporting or implementing the system component inventory updates]

REFERENCES

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

03.04.11 Information Location

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]: changes to the system or system component location where CUI is processed are documented.

A.03.04.11.b[02]: changes to the system or system component location 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, 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

03.04.12 System and Component Configuration for High-Risk Areas

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]: ***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]: security 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

03.05.01 User Identification, Authentication, and Re-Authentication

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.

A.03.05.01.a[02]: system users are authenticated.

A.03.05.01.a[03]: processes acting on behalf of users are associated with uniquely identified and authenticated system 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 or implementing identification and authentication capabilities]

REFERENCES

Source Assessment Procedures: IA-02, IA-11

03.05.02 Device Identification and Authentication

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.02.ODP[01]: *devices or types of devices to be uniquely identified and authenticated before establishing a connection are defined*.

A.03.05.02[01]: *<A.03.05.02.ODP[01]: devices or types of devices>* are uniquely identified before establishing a system connection.

A.03.05.02[02]: *<A.03.05.02.ODP[01]: devices or types of devices>* are 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 or implementing device identification and authentication capabilities]

REFERENCES

Source Assessment Procedure: IA-03

03.05.03 Multi-Factor Authentication

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.03[01]: multi-factor authentication for access to privileged accounts is implemented.

A.03.05.03[02]: multi-factor authentication for access to non-privileged 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 or implementing a multi-factor authentication capability]

REFERENCES

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

03.05.04 Replay-Resistant Authentication

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.04[01]: replay-resistant authentication mechanisms for access to privileged accounts are implemented.

A.03.05.04[02]: replay-resistant authentication mechanisms for access to non-privileged 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 or implementing identification and authentication capabilities; mechanisms for supporting or implementing replay-resistance]

REFERENCES

Source Assessment Procedure: IA-02(08)

03.05.05 Identifier Management

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.05.ODP[01]: *the time period for preventing the reuse of identifiers is defined*.

A.03.05.05.ODP[02]: *characteristics used to identify individual status are defined*.

A.03.05.05.a: authorization is received from organizational 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[01]: time period>*** is prevented.

A.03.05.05.d: individual identifiers are managed by uniquely identifying each individual as ***<A.03.05.05.ODP[02]: 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 or implementing identifier management]

REFERENCES

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

03.05.06 Withdrawn

Consistency with SP 800-53 [8].

03.05.07 Password Management

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.07.ODP[01]: ***the frequency at which to update the list of commonly used, expected, or compromised passwords is defined*****.**

A.03.05.07.ODP[02]: ***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 ***<A.03.05.07.ODP[01]: frequency>***.

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 for passwords are enforced: ***<A.03.05.07.ODP[02]: 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 or implementing a password-based authenticator management capability]

REFERENCES

Source Assessment Procedure: IA-05(01)

03.05.08 Withdrawn

Consistency with SP 800-53 [8].

03.05.09 Withdrawn

Consistency with SP 800-53 [8].

03.05.10 Withdrawn

Incorporated into 03.05.07.

03.05.11 Authentication Feedback

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 or implementing the obscuring of feedback of authentication information during authentication]

REFERENCES

Source Assessment Procedure: IA-06

03.05.12 Authenticator Management

ASSESSMENT OBJECTIVE

Determine if:

A.03.05.12.ODP[01]: *the frequency for changing or refreshing authenticators is defined*.

A.03.05.12.ODP[02]: *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.

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

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

A.03.05.12.c[04]: administrative procedures for initial authenticator distribution are implemented.

A.03.05.12.c[05]: administrative procedures for lost, compromised, or damaged authenticators are implemented.

A.03.05.12.c[06]: administrative procedures for revoking authenticators are implemented.

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

A.03.05.12.e: authenticators are changed or refreshed ***<A.03.05.12.ODP[01]: frequency>*** or when the following events occur: ***<A.03.05.12.ODP[02]: events>***.

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

A.03.05.12.f[02]: 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 or implementing the authenticator management capability]

REFERENCES

Source Assessment Procedure: IA-05

3.6. Incident Response

03.06.01 Incident Handling

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

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

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

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

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 Procedure: IR-04

03.06.02 Incident Monitoring, Reporting, and Response Assistance

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 system users on handling and reporting 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 or implementing the tracking and documenting of system security incidents; mechanisms for supporting or implementing incident reporting; mechanisms for supporting or implementing incident response assistance; processes for incident response assistance]

REFERENCES

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

03.06.03 Incident Response Testing

ASSESSMENT OBJECTIVE

Determine if:

A.03.06.03.ODP[01]: ***the frequency at which to test the effectiveness of the incident response capability for the system is defined.***

A.03.06.03: the effectiveness of the incident response capability is tested ***<A.03.06.03.ODP[01]: frequency>***.

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

03.06.04 Incident Response Training

ASSESSMENT OBJECTIVE

Determine if:

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

A.03.06.04.ODP[02]: ***the frequency at which to provide incident response training to users after initial training is defined.***

A.03.06.04.ODP[03]: ***the frequency at which to review and update incident response training content is defined.***

A.03.06.04.ODP[04]: ***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 ***<A.03.06.04.ODP[02]: frequency>*** thereafter.

A.03.06.04.b[01]: incident response training content is reviewed ***<A.03.06.04.ODP[03]: frequency>***.

A.03.06.04.b[02]: incident response training content is updated ***<A.03.06.04.ODP[03]: frequency>***.

A.03.06.04.b[03]: incident response training content is reviewed following ***<A.03.06.04.ODP[04]: events>***.

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

03.06.05 Incident Response Plan

ASSESSMENT OBJECTIVE

Determine if:

A.03.06.05.a.01: an incident response plan is developed that provides the organization with a roadmap for implementing its incident response capability.

A.03.06.05.a.02: an incident response plan is developed that describes the structure and organization of the incident response capability.

A.03.06.05.a.03: an incident response plan is developed that provides a high-level approach for how the incident response capability fits into the overall organization.

A.03.06.05.a.04: an incident response plan is developed that defines reportable incidents.

A.03.06.05.a.05: an incident response plan is developed that addresses the sharing of incident information.

A.03.06.05.a.06: an incident response plan is developed that designates responsibilities to organizational entities, personnel, or roles.

A.03.06.05.b[01]: copies of the incident response plan are distributed to designated incident response personnel (identified by name or by role).

A.03.06.05.b[02]: copies of the incident response plan are distributed to organizational elements.

A.03.06.05.c: the incident response plan is updated to address system and organizational changes or problems encountered during plan implementation, execution, or testing.

A.03.06.05.d: the incident response plan is protected from unauthorized disclosure.

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

[SELECT FROM: incident response plan and related processes]

REFERENCES

Source Assessment Procedure: IR-08

3.7. Maintenance

03.07.01 Withdrawn

Recategorized as NCO.

03.07.02 Withdrawn

Incorporated into 03.07.04 and 03.07.06.

03.07.03 Withdrawn

Incorporated into 03.08.03.

03.07.04 Maintenance Tools

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: media with diagnostic and test programs are checked for malicious code before the media are used in the system.

A.03.07.04.c: 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 or implementing the approval, control, 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 or implementing the inspection of maintenance tools; mechanisms for supporting or implementing the inspection of media used for maintenance]

REFERENCES

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

03.07.05 Nonlocal Maintenance

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[01]: multi-factor authentication is implemented in the establishment of nonlocal maintenance and diagnostic sessions.

A.03.07.05.b[02]: replay resistance is 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, 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

03.07.06 Maintenance Personnel

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: non-escorted personnel who perform maintenance on the system possess the required access authorizations.

A.03.07.06.d[01]: organizational personnel with required access authorizations are designated to supervise the maintenance activities of personnel who do not possess the required access authorizations.

A.03.07.06.d[02]: organizational personnel with required 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 or implementing the authorization of maintenance personnel]

REFERENCES

Source Assessment Procedure: MA-05

3.8. Media Protection

03.08.01 Media Storage

ASSESSMENT OBJECTIVE

Determine if:

A.03.08.01[01]: system media that contain CUI are physically controlled.

A.03.08.01[02]: system media that contain CUI are securely stored.

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 or implementing secure media storage/media protection]

REFERENCES

Source Assessment Procedure: MP-04

03.08.02 Media Access

ASSESSMENT OBJECTIVE

Determine if:

A.03.08.02: access to CUI on system media is restricted to authorized personnel or roles.

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 for supporting or implementing media access restrictions]

REFERENCES

Source Assessment Procedure: MP-02

03.08.03 Media Sanitization

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 or implementing media sanitization]

REFERENCES

Source Assessment Procedure: MP-06

03.08.04 Media Marking

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 applicable CUI 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 or implementing media marking]

REFERENCES

Source Assessment Procedure: MP-03

03.08.05 Media Transport

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: accountability for system media that contain CUI is maintained during transport outside of controlled areas.

A.03.08.05.c: activities associated with the transport of system media that contain CUI are documented.

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 or implementing media storage/media protection; mechanisms for supporting or implementing confidentiality protections for information at rest]

REFERENCES

Source Assessment Procedures: MP-05, SC-28

03.08.06 Withdrawn

Addressed by 03.13.08.

03.08.07 Media Use

ASSESSMENT OBJECTIVE

Determine if:

A.03.08.07.ODP[01]: *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 audit records; system design documentation; 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

03.08.08 Withdrawn

Incorporated into 03.08.07.

03.08.09 System Backup – Cryptographic Protection

ASSESSMENT OBJECTIVE

Determine if:

A.03.08.09.a: the confidentiality of backup information is protected.

A.03.08.09.b: 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 or implementing the cryptographic protection of backup information]

REFERENCES

Source Assessment Procedures: CP-09, CP-09(08)

3.9. Personnel Security

03.09.01 Personnel Screening

ASSESSMENT OBJECTIVE

Determine if:

A.03.09.01.ODP[01]: *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 and rescreening; 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 and rescreening]

REFERENCES

Source Assessment Procedure: PS-03

03.09.02 Personnel Termination and Transfer

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

A.03.09.02.a.02[01]: upon termination of individual employment, authenticators associated with the individual are terminated or revoked.

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

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

A.03.09.02.b.01[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 is reviewed.

A.03.09.02.b.01[02]: 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 is confirmed.

A.03.09.02.b.02: 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 or implementing personnel transfer notifications; mechanisms for supporting 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

03.10.01 Physical Access Authorizations

ASSESSMENT OBJECTIVE

Determine if:

A.03.10.01.ODP[01]: ***the frequency at which to review the access list detailing authorized facility access by individuals is defined.***

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

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

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

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

A.03.10.01.c: the facility access list is reviewed ***<A.03.10.01.ODP[01]: frequency>***.

A.03.10.01.d: individuals from the facility 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 or implementing physical access authorizations]

REFERENCES

Source Assessment Procedure: PE-02

03.10.02 Monitoring Physical Access

ASSESSMENT OBJECTIVE

Determine if:

A.03.10.02.ODP[01]: ***the frequency at which to review physical access logs is defined.***

A.03.10.02.ODP[02]: ***events or potential indications of events requiring physical access logs to be reviewed are defined.***

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

A.03.10.02.a[02]: physical security incidents are responded to.

A.03.10.02.b[01]: physical access logs are reviewed ***<A.03.10.02.ODP[01]: frequency>***.

A.03.10.02.b[02]: physical access logs are reviewed upon occurrence of ***<A.03.10.02.ODP[02]: events or potential indications of events>***.

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 for supporting or implementing physical access monitoring; mechanisms for supporting or implementing the review of physical access logs]

REFERENCES

Source Assessment Procedure: PE-06

03.10.03 Withdrawn

Incorporated into 03.10.07.

03.10.04 Withdrawn

Incorporated into 03.10.07.

03.10.05 Withdrawn

Incorporated into 03.10.07.

03.10.06 Alternate Work Site

ASSESSMENT OBJECTIVE

Determine if:

A.03.10.06.ODP[01]: *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 determined.

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

03.10.07 Physical Access Control

ASSESSMENT OBJECTIVE

Determine if:

A.03.10.07.a.01: physical access authorizations are enforced at entry and exit points to the facility where the system resides by verifying individual physical access authorizations before granting access.

A.03.10.07.a.02: physical access authorizations are enforced at entry and exit points to the facility 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.

A.03.10.07.d: keys, combinations, and other physical access devices are secured.

A.03.10.07.e: 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 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 or implementing physical access control; physical access control devices]

REFERENCES

Source Assessment Procedure: PE-03, PE-05

03.10.08 Access Control for Transmission

ASSESSMENT OBJECTIVE

Determine if:

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

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; list of output devices and associated outputs that require physical access controls; actual displays from system components; 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 or implementing access control for distribution and transmission lines; processes for access control to output devices; mechanisms for supporting or implementing access control for output devices]

REFERENCES

Source Assessment Procedure: PE-04

3.11. Risk Assessment

03.11.01 Risk Assessment

ASSESSMENT OBJECTIVE

Determine if:

A.03.11.01.ODP[01]: ***the frequency at which to update the risk assessment is defined.***

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 ***<A.03.11.01.ODP[01]: frequency>***.

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 or conducting, documenting, reviewing, disseminating, and updating risk assessments; mechanisms for supporting or conducting, documenting, reviewing, disseminating, and updating supply chain risk assessments]

REFERENCES

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

03.11.02 Vulnerability Monitoring and Scanning

ASSESSMENT OBJECTIVE

Determine if:

A.03.11.02.ODP[01]: ***the frequency at which the system is monitored for vulnerabilities is defined.***

A.03.11.02.ODP[02]: ***the frequency at which the system is scanned for vulnerabilities is defined.***

A.03.11.02.ODP[03]: ***response times to remediate system vulnerabilities are defined*.**

A.03.11.02.ODP[04]: ***the frequency at which to update system vulnerabilities to be scanned is defined.***

A.03.11.02.a[01]: the system is monitored for vulnerabilities ***<A.03.11.02.ODP[01]: frequency>***.

A.03.11.02.a[02]: the system is scanned for vulnerabilities ***<A.03.11.02.ODP[02]: frequency>***.

A.03.11.02.a[03]: the system is monitored for vulnerabilities when new vulnerabilities that affect the system are identified.

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 within ***<A.03.11.02.ODP[03]: response times>***.

A.03.11.02.c[01]: system vulnerabilities to be scanned are updated ***<A.03.11.02.ODP[04]: frequency>***.

A.03.11.02.c[02]: system vulnerabilities to be scanned are updated when new vulnerabilities are identified and 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 monitoring, scanning, analysis, and remediation; mechanisms for supporting or implementing vulnerability monitoring, scanning, analysis, and remediation]

REFERENCES

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

03.11.03 Withdrawn

Incorporated into 03.11.02.

03.11.04 Risk Response

ASSESSMENT OBJECTIVE

Determine if:

A.03.11.04[01]: findings from security assessments are responded to.

A.03.11.04[02]: findings from security monitoring are responded to.

A.03.11.04[03]: findings from security audits are responded to.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: risk assessment policy; assessment reports; system audit records; event logs; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with assessment and auditing responsibilities; system administrators; personnel with security responsibilities]

Test

[SELECT FROM: processes for assessments and audits; mechanisms and tools supporting or implementing assessments and auditing]

REFERENCES

Source Assessment Procedure: RA-07

3.12. Security Assessment and Monitoring

03.12.01 Security Assessment

ASSESSMENT OBJECTIVE

Determine if:

A.03.12.01.ODP[01]: ***the frequency at which to assess the security requirements for the system and its environment of operation is defined.***

A.03.12.01: the security requirements for the system and its environment of operation are assessed ***<A.03.12.01.ODP[01]: frequency>*** 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 for supporting security assessments, processes for security assessment plan development, or security assessment reporting]

REFERENCES

Source Assessment Procedure: CA-02

03.12.02 Plan of Action and Milestones

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 based on the findings from security assessments.

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

A.03.12.02.b.03: the existing plan of action and milestones is updated 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

03.12.03 Continuous Monitoring

ASSESSMENT OBJECTIVE

Determine if:

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

A.03.12.03[02]: a system-level continuous monitoring strategy is implemented.

A.03.12.03[03]: ongoing monitoring is included in the continuous monitoring strategy.

A.03.12.03[04]: security assessments are included in 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 for supporting response actions for assessment and monitoring results; mechanisms for supporting security status reporting]

REFERENCES

Source Assessment Procedure: CA-07

03.12.04 Withdrawn

Incorporated into 03.15.02.

03.12.05 Information Exchange

ASSESSMENT OBJECTIVE

Determine if:

A.03.12.05.ODP[01]: ***one or more of the following PARAMETER VALUES are selected: {interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; non-disclosure agreements***; ***other types of agreements}*****.**

A.03.12.05.ODP[02]: ***the frequency at which to review and update agreements is defined.***

A.03.12.05.a[01]: the exchange of CUI between the system and other systems is approved using ***<A.03.12.05.ODP[01]: SELECTED PARAMETER VALUES>***.

A.03.12.05.a[02]: the exchange of CUI between the system and other systems is managed using ***<A.03.12.05.ODP[01]: SELECTED PARAMETER VALUES>***.

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

A.03.12.05.b[02]: security requirements for each system 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 ***<A.03.12.05.ODP[02]: frequency>***.

A.03.12.05.c[02]: exchange agreements are updated ***<A.03.12.05.ODP[02]: frequency>***.

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

03.13.01 Boundary Protection

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

03.13.02 Withdrawn

Recategorized as NCO.

03.13.03 Withdrawn

Addressed by 03.01.01, 03.01.02, 03.01.03, 03.01.04, 03.01.05, 03.01.06, and 03.01.07.

03.13.04 Information in Shared System Resources

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

03.13.05 Withdrawn

Incorporated into 03.13.01.

03.13.06 Network Communications – Deny by Default – Allow by Exception

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)

03.13.07 Withdrawn

Addressed by 03.01.12, 03.04.02 and 03.04.06.

03.13.08 Transmission and Storage Confidentiality

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 or implementing transmission confidentiality; cryptographic mechanisms for supporting or implementing transmission confidentiality; mechanisms for supporting or implementing confidentiality protection for information in storage; cryptographic mechanisms for implementing confidentiality protections for information in storage]

REFERENCES

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

03.13.09 Network Disconnect

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.09.ODP[01]: *the time period of inactivity after which the system terminates a network connection associated with a communications session is defined.*

A.03.13.09: the network connection associated with a communications session is terminated at the end of the session or after ***<A.03.13.09.ODP[01]: time period>*** 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 or implementing a network disconnect capability]

REFERENCES

Source Assessment Procedure: SC-10

03.13.10 Cryptographic Key Establishment and Management

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.10.ODP[01]: *requirements for key generation, distribution, storage, access, and destruction 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 or management; personnel with information security responsibilities; system administrators]

Test

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

REFERENCES

Source Assessment Procedure: SC-12

03.13.11 Cryptographic Protection

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 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 or implementing cryptographic protection]

REFERENCES

Source Assessment Procedure: SC-13

03.13.12 Collaborative Computing Devices and Applications

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.12.ODP[01]: ***exceptions where remote activation is to be allowed are defined.***

A.03.13.12.a: the remote activation of collaborative computing devices and applications is prohibited with the following exceptions: ***<A.03.13.12.ODP[01]: exceptions>***.

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 for supporting 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

03.13.13 Mobile Code

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 or implementing the management of mobile code; mechanisms for supporting or implementing mobile code monitoring]

REFERENCES

Source Assessment Procedure: SC-18

03.13.14 Withdrawn

Technology-specific.

03.13.15 Session Authenticity

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 or implementing session authenticity]

REFERENCES

Source Assessment Procedure: SC-23

03.13.16 Withdrawn

Incorporated into 03.13.08.

3.14. System and Information Integrity

03.14.01 Flaw Remediation

ASSESSMENT OBJECTIVE

Determine if:

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

A.03.14.01.ODP[02]: ***the 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, 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 or implementing the reporting and correction of system flaws; mechanisms for supporting or implementing the testing software and firmware updates]

REFERENCES

Source Assessment Procedure: SI-02

03.14.02 Malicious Code Protection

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 system entry and exit points to detect malicious code.

A.03.14.02.a[02]: malicious code protection mechanisms are implemented at system entry and exit points 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]: 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 system 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, 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 or implementing, employing, updating, and configuring malicious code protection mechanisms; mechanisms for supporting or implementing malicious code scanning and the execution of subsequent actions]

REFERENCES

Source Assessment Procedure: SI-03

03.14.03 Security Alerts, Advisories, and Directives

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.

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, 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 or implementing security directives; mechanisms for supporting or implementing the definition, receipt, generation, and dissemination of security alerts, advisories, and directives]

REFERENCES

Source Assessment Procedure: SI-05

03.14.04 Withdrawn

Incorporated into 03.14.02.

03.14.05 Withdrawn

Addressed by 03.14.02.

03.14.06 System Monitoring

ASSESSMENT OBJECTIVE

Determine if:

A.03.14.06.a.01[01]: the system is monitored to detect attacks.

A.03.14.06.a.01[02]: the system is monitored to detect 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, 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 for supporting or implementing system monitoring capabilities; mechanisms for supporting or implementing intrusion detection and system monitoring capabilities; mechanisms for supporting or implementing the monitoring of inbound and outbound communications traffic]

REFERENCES

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

03.14.07 Withdrawn

Incorporated into 03.14.06.

03.14.08 Information Management and Retention

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 or implementing information management, retention, and disposition]

REFERENCES

Source Assessment Procedure: SI-12

3.15. Planning

03.15.01 Policy and Procedures

ASSESSMENT OBJECTIVE

Determine if:

A.03.15.01.ODP[01]: ***the frequency at which the policies and procedures for satisfying security requirements are reviewed and updated is defined.***

A.03.15.01.a[01]: policies needed to satisfy the security requirements for the protection of CUI are developed and documented.

A.03.15.01.a[02]: policies needed to satisfy the security requirements for the protection of CUI are disseminated to organizational personnel or roles.

A.03.15.01.a[03]: procedures needed to satisfy the security requirements for the protection of CUI are developed and documented.

A.03.15.01.a[04]: procedures needed to satisfy the security requirements for the protection of CUI are disseminated to organizational personnel or roles.

A.03.15.01.b[01]: policies and procedures are reviewed ***<A.03.15.01.ODP[01]: frequency>***.

A.03.15.01.b[02]: policies and procedures are updated ***<A.03.15.01.ODP[01]: frequency>***.

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

03.15.02 System Security Plan

ASSESSMENT OBJECTIVE

Determine if:

A.03.15.02.ODP[01]: ***the frequency at which the system security plan is reviewed and updated is defined.***

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 identifies the information types processed, stored, and transmitted by the system is developed.

A.03.15.02.a.03: a system security plan that describes 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 describes the operational environment for the system and any dependencies on or connections to other systems or system components is developed.

A.03.15.02.a.05: a system security plan that provides an overview of the security requirements for the system is developed.

A.03.15.02.a.06: a system security plan that describes the safeguards in place or planned for meeting the security requirements is developed.

A.03.15.02.a.07: a system security plan that identifies individuals that fulfill system roles and responsibilities is developed.

A.03.15.02.a.08: 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 ***<A.03.15.02.ODP[01]: frequency>***.

A.03.15.02.b[02]: the system security plan is updated ***<A.03.15.02.ODP[01]: frequency>***.

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 system 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

03.15.03 Rules of Behavior

ASSESSMENT OBJECTIVE

Determine if:

A.03.15.03.ODP[01]: ***the frequency at which the rules of behavior are reviewed and updated is defined.***

A.03.15.03.a: rules that describe responsibilities and expected behavior for system usage and protecting CUI are established.

A.03.15.03.b: rules are provided to individuals who require access to the system.

A.03.15.03.c: 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.d[01]: the rules of behavior are reviewed ***<A.03.15.03.ODP[01]: frequency>***.

A.03.15.03.d[02]: the rules of behavior are updated ***<A.03.15.03.ODP[01]: frequency>***.

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 or implementing the establishment, dissemination, review, and update of rules of behavior]

REFERENCES

Source Assessment Procedure: PL-04

3.16. System and Services Acquisition

03.16.01 Systems Security Engineering Principles

ASSESSMENT OBJECTIVE

Determine if:

A.03.16.01.ODP[01]: ***systems security engineering principles to be applied to the development or modification of the system and system components are defined.***

A.03.16.01: ***<A.03.16.01.ODP[01]: systems security engineering principles>*** are applied to the development or modification of the system and system components.

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: system and services acquisition policy; system and services acquisition procedures; procedures addressing security engineering principles used in the development and modification of the system; system design documentation; security requirements and specifications for the system; system security plan; other relevant documents or records]

Interview

[SELECT FROM: personnel with acquisition/contracting responsibilities; personnel with information security responsibilities; personnel with system development and modification responsibilities; system developers]

Test

[SELECT FROM: processes for applying security engineering principles in system development and modification; mechanisms supporting the application of security engineering principles in system development and modification]

REFERENCES

Source Assessment Procedure: SA-08

03.16.02 Unsupported System Components

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 that cannot be replaced are provided.

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 or implementing the replacement of unsupported system components]

REFERENCES

Source Assessment Procedure: SA-22

03.16.03 External System Services

ASSESSMENT OBJECTIVE

Determine if:

A.03.16.03.ODP[01]: ***security requirements to be satisfied 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 service 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

03.17.01 Supply Chain Risk Management Plan

ASSESSMENT OBJECTIVE

Determine if:

A.03.17.01.ODP[01]: ***the frequency at which to review and update the supply chain risk management plan is defined.***

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 operation of the system, system components, or system services.

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

A.03.17.01.a[10]: 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 ***<A.03.17.01.ODP[01]: frequency>***.

A.03.17.01.b[02]: the SCRM plan is updated ***<A.03.17.01.ODP[01]: frequency>***.

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, including research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal; 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 or implementing the SDLC]

REFERENCES

Source Assessment Procedure: SR-02

03.17.02 Acquisition Strategies, Tools, and Methods

ASSESSMENT OBJECTIVE

Determine if:

A.03.17.02[01]: acquisition strategies, contract tools, and procurement methods are developed to identify supply chain risks.

A.03.17.02[02]: acquisition strategies, contract tools, and procurement methods are developed to protect against supply chain risks.

A.03.17.02[03]: acquisition strategies, contract tools, and procurement methods are developed to mitigate supply chain risks.

A.03.17.02[04]: acquisition strategies, contract tools, and procurement methods are implemented to identify supply chain risks.

A.03.17.02[05]: acquisition strategies, contract tools, and procurement methods are implemented to protect against supply chain risks.

A.03.17.02[06]: acquisition strategies, contract tools, and procurement methods are 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 identified supply chain risks; mitigation plans for supply chain risks; 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 implementing tailored acquisition strategies, contract tools, and procurement methods]

REFERENCES

Source Assessment Procedure: SR-05

03.17.03 Supply Chain Requirements and Processes

ASSESSMENT OBJECTIVE

Determine if:

A.03.17.03.ODP[01]: ***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[01]: a process for identifying weaknesses or deficiencies in the supply chain elements and processes is established.

A.03.17.03.a[02]: a process for 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); shipping and handling procedures; configuration management documentation and records; 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 (2024) 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. https://doi.org/10.6028/NIST.SP.800-171r3

[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] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[9] 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

[10] 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

OSCAL
Open Security Controls Assessment Language

SCRM
Supply Chain Risk Management

SDLC
System Development Life Cycle

Appendix B. Glossary

Appendix B provides definitions for the terminology used in SP 800-171A. The definitions are consistent with the definitions contained in the Committee on National Security Systems (CNSS) Glossary [9] 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. [10]

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. [9]

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 or plans to meet the security requirements for a system. In particular, the system security plan describes the system boundary, the environment in which the system operates, how the security requirements are satisfied, and the relationships with or connections to other systems.

Appendix C. Security Requirement Assessment

This appendix provides an overview of the process for assessing the security requirements in SP 800-171 [3]. The four-phase process is based on the methodology in SP 800-53A [5][6] and includes:

- Preparing for assessments
- Developing assessment plans
- Conducting assessments
- Analyzing, documenting, and reporting assessment results

C.1. Preparing for Assessments

Thorough preparation by the organization and assessors is an important aspect of conducting an effective assessment. Preparatory activities address a range of issues relating to the cost, schedule, and conduct of the assessment. From an organizational perspective, preparing for an assessment includes the following activities:

- Ensuring that appropriate policies that cover the assessment are in place and understood by affected organizational elements
- Establishing the objective and scope of the assessment (i.e., the purpose of the assessment and what is being assessed)
- Notifying appropriate organizational officials of the impending assessment and allocating the necessary resources to carry out the assessment
- Establishing appropriate communication channels among organizational officials with an interest in the assessment
- Establishing the time frame for completing the assessment and the key milestone decision points required by the organization
- Identifying and selecting the assessors who will be responsible for conducting the assessment and considering issues of assessor independence
- Providing artifacts to the assessors (e.g., policies, procedures, plans, specifications, designs, records, administrator/operator manuals, information exchange agreements, system documentation, previous assessment results, legal requirements)
- Establishing a mechanism between the organization and the assessors to minimize ambiguities or misunderstandings about the security requirements, implementation issues, and deficiencies identified during the assessment

[6] For additional detail and guidance, see SP 800-53A, Section 3.

Assessors begin preparing for the assessment by:

- Developing a general understanding of the organization's operations and how the scope of the assessment supports those organizational operations
- Understanding the structure of the system (i.e., the system architecture) and the security requirements being assessed
- Meeting with organizational officials to ensure that there is a common understanding of the assessment objectives and the proposed rigor and scope of the assessment
- Obtaining the artifacts needed for the assessment (e.g., policies, procedures, plans, specifications, administrator/operator manuals, system documentation, information exchange agreements, designs, records, previous assessment results[7])
- Establishing organizational points of contact to carry out the assessment

Table 2 provides a summary of the purpose and expected outcomes of the *assessment preparation phase*.

Table 2. Summary of Assessment Preparation Phase

PURPOSE	**Address a range of issues pertaining to the cost, schedule, scope, and conduct of the assessment.**
OUTCOMES	• The objective, scope, and time frame of the assessment are determined. • Key organizational stakeholders are notified, and the necessary resources are allocated. • Assessors are identified and selected. • Artifacts are collected and provided to assessors. • Mechanisms to minimize ambiguities and misunderstandings about the security requirements, implementation issues, and weaknesses/deficiencies identified during the assessment are established. • The organization's operations, structure, objective, scope, and time frame of assessment are understood by assessors.

C.2. Developing Assessment Plans

The assessment plan establishes the objectives for the security requirement assessment and a detailed roadmap of how to conduct the assessment based on the system security plan. The following steps are considered by assessors when developing an assessment plan:

- Determine which security requirements are to be included in the assessment based on the contents of the system security plan and the purpose and scope of the assessment.
- Select the appropriate assessment procedures.

[7] Previous assessment results that may be reused for the current assessment include Inspector General reports, audits, vulnerability scans, physical security inspections, developmental testing and evaluation, vendor flaw remediation activities, and ISO 15408 [6] evaluations.

- Tailor the selected assessment procedures (e.g., select appropriate assessment methods and objects, and assign depth and coverage attribute values).[8]
- Optimize the assessment procedures to reduce the duplication of effort (e.g., sequence and consolidate assessment procedures) and provide a cost-effective assessment solution.
- Finalize the assessment plan, and obtain the necessary approvals to execute the plan.

Table 3 provides a summary of the purpose and expected outcomes of the *assessment plan development phase*.

Table 3. Summary of Assessment Plan Development Phase

PURPOSE	**Establish the objectives for the security requirement assessment and a detailed roadmap of how to conduct the assessment based on the system security plan.**
OUTCOMES	• Security requirements to be included in the assessment are determined. • Assessment procedures are selected and tailored. • Assessment procedures are optimized to reduce the duplication of effort. • The assessment plan is finalized, and organizational approvals are obtained.

C.3. Conducting Assessments

After the assessment plan is approved by the organization, the assessors execute the plan in accordance with the agreed-upon schedule. Assessment objectives are achieved by applying the designated assessment methods to selected assessment objects and compiling or producing the evidence necessary to make the determination associated with each assessment objective. Each determination statement contained within an assessment procedure executed by an assessor produces one of the following findings:

- Satisfied or
- Other than satisfied.

A finding of *satisfied* indicates that the assessment objective for the security requirement (or subset of the requirement) addressed by the determination statement has been met and produced an acceptable result. A finding of *other than satisfied* indicates that the assessment objective for the requirement has not been met and has produced an unacceptable result. 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.

[8] In addition to selecting assessment methods and objects, each assessment method (i.e., examine, interview, and test) is associated with depth and coverage attributes. The attribute values identify the rigor (depth) and scope (coverage) of the assessment procedures executed by the assessor. The depth and coverage attribute values are associated with the assurance requirements specified by the organization. SP 800-53A, Appendix C provides additional guidance on depth and coverage attributes.

Table 4 provides a summary of the purpose and expected outcomes of the *assessment execution phase*.

Table 4. Summary of Assessment Execution Phase

PURPOSE	**Conduct the assessment in accordance with the assessment plan, and document the results in an assessment report.**
OUTCOMES	• Security requirements are assessed in accordance with the assessment plan. • An assessment report that documents whether the security requirements have been satisfied is produced.

C.4. Analyzing, Documenting, and Reporting Assessment Results

The assessment report includes information from assessors (in the form of findings) that is necessary to determine whether the security requirements in SP 800-171 have been satisfied.[9] The report conveys the results of the assessment to designated organizational officials. The report can also provide recommendations for correcting any deficiencies discovered during the assessment. Depending on the organization's objective for the assessment, the assessment results can trigger a variety of risk response actions, including risk acceptance, risk mitigation, risk rejection, risk transfer, or risk sharing. The assessment results can also influence changes to the system security plan and plan of action and milestones.

Table 5 provides a summary of the purpose and expected outcomes of the *assessment analysis, documentation, and reporting phase*.

Table 5. Summary of Assessment Analysis, Documentation, and Reporting Phase

PURPOSE	**Analyze the risks that result from the weaknesses and deficiencies identified during the assessment, and determine an approach to respond to those risks in accordance with organizational priorities.**
OUTCOMES	• Assessment findings are reviewed and analyzed. • Subsequent risk responses are initiated to manage risks. • The system security plan and plan of action and milestones are updated to reflect the results of the assessment and any subsequent risk response actions.

[9] SP 800-53A, Appendix E provides additional guidance on security assessment reports.

Appendix D. Organization-Defined Parameters

This appendix lists the organization-defined parameters (ODPs) that are included in the assessment procedures in Sec. 3. The ODPs are listed sequentially by requirement family, beginning with the first requirement containing an ODP in the Access Control (AC) family and ending with the last requirement containing an ODP in the Supply Chain Risk Management (SR) family.

Table 6. Organization-Defined Parameters

SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.01.01	A.03.01.01.ODP[01]	*the time period for account inactivity before disabling is defined.*
03.01.01	A.03.01.01.ODP[02]	*the time period within which to notify account managers and designated personnel or roles when accounts are no longer required is defined.*
03.01.01	A.03.01.01.ODP[03]	*the time period within which to notify account managers and designated personnel or roles when users are terminated or transferred is defined.*
03.01.01	A.03.01.01.ODP[04]	*the time period within which to notify account managers and designated personnel or roles when system usage or the need-to-know changes for an individual is defined.*
03.01.01	A.03.01.01.ODP[05]	*the time period of expected inactivity requiring users to log out of the system is defined.*
03.01.01	A.03.01.01.ODP[06]	*circumstances requiring users to log out of the system are defined.*
03.01.05	A.03.01.05.ODP[01]	*security functions for authorized access are defined.*
03.01.05	A.03.01.05.ODP[02]	*security-relevant information for authorized access is defined.*
03.01.05	A.03.01.05.ODP[03]	*the frequency at which to review the privileges assigned to roles or classes of users is defined.*
03.01.06	A.03.01.06.ODP[01]	*personnel or roles to which privileged accounts on the system are to be restricted are defined.*
03.01.08	A.03.01.08.ODP[01]	*the number of consecutive invalid logon attempts by a user allowed during a time period is defined.*
03.01.08	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.*
03.01.08	A.03.01.08.ODP[03]	*one or more of the following PARAMETER VALUES are selected: {the account or node is locked automatically for <A.03.01.08.ODP[04]: time period>; the account or node is locked automatically until released by an administrator; the next logon prompt is delayed automatically; the system administrator is notified automatically; other action is taken automatically}.*
03.01.08	A.03.01.08.ODP[04]	*the time period for an account or node to be locked is defined (if selected).*

SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.01.10	A.03.01.10.ODP[01]	*one or more of the following PARAMETER VALUES are selected: {a device lock is initiated after <A.03.01.10.ODP[02]: time period> of inactivity; the user is required to initiate a device lock before leaving the system unattended}.*
03.01.10	A.03.01.10.ODP[02]	*the time period of inactivity after which a device lock is initiated is defined (if selected).*
03.01.11	A.03.01.11.ODP[01]	*conditions or trigger events that require session disconnect are defined.*
03.01.20	A.03.01.20.ODP[01]	*security requirements to be satisfied on external systems prior to allowing the use of or access to those systems by authorized individuals are defined.*
03.02.01	A.03.02.01.ODP[01]	*the frequency at which to provide security literacy training to system users after initial training is defined.*
03.02.01	A.03.02.01.ODP[02]	*events that require security literacy training for system users are defined.*
03.02.01	A.03.02.01.ODP[03]	*the frequency at which to update security literacy training content is defined.*
03.02.01	A.03.02.01.ODP[04]	*events that require security literacy training content updates are defined.*
03.02.02	A.03.02.02.ODP[01]	*the frequency at which to provide role-based security training to assigned personnel after initial training is defined.*
03.02.02	A.03.02.02.ODP[02]	*events that require role-based security training are defined.*
03.02.02	A.03.02.02.ODP[03]	*the frequency at which to update role-based security training content is defined.*
03.02.02	A.03.02.02.ODP[04]	*events that require role-based security training content updates are defined.*
03.03.01	A.03.03.01.ODP[01]	*event types selected for logging within the system are defined.*
03.03.01	A.03.03.01.ODP[02]	*the frequency of event types selected for logging are reviewed and updated.*
03.03.04	A.03.03.04.ODP[01]	*the time period for organizational personnel or roles receiving audit logging process failure alerts is defined.*
03.03.04	A.03.03.04.ODP[02]	*additional actions to be taken in the event of an audit logging process failure are defined.*
03.03.05	A.03.03.05.ODP[01]	*the frequency at which system audit records are reviewed and analyzed is defined.*
03.03.07	A.03.03.07.ODP[01]	*granularity of time measurement for audit record time stamps is defined.*
03.04.01	A.03.04.01.ODP[01]	*the frequency of baseline configuration review and update is defined.*
03.04.02	A.03.04.02.ODP[01]	*configuration settings for the system that reflect the most restrictive mode consistent with operational requirements are defined.*
03.04.06	A.03.04.06.ODP[01]	*functions to be prohibited or restricted are defined.*
03.04.06	A.03.04.06.ODP[02]	*ports to be prohibited or restricted are defined.*

SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.04.06	A.03.04.06.ODP[03]	*protocols to be prohibited or restricted are defined.*
03.04.06	A.03.04.06.ODP[04]	*connections to be prohibited or restricted are defined.*
03.04.06	A.03.04.06.ODP[05]	*services to be prohibited or restricted are defined.*
03.04.06	A.03.04.06.ODP[06]	*the frequency at which to review the system to identify unnecessary or nonsecure functions, ports, protocols, connections, or services is defined.*
03.04.08	A.03.04.08.ODP[01]	*the frequency at which to review and update the list of authorized software programs is defined.*
03.04.10	A.03.04.10.ODP[01]	*the frequency at which to review and update the system component inventory is defined.*
03.04.12	A.03.04.12.ODP[01]	*configurations for systems or system components to be issued to individuals traveling to high-risk locations are defined.*
03.04.12	A.03.04.12.ODP[02]	*security requirements to be applied to the system or system components when individuals return from travel are defined.*
03.05.01	A.03.05.01.ODP[01]	*circumstances or situations that require re-authentication are defined.*
03.05.02	A.03.05.02.ODP[01]	*devices or types of devices to be uniquely identified and authenticated before establishing a connection are defined.*
03.05.05	A.03.05.05.ODP[01]	*the time period for preventing the reuse of identifiers is defined.*
03.05.05	A.03.05.05.ODP[02]	*characteristics used to identify individual status are defined.*
03.05.07	A.03.05.07.ODP[01]	*the frequency at which to update the list of commonly used, expected, or compromised passwords is defined.*
03.05.07	A.03.05.07.ODP[02]	*password composition and complexity rules are defined.*
03.05.12	A.03.05.12.ODP[01]	*the frequency for changing or refreshing authenticators is defined.*
03.05.12	A.03.05.12.ODP[02]	*events that trigger the change or refreshment of authenticators are defined.*
03.06.02	A.03.06.02.ODP[01]	*the time period to report suspected incidents to the organizational incident response capability is defined.*
03.06.02	A.03.06.02.ODP[02]	*authorities to whom incident information is to be reported are defined.*
03.06.03	A.03.06.03.ODP[01]	*the frequency at which to test the effectiveness of the incident response capability for the system is defined.*
03.06.04	A.03.06.04.ODP[01]	*the time period within which incident response training is to be provided to system users is defined.*
03.06.04	A.03.06.04.ODP[02]	*the frequency at which to provide incident response training to users is defined.*
03.06.04	A.03.06.04.ODP[03]	*the frequency at which to review and update incident response training content is defined.*
03.06.04	A.03.06.04.ODP[04]	*events that initiate a review of the incident response training content are defined.*
03.08.07	A.03.08.07.ODP[01]	*types of system media with usage restrictions or that are prohibited from use are defined.*

SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.09.01	A.03.09.01.ODP[01]	*conditions that require the rescreening of individuals are defined.*
03.09.02	A.03.09.02.ODP[01]	*the time period within which to disable system access is defined.*
03.10.01	A.03.10.01.ODP[01]	*the frequency at which to review the access list detailing authorized facility access by individuals is defined.*
03.10.02	A.03.10.02.ODP[01]	*the frequency at which to review physical access logs is defined.*
03.10.02	A.03.10.02.ODP[02]	*events or potential indications of events requiring physical access logs to be reviewed are defined.*
03.10.06	A.03.10.06.ODP[01]	*security requirements to be employed at alternate work sites are defined.*
03.11.01	A.03.11.01.ODP[01]	*the frequency at which to update the risk assessment is defined.*
03.11.02	A.03.11.02.ODP[01]	*the frequency at which the system is monitored and scanned for vulnerabilities is defined.*
03.11.02	A.03.11.02.ODP[02]	*response times to remediate system vulnerabilities are defined.*
03.11.02	A.03.11.02.ODP[03]	*the frequency at which to update system vulnerabilities to be scanned is defined.*
03.12.01	A.03.12.01.ODP[01]	*the frequency at which to assess the security requirements for the system and its environment of operation is defined.*
03.12.05	A.03.12.05.ODP[01]	*one or more of the following PARAMETER VALUES are selected: {interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; non-disclosure agreements; other types of agreements}.*
03.12.05	A.03.12.05.ODP[02]	*the frequency at which to review and update agreements is defined.*
03.13.09	A.03.13.09.ODP[01]	*the time period of inactivity after which the system terminates a network connection associated with a communications session is defined.*
03.13.10	A.03.13.10.ODP[01]	*requirements for key generation, distribution, storage, access, and destruction are defined.*
03.13.11	A.03.13.11.ODP[01]	*the types of cryptography for protecting the confidentiality of CUI are defined.*
03.13.12	A.03.13.12.ODP[01]	*exceptions where remote activation is to be allowed are defined.*
03.14.01	A.03.14.01.ODP[01]	*the time period within which to install security-relevant software updates after the release of the updates is defined.*
03.14.01	A.03.14.01.ODP[02]	*the time period within which to install security-relevant firmware updates after the release of the updates is defined.*
03.14.02	A.03.14.02.ODP[01]	*the frequency at which malicious code protection mechanisms perform scans is defined.*
03.15.01	A.03.15.01.ODP[01]	*the frequency at which the policies and procedures for implementing security requirements are reviewed and updated is defined.*
03.15.02	A.03.15.02.ODP[01]	*the frequency at which the system security plan is reviewed and updated is defined.*

SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.15.03	A.03.15.03.ODP[01]	*the frequency at which the rules of behavior are reviewed and updated is defined.*
03.16.01	A.03.16.01.ODP[01]	*systems security engineering principles to be applied to the development or modification of the system and system components are defined.*
03.16.03	A.03.16.03.ODP[01]	*security requirements to be satisfied by external system service providers are defined.*
03.17.01	A.03.17.01.ODP[01]	*the frequency at which to review and update the supply chain risk management plan is defined.*
03.17.03	A.03.17.03.ODP[01]	*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.*

Appendix E. Change Log

This publication incorporates the following changes from the original edition (June 2018):

- Assessment procedures have been updated to be consistent with SP 800-171r3 (Revision 3) [3].
- Organization-defined parameters (ODPs) have been added to determination statements.
- A references section has been added to each assessment procedure to provide a hyperlink to the source assessment procedure in SP 800-53A [5].

Table 7 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 7. Change Log

Publication ID	Date	Type of Edit	Change	Location