



Communications Security
Establishment Canada

Centre de la sécurité des
télécommunications Canada

CANADIAN CENTRE^{FOR} **CYBER SECURITY**

Assessing security requirements for specified information

Practitioner

Overview

This publication is a Canadian version of the National Institute of Standards and Technology (NIST) [SP 800-171A Rev. 3 Assessing Security Requirements for Controlled Unclassified Information](#). This publication provides a comprehensive set of procedures to assess security requirements. It serves a complementary guideline to [Protecting specified information in non-Government of Canada systems and organizations \(ITSP.10.171\)](#).

Protecting specified information is of paramount importance to the Government of Canada (GC) departments and agencies. It can directly impact the GC's ability to successfully conduct its essential missions and functions. This publication provides GC departments and agencies with recommended security requirements assessment procedures for ensuring the protection of the confidentiality of specified information when it resides in non-GC systems and organizations. These assessment procedures apply to the security requirements specified by GC departments and agencies in contractual vehicles or other agreements established between those departments and agencies and non-GC organizations. The assessment procedures can be used by organizations to generate evidence that the security requirements specified in contracts or agreements have been satisfied.

Acknowledgments

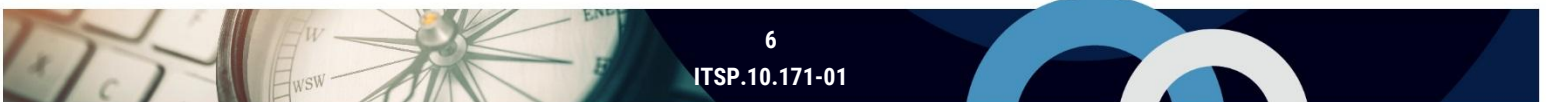
The Cyber Centre wishes to acknowledge and thank Dr. Ron Ross and Victoria Pillitteri from the Computer Security Division at NIST for allowing the Cyber Security Guidance (CSG) team to use their guidance and modify it to the Canadian context.

Table of contents

1	Introduction	10
1.1	Purpose	10
1.2	Audience.....	10
1.3	Publication organization	11
2	Fundamentals	12
2.1	Assessment procedures	12
2.2	Assurance cases	15
3	Procedures	18
3.1	Access control	18
03.01.01	Account management	18
03.01.02	Access enforcement	20
03.01.03	Information flow enforcement	20
03.01.04	Separation of duties.....	21
03.01.05	Least privilege	22
03.01.06	Least privilege – privileged accounts.....	23
03.01.07	Least privilege – privileged functions	23
03.01.08	Unsuccessful logon attempts	24
03.01.09	System use notification.....	25
03.01.10	Device lock.....	25
03.01.11	Session termination	26
03.01.12	Remote access	26
03.01.13	Not allocated	27
03.01.14	Not allocated	27
03.01.15	Not allocated	27
03.01.16	Wireless access.....	28
03.01.17	Not allocated	28
03.01.18	Access control for mobile devices	28
03.01.19	Not allocated	29

03.01.20	Use of external systems	29
03.01.21	Not allocated	30
03.01.22	Publicly accessible content	30
3.2	Awareness and training	31
03.02.01	Literacy training and awareness	31
03.02.02	Role-based training	32
03.02.03	Not allocated	33
3.3	Audit and accountability	33
03.03.01	Event logging	33
03.03.02	Audit record content	34
03.03.03	Audit record generation	35
03.03.04	Response to audit logging process failures	35
03.03.05	Audit record review, analysis, and reporting	36
03.03.06	Audit record reduction and report generation	37
03.03.07	Time stamps	37
03.03.08	Protection of audit information	38
03.03.09	Not allocated	39
3.4	Configuration management	39
03.04.01	Baseline configuration	39
03.04.02	Configuration settings	40
03.04.03	Configuration change control	41
03.04.04	Impact analyses	41
03.04.05	Access restrictions for change	42
03.04.06	Least functionality	43
03.04.07	Not allocated	44
03.04.08	Authorized software – allow by exception	44
03.04.09	Not allocated	45
03.04.10	System component inventory	45
03.04.11	Information location	46
03.04.12	System and component configuration for high-risk areas	46

3.5	Identification and authentication.....	47
03.05.01	User identification, authentication, and reauthentication.....	47
03.05.02	Device identification and authentication	48
03.05.03	Multi-factor authentication	49
03.05.04	Replay-resistant authentication	49
03.05.05	Identifier management	50
03.05.06	Not allocated	51
03.05.07	Password management.....	51
03.05.08	Not allocated	52
03.05.09	Not allocated	52
03.05.10	Not allocated	52
03.05.11	Authentication feedback	52
03.05.12	Authenticator management	52
3.6	Incident response.....	53
03.06.01	Incident handling	54
03.06.02	Incident monitoring, reporting, and response assistance	55
03.06.03	Incident response testing	55
03.06.04	Incident response training	56
03.06.05	Incident response plan	57
3.7	Maintenance	58
03.07.01	Not allocated	58
03.07.02	Not allocated	58
03.07.03	Not allocated	58
03.07.04	Maintenance tools	58
03.07.05	Non-local maintenance	59
03.07.06	Maintenance personnel	60
3.8	Media protection	60
03.08.01	Media storage	61
03.08.02	Media access	61
03.08.03	Media sanitization	62



03.08.04	Media marking.....	62
03.08.05	Media transport.....	63
03.08.06	Not allocated.....	63
03.08.07	Media use.....	64
03.08.08	Not allocated.....	64
03.08.09	System backup – cryptographic protection.....	64
3.9	Personnel security.....	65
03.09.01	Personnel screening.....	65
03.09.02	Personnel termination and transfer.....	66
3.10	Physical protection.....	67
03.10.01	Physical access authorizations.....	67
03.10.02	Monitoring physical access.....	68
03.10.03	Not allocated.....	68
03.10.04	Not allocated.....	68
03.10.05	Not allocated.....	68
03.10.06	Alternate work site.....	69
03.10.07	Physical access control.....	69
03.10.08	Access control for transmission.....	70
3.11	Risk assessment.....	71
03.11.01	Risk assessment.....	71
03.11.02	Vulnerability monitoring and scanning.....	72
03.11.03	Not allocated.....	72
03.11.04	Risk response.....	73
3.12	Security assessment and monitoring.....	73
03.12.01	Security assessment.....	73
03.12.02	Plan of action and milestones.....	74
03.12.03	Continuous monitoring.....	75
03.12.04	Not allocated.....	75
03.12.05	Information exchange.....	75
3.13	System and communications protection.....	76

03.13.01	Boundary protection.....	76
03.13.02	Not allocated.....	77
03.13.03	Not allocated.....	77
03.13.04	Information in shared system resources	77
03.13.05	Not allocated.....	78
03.13.06	Network communications – deny by default – allow by exception.....	78
03.13.07	Not allocated.....	78
03.13.08	Transmission and storage confidentiality	79
03.13.09	Network disconnect.....	79
03.13.10	Cryptographic key establishment and management.....	80
03.13.11	Cryptographic protection.....	81
03.13.12	Collaborative computing devices and applications	81
03.13.13	Mobile code.....	82
03.13.14	Not allocated.....	82
03.13.15	Session authenticity.....	83
03.13.16	Not allocated.....	83
3.14	System and information integrity	83
03.14.01	Flaw remediation	83
03.14.02	Malicious code protection	84
03.14.03	Security alerts, advisories, and directives.....	85
03.14.04	Not allocated.....	86
03.14.05	Not allocated.....	86
03.14.06	System monitoring.....	86
03.14.07	Not allocated.....	87
03.14.08	Information management and retention	87
3.15	Planning	88
03.15.01	Policy and procedures.....	88
03.15.02	System security plan.....	89
03.15.03	Rules of behaviour	90
3.16	System and services acquisition	91

03.16.01	Systems security engineering principles	91
03.16.02	Unsupported system components	91
03.16.03	External system services	92
3.17	Supply chain risk management	93
03.17.01	Supply chain risk management plan	93
03.17.02	Acquisition strategies, tools, and methods	94
03.17.03	Supply chain requirements and processes	95
A.1	Organization-defined parameters	97

List of figures

Figure 1:	Structure and content of an assessment procedure	14
-----------	--	----

List of tables

Table 1:	Organization-defined parameters	97
----------	---------------------------------------	----

List of annexes

A.1	Organization-defined parameters	97
-----	---------------------------------------	----

1 Introduction

This publication is the Canadian version of [NIST SP 800-171A Rev. 3 Assessing Security Requirements for Controlled Unclassified Information](#). There are no substantial technical changes between the Canadian publication and NIST SP 800-171A Rev. 3. The primary modifications arise from differences in laws, policies, directives, standards and guidelines. In other words, the changes reflect the distinct Canadian regulatory and compliance landscape, there are no changes to the underlying technical context.

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

This publication provides a comprehensive set of procedures for assessing the effectiveness of security requirements for protecting the confidentiality of specified information when this information resides in non-GC systems and organizations. The guidelines apply to the security requirements defined in [Protecting specified information in non-Government of Canada systems and organizations \(ITSP.10.171\)](#).

The overarching objective of the assessment is to ensure that the security controls are implemented with sufficient robustness and coverage to address the threat actors that have been identified to be mitigated.

1.2 Audience

This publication is intended for individuals and organizations in the public and private sectors, including those with:

- system development lifecycle responsibilities, for example
 - program managers
 - mission/business owners
 - information custodians
 - system designers and developers
 - system/security engineers
 - system integrators

- acquisition or procurement responsibilities, for example, contracting officers
- system, security, privacy or risk management and oversight responsibilities, for example
 - authorizing officials
 - chief information officers
 - chief information security officers
 - chief privacy officers
 - system owners
 - information security managers
- security or privacy assessment and monitoring responsibilities, for example
 - auditors
 - system evaluators
 - assessors
 - independent verifiers/validators
 - analysts

The above roles and responsibilities can be viewed from 2 perspectives:

- GC perspective: the entity establishing and conveying security assessment requirements in contractual vehicles or other types of agreements
- non-GC perspective: the entity responding to and complying with the security assessment requirements set forth in contracts or agreements

1.3 Publication organization

The remainder of this publication is organized as follows:

- [Section 2: Fundamentals](#) 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: Procedures](#): provides assessment procedures for the security requirements in [Protecting specified information in non-Government of Canada systems and organizations \(ITSP.10.171\)](#), including assessment objectives and potential assessment methods and objects for each procedure
- [Annex A: Organization-defined parameters](#): provides additional information to support the protection of specified information

2 Fundamentals

The process used by organizations and assessors to assess the security requirements in ITSP.10.171 includes the following steps:

1. Preparing for the assessment
2. Developing a security and privacy assessment plan
3. Conducting the assessment
4. Documenting, analyzing and reporting the assessment results

Assessment of security and privacy controls and assurance activities (ITSP.10.033-02) provides additional information on the assessment process and the individual steps listed above.

This section describes the structure and content of the assessment procedures and the importance of assurance cases in providing the evidence necessary to determine compliance with the requirements.

2.1 Assessment procedures

ITSP.10.171 security requirements represent a subset of the controls that are necessary to protect the confidentiality of specified information. The security requirements are organized into 17 families. Each family contains the requirements related to its general security topic. The assessment procedures in [Section 3](#) are grouped by similar family designations to ensure the completeness and consistency of assessments. The procedures have been derived from the assessment procedures in ITSP.10.033-02.

The following are the security requirements families:

- Access control
- Awareness and training
- Audit and accountability
- Configuration management
- Identification and authentication
- Incident response
- Maintenance
- Media protection
- Personnel security
- Physical protection
- Risk assessment
- Security assessment and monitoring
- System and communications protection
- System and information integrity

- Planning
- System and services acquisition
- Supply chain risk management

An assessment procedure consists of a set of assessment objectives, each with an associated set of potential assessment methods and objects. The assessment procedures in [Section 3](#) have been derived from the assessment procedures in ITSP.10.033-02. Security requirement assessments comprise several key elements:

- **Assessment objects** identify the specific items being assessed as part of a given control or activity and include specifications, mechanisms, procedures and individuals
- **Specifications** are the document-based artifacts associated with a system-specific or common control or activity. These artifacts include
 - policies
 - procedures
 - plans
 - system security and privacy requirements
 - functional specifications
 - architectural designs
- **Mechanisms** are the specific hardware, software or firmware, including physical protection devices, that comprise safeguards and countermeasures employed within a system or common control or activity
- **Procedures** are the specific protection-related actions supporting a system or common control or activity that involve people, for example
 - conducting system backup operations
 - monitoring network traffic
 - exercising a contingency plan
- **Assessment methods** define the nature of the assessor's actions and include the following
 - **Examine:** the process of reviewing, inspecting, observing, studying or analyzing 1 or more assessment objects (that is, specifications, mechanisms or procedures) to facilitate assessor understanding, achieve clarification, or obtain evidence
 - **Interview:** the process of holding discussions with individuals or groups of individuals within an organization to facilitate assessor understanding, achieve clarification, or obtain evidence
 - **Test:** the process of exercising 1 or more assessment objects (that is, procedures or mechanisms) under specified conditions to compare the actual state of the object to the desired state or expected behaviour of the object
- Assessment methods have a set of associated **attributes** (scope and depth) that help define the level of effort for the assessment. The attributes are hierarchical, providing the means to define the scope, depth and rigour of the assessment for the increased assurances that may be needed for some systems

- The depth attribute addresses the rigour of and level of detail in the assessment efforts
- The scope attribute addresses the breadth of the assessment efforts, including the number and types of specifications, mechanisms and procedures to be examined or tested, and individuals to be interviewed
- The **level of effort** for the assessment is primarily determined by the privacy risk assessment or security categorization of the system or common control or activity being assessed, as described in Organizational cyber security and privacy risk management activities (ITSP.10.036). The values for these attributes range from security assurance level (SAL) 1 to SAL 5 (the SALs are defined in System lifecycle cyber security and privacy risk management activities (ITSP.10.037))
- The appropriate attribute values for a particular assessment method are based on the assurance requirements specified by the organization and are an important component of protecting information commensurate with risk are known as **risk management**

Figure 1: Structure and content of an assessment procedure

03.01.06 Least privilege – privileged accounts	Security requirement name
ODP:	ODP for security requirement
A.03.01.06.ODP: personnel or roles to which privileged accounts on the system are to be restricted are defined	
Determine if:	Multi-part determination statement
A.03.01.06.A: privileged accounts on the system are restricted to < A.03.01.06.ODP: 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	
A.03.01.06.C: administrative or superuser actions are required to be performed from a physical workstation which is dedicated to those specific tasks and isolated from all other functions and networks	
Potential 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; system management architecture documentation; DAW configuration settings; other relevant documents or records]	
Interview	
[Select from: personnel with responsibilities for defining least privileges; personnel with information security responsibilities; personnel with systems security engineering responsibilities; security architects; system administrators]	
Test	
[Select from: mechanisms for implementing least privilege functions; penetration testing on the DAW]	
References:	
Source assessment procedures: AC-06(02), AC-06(05), SI-400	

Figure 1 long description:

Figure 1 presents a screenshot of the security requirement 03.01.06 Least privilege – privileged accounts. The figure is intended to illustrate the structure and key components of a security requirement as it appears in the publication. Three annotated boxes are used to highlight specific elements of the requirement. The first box appears next to the header of the requirement and identifies the name of the security requirement. The second box is positioned next to the text “ODP:” and indicates that the text immediately below contains the organization-defined parameters (ODPs) associated with the requirement. The third box contains the text “Multi-part determination statement” and is placed next to the phrase “Determine if:”. The text that follows lists the set of actions or conditions that must be satisfied in order for the requirement to be considered implemented.

The structure and content of assessment procedures include the following elements in Figure 1:

- **Determination statements** have alphanumeric identifiers. Each determination statement begins with the letter “A” to indicate that it is part of an assessment procedure. They often present as “multi-part determination statements” as they have more than one action to take.
- The next **sequence of numbers or letters** (for example, 03.01.01.E or 03.01.01.F.02) indicates the security requirement name or identifier from ITSP.10.171 (and the specific control item if it is a multi-part requirement) that is the target of the assessment.
- **Organization-defined parameters (ODP)** for the security requirement are indicated by the letters “ODP”. If there are multiple ODPs in the determination statement, the ODP number is indicated in a square bracket (for example, 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 (for example, A.03.01.12.A[01], A.03.01.12.A[02], A.03.01.12.A[03])
- Applying an assessment procedure to a security requirement produces assessment results or **findings**. 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 **other than satisfied** indicates that there are potential anomalies that may need to be addressed by the organization. A finding 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 for control effectiveness and quality of activity execution is a process that involves compiling evidence from various assurance procedures conducted during the system lifecycle. The evidence comes from the implementation of the security and privacy controls and activities in the system and inherited by the system (common controls) and from the assessment of that implementation.

Assurance activities can be performed at 2 different levels:

- they can be related to a specific control, in support of a specific product or security mechanism
- they can support the system as a whole to assess its development and the integration of the controls in the system

Assurance activities that support system development are intended to improve the design, architecture, and engineering outcomes. The assurance activities that were labelled as “activities” in the [Security and privacy controls and assurance activities catalogue \(ITSP.10.033\)](#) function as such.

Assessing a control or an activity constitutes an assurance procedure. When evaluating an assurance activity, as defined in ITSP.10.033, the focus is on assessing the quality of its execution. This process is described in detail in ITSP.10.037.

Together, strength and assurance define the requirements that must be met in the implementation of a control to satisfy the control’s security or privacy objective.

The security or privacy **strength** is related to the implemented control’s potential ability to protect the confidentiality, integrity or availability of assets. As the strength increases, so does the effort or cost required by the threat actor to defeat the implemented control.

The protective potential of a control can be fulfilled only when it is implemented with adequate assurance.

Assurance consists of confidence-building tasks aimed at ensuring that a control is designed and implemented correctly and is operating as intended, or that an assurance activity is properly executed. Assurance also includes tasks that ensure that all controls in system design, implementation and operation satisfy the business needs for security and privacy.

Assurance is provided through tasks completed by system developers, implementers, operators, maintainers, and security and privacy assessors. Assurance is increased through additional efforts in the scope and depth of these tasks by contributing to the efficacy of the evidence and measures of confidence. Rigour and depth usually follow the same trajectory: when one is increased, the other should also be increased.

Robustness is a characterization of the strength and assurance of a security or privacy control. The strength is related to the control’s potential ability to protect the confidentiality, integrity or availability of assets. Assurance activities, as outlined in the catalogue, are assigned an assurance level only, not a robustness level.

A control incorporates a strength element when it mitigates a specific tradecraft. Since assurance activities do not directly counter tradecraft, the concept of strength is not applicable. The assurance of a control is related to the confidence that the control is designed and implemented correctly, is operating as intended, and is achieving the intended results in fulfilling the system and organizational security and privacy requirements.

For example, a security control can be conceptually strong (like an MFA mechanism) but come with no assurance (where there is no evidence like a security review or vulnerability testing to demonstrate the quality of its implementation). In this case it will have a lower effective robustness than a similar system that has higher assurance (like when a mechanism has been validated by undergoing rigorous testing and validation to confirm its security).

Controls that protect more sensitive or critical assets, or that are exposed to more significant threats will generally require stronger security or privacy solutions, more assurance in their implementation, and higher levels of robustness.

The robustness model defines a hierarchy of robustness levels that are based on expected injury and threat levels.

ITSP.10.037 and [Calculating robustness for boundary controls \(ITSP.80.032\)](#) provide more information on the robustness model.

The coverage assessment of a control answers the following questions:

- Does the control adequately safeguard the desired assets or other related controls that it supports?

- Is the control properly applied throughout the system?

For example, if an organization has a perimeter and builds a fence (control) to secure only three-quarters of the perimeter, leaving one-quarter unprotected, the security provided by the fence is incomplete. The unprotected quarter undermines the effectiveness of the secured sections, rendering the overall perimeter vulnerable.

An assessment must consider more than just the presence of a control. While the response to a question about whether a control exists is “yes, there is a fence,” the critical question is, “does the control provide appropriate coverage?” In this case, the answer is no, as the coverage is insufficient. This illustrates the importance of evaluating the adequacy and effectiveness of the control’s implementation.

3 Procedures

This section provides assessment procedures for the security requirements defined in [Protecting specified information in non-Government of Canada systems and organizations \(ITSP.10.171\)](#). Organizations that conduct security requirement assessments can develop their security assessment plans by using the information provided in the assessment procedures and selecting the specific assessment methods and objects that meet the organization's needs. Organizations also have flexibility in defining the level of rigour and detail associated with the assessment based on the assurance requirements of the organization.

3.1 Access control

The controls in the Access control family support the ability to permit or deny user access to resources within the system.

03.01.01 Account management

ODPs:

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

Determine if:

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 (for example, 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>**

Potential 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; privacy 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 and privacy 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

Determine if:

A.03.01.02[01]: approved authorizations for logical access to specified information 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

Potential 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 (for example, 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

Determine if:

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

A.03.01.03[02]: approved authorizations are enforced for controlling the flow of specified information between connected systems

Potential 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; privacy plan; other relevant documents or records]

Interview

[Select from: system administrators; personnel with security and privacy architecture responsibilities; personnel with information security and privacy 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**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

Potential 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

ODPs:

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

Determine if:

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

Potential assessment methods and objects:

Examine

[Select from: access control policy and procedures; procedures for least privilege; list of assigned access authorizations (user 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 privilege; 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

ODP:

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

Determine if:

A.03.01.06.A: privileged accounts on the system are restricted to **<A.03.01.06.ODP: 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

A.03.01.06.C: administrative or superuser actions are required to be performed from a physical workstation which is dedicated to those specific tasks and isolated from all other functions and networks

Potential 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; system management architecture documentation; dedicated administration workstation (DAW) configuration settings; other relevant documents or records]

Interview

[Select from: personnel with responsibilities for defining least privileges; personnel with information security responsibilities; personnel with systems security engineering responsibilities; security architects; system administrators]

Test

[Select from: mechanisms for implementing least privilege functions; penetration testing on the DAW]

References:

Source assessment procedures: AC-06(02), AC-06(05), SI-400

03.01.07 Least privilege – privileged functions

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

Potential 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 privilege; 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**ODPs:**

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

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

A.03.01.08.ODP[03]: 1 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)

Determine if:

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

Potential 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**Determine if:**

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

Potential 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; privacy plan; privacy impact assessment (PIA); privacy assessment report; other relevant documents or records]

Interview

[Select from: personnel with information security and privacy 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**ODPs:**

A.03.01.10.ODP[01]: 1 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)

Determine if:

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 re-establishes 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

Potential 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**ODP:**

A.03.01.11.ODP: conditions or trigger events that require session disconnect are defined

Determine if:

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

Potential 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**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[01]: remote execution of privileged commands is authorized

A.03.01.12.D[02]: remote access to security-relevant information is authorized

Potential 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 Not allocated

Withdrawn by NIST.

03.01.14 Not allocated

Withdrawn by NIST.

03.01.15 Not allocated

Withdrawn by NIST.

03.01.16 Wireless access

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

Potential 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 Not allocated

Withdrawn by NIST.

03.01.18 Access control for mobile devices

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 specified information on mobile devices

Potential 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 specified information on mobile devices; configurations of mobile devices]

References:

Source assessment procedures: AC-19, AC-19(05)

03.01.19 Not allocated

Withdrawn by NIST.

03.01.20 Use of external systems

ODP:

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

Determine if:

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: 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 specified information 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 specified information 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

Potential 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 Not allocated

Withdrawn by NIST.

03.01.22 Publicly accessible content

Determine if:

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

A.03.01.22.B[01]: the content on publicly accessible systems is reviewed for specified information

A.03.01.22.B[02]: specified information is removed from publicly accessible systems, if discovered

Potential 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 specified information 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

The Awareness and training controls deal with the education of users with respect to the security of the system.

03.02.01 Literacy training and awareness

ODPs:

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

Determine if:

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**>

Potential assessment methods and objects:

Examine

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

Interview

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

Test

[Select from: mechanisms for managing information security and privacy literacy training and awareness]

References:

Source assessment procedures: AT-02, AT-02(02), AT-02(03)

03.02.02 Role-based training

ODPs:

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

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

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

A.03.02.02.ODP[04]: events that require role-based security and privacy training content updates are defined

Determine if:

A.03.02.02.A.01[01]: role-based security and privacy training is provided to organizational personnel before authorizing access to the system or specified information

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

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

A.03.02.02.B[02]: role-based security and privacy training content is updated following <**A.03.02.02.ODP[04]: events**>

Potential assessment methods and objects:**Examine**

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

Interview

[Select from: personnel with responsibilities for role-based security and privacy training; personnel with assigned system security and privacy roles and responsibilities]

Test

[Select from: mechanisms for managing role-based security and privacy training and awareness]

References:

Source assessment procedure: AT-03

03.02.03 Not allocated

Withdrawn by NIST.

3.3 Audit and accountability

The Audit and accountability controls support the ability to collect, analyze, and store audit records associated with user operations performed within the system.

03.03.01 Event logging**ODPs:**

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

Determine if:

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**>

Potential 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; privacy plan; other relevant documents or records]

Interview

[Select from: personnel with audit and accountability responsibilities; personnel with information security and privacy responsibilities; system administrators]

Test

[Select from: mechanisms for implementing system auditing]

References:

Source assessment procedure: AU-02

03.03.02 Audit record content

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

Potential 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

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

Potential 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; privacy 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 and privacy 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

ODPs:

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

Determine if:

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>**

Potential 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; privacy plan; other relevant documents or records]

Interview

[Select from: personnel with audit and accountability responsibilities; personnel with information security and privacy 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

ODP:

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

Determine if:

A.03.03.05.A: system audit records are reviewed and analyzed **<A.03.03.05.ODP: 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

Potential 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; privacy 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 and privacy 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

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

Potential 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

ODP:

A.03.03.07.ODP: granularity of time measurement for audit record time stamps is defined

Determine if:

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: 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

Potential 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 time stamp generation]

References:

Source assessment procedure: AU-08

03.03.08 Protection of audit information

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

Potential 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; privacy plan; other relevant documents or records]

Interview

[Select from: personnel with audit and accountability responsibilities; personnel with information security and privacy 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 Not allocated

Withdrawn by NIST.

3.4 Configuration management

The Configuration management controls support the management and control of all components of the system such as hardware, software, and configuration items.

03.04.01 Baseline configuration

ODP:

A.03.04.01.ODP: the frequency of baseline configuration review and update is defined

Determine if:

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

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

A.03.04.01.B[01]: the baseline configuration of the system is reviewed <**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

Potential assessment methods and objects:

Examine

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

Interview

[Select from: personnel with configuration management responsibilities; personnel with information security and privacy 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

ODP:

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

Determine if:

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: configuration settings>**

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

Potential 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; privacy plan; other relevant documents or records]

Interview

[Select from: personnel with security configuration management responsibilities; personnel with privacy configuration management responsibilities; personnel with information security and privacy 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

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

Potential assessment methods and objects:

Examine

[Select from: configuration management policy and procedures; procedures for system configuration change control; configuration management plan; system architecture documentation; 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; privacy plan; PIAs; other relevant documents or records]

Interview

[Select from: personnel with configuration change control responsibilities; personnel with information security and privacy 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

Determine if:

A.03.04.04.A[01]: changes to the system are analyzed to determine potential security impacts prior to change implementation

A.03.04.04.A[02]: changes to the system are analyzed to determine potential privacy 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

Potential 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; privacy impact analysis documentation; PIA; privacy risk assessment documentation; system design documentation; analysis tools and outputs; change control records; system audit records; system security plan; privacy plan; other relevant documents or records]

Interview

[Select from: personnel with security impact analysis responsibilities; personnel with responsibility for conducting privacy impact analyses; personnel with information security and privacy responsibilities; members of change control board; system developers; system administrators]

Test

[Select from: processes for security impact analyses; processes for privacy impact analyses]

References:

Source assessment procedure: CM-04, CM-04(02)

03.04.05 Access restrictions for change

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

Potential 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 documentation; 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**ODPs:**

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

Determine if:

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

Potential 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 Not allocated

Withdrawn by NIST

03.04.08 Authorized software – allow by exception

ODP:

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

Determine if:

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

A.03.04.08.B: a deny-all, allow-by-exception policy for the execution of 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: frequency**>

Potential 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 Not allocated

Withdrawn by NIST.

03.04.10 System component inventory

ODP:

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

Determine if:

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

A.03.04.10.B[01]: the system component inventory is reviewed <**A.03.04.10.ODP: frequency**>

A.03.04.10.B[02]: the system component inventory is updated <**A.03.04.10.ODP: 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

Potential 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

Determine if:

A.03.04.11.A[01]: the location of specified information is identified and documented

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

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

A.03.04.11.B[01]: changes to the system or system component location where specified information is processed are documented

A.03.04.11.B[02]: changes to the system or system component location where specified information is stored are documented

Potential 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; security categorization of the information; personal information inventory documentation; data mapping documentation; audit records; list of users with system and system component access; change control records; system component inventory; system security plan; privacy 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 and privacy 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

ODPs:

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

Determine if:

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**>

Potential 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 documentation; 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

The Identification and authentication controls support the unique identification of users, processes acting on behalf of users and devices. They also support the authentication or verification of the identities of those users, processes or devices as a prerequisite to allowing access to organizational systems.

03.05.01 User identification, authentication, and reauthentication

ODP:

A.03.05.01.ODP: circumstances or situations that require reauthentication are defined

Determine if:

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: circumstances or situations>**

Potential assessment methods and objects:

Examine

[Select from: identification and authentication policy and procedures; list of circumstances or situations requiring reauthentication; 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

ODP:

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

Determine if:

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

A.03.05.02[02]: <A.03.05.02.ODP: devices or types of devices> are authenticated before establishing a system connection

Potential 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

Determine if:

A.03.05.03[01]: strong MFA for access to privileged accounts is implemented

A.03.05.03[02]: strong MFA for access to non-privileged accounts is implemented

Potential 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 MFA capability]

References:

Source assessment procedures: IA-02(01), IA-02(02)

03.05.04 Replay-resistant authentication

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

Potential 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

ODPs:

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

Determine if:

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>**

Potential 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 Not allocated

Withdrawn by NIST.

03.05.07 Password management

ODPs:

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

Determine if:

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**>

Potential 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 Not allocated

Withdrawn by NIST.

03.05.09 Not allocated

Withdrawn by NIST.

03.05.10 Not allocated

Withdrawn by NIST.

03.05.11 Authentication feedback**Determine if:**

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

Potential 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**ODPs:**

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

Determine if:

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

Potential 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

The Incident response controls support the establishment of an operational incident handling capability for organizational systems that includes:

- adequate preparation
- monitoring
- detection
- analysis
- containment
- recovery
- response

Incidents are monitored, documented, and reported to appropriate organizational officials and authorities.

03.06.01 Incident handling

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

Potential 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; privacy 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 and privacy 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

ODPs:

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

Determine if:

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

Potential 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; privacy 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 and privacy 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

ODP:

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

Determine if:

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

Potential 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; privacy plan; other relevant documents or records]

Interview

[Select from: personnel with incident response testing responsibilities; personnel with information security and privacy responsibilities]

References:

Source assessment procedure: IR-03

03.06.04 Incident response training

ODPs:

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

Determine if:

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>**

Potential 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; privacy plan; other relevant documents or records]

Interview

[Select from: personnel with incident response training and operational responsibilities; personnel with information security and privacy responsibilities]

References:

Source assessment procedure: IR-02

03.06.05 Incident response plan**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

Potential assessment methods and objects:**Examine**

[Select from: incident response policy; procedures addressing incident response planning; incident response plan; system security plan; privacy 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 and privacy responsibilities]

Test

[Select from: incident response plan and related processes]

References:

Source assessment procedure: IR-08

3.7 Maintenance

The Maintenance controls support periodic and timely maintenance on organizational systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance to ensure its ongoing availability.

03.07.01 Not allocated

Withdrawn by NIST.

03.07.02 Not allocated

Withdrawn by NIST.

03.07.03 Not allocated

Withdrawn by NIST.

03.07.04 Maintenance tools

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 specified information is prevented by verifying that there is no specified information on the equipment, sanitizing or destroying the equipment, or retaining the equipment within the facility

Potential 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 Non-local maintenance**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]: MFA is implemented in the establishment of non-local maintenance and diagnostic sessions

A.03.07.05.B[02]: replay resistance is implemented in the establishment of non-local maintenance and diagnostic sessions

A.03.07.05.C[01]: session connections are terminated when non-local maintenance is completed

A.03.07.05.C[02]: network connections are terminated when non-local maintenance is completed

Potential assessment methods and objects:**Examine**

[Select from: maintenance policy and procedures; remote access policy and procedures; procedures for non-local 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 non-local maintenance; mechanisms for implementing, supporting, or managing non-local maintenance; mechanisms for implementing MFA and replay resistance; mechanisms for terminating non-local maintenance sessions and network connections]

References:

Source assessment procedure: MA-04

03.07.06 Maintenance personnel**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

Potential 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

The Media protection controls support the protection of system media throughout their lifecycle. They help limit access to information on system media to authorized users and sanitize or destroy system media before disposal or release for reuse.

03.08.01 Media storage

Determine if:

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

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

Potential 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

Determine if:

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

Potential 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

Determine if:

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

Potential 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; privacy 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 and privacy 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

Determine if:

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

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

A.03.08.04[03]: system media that contain specified information are marked to indicate applicable specified information markings

Potential 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**Determine if:**

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

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

A.03.08.05.B: accountability for system media that contain specified information is maintained during transport outside of controlled areas

A.03.08.05.C: activities associated with the transport of system media that contain specified information are documented

Potential 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 Not allocated

Withdrawn by NIST.

03.08.07 Media use

ODP:

A.03.08.07.ODP: types of system media with usage restrictions or that are prohibited from use are defined

Determine if:

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

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

Potential assessment methods and objects:

Examine

[Select from: system media protection policy and procedures; system use policy; procedures for media usage restrictions; rules of behaviour; 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 Not allocated

Withdrawn by NIST.

03.08.09 System backup – cryptographic protection

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 specified information at backup storage locations

Potential 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

The Personnel security controls support the procedures required to ensure that all personnel who have access to systems have the necessary authorization as well as appropriate security screening levels. They ensure that organizational information and systems are protected during and after personnel actions such as terminations and transfers.

03.09.01 Personnel screening

ODP:

A.03.09.01.ODP: conditions that require the rescreening of individuals are defined

Determine if:

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: conditions>**

Potential 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

ODP:

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

Determine if:

A.03.09.02.A.01: upon termination of individual employment, system access is disabled within <**A.03.09.02.ODP: 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

Potential 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

The Physical protection controls support the control of physical access to systems, equipment, and the respective operating environments to authorized individuals. They facilitate the protection of the physical plant and support infrastructure for systems, the protection of systems against environmental hazards, and provide appropriate environmental controls in facilities containing systems.

03.10.01 Physical access authorizations

ODP:

A.03.10.01.ODP: the frequency at which to review the access list detailing authorized physical access by individuals is defined

Determine if:

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 physical access list is reviewed <**A.03.10.01.ODP: frequency**>

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

Potential 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

ODPs:

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

Determine if:

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**>

Potential 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 Not allocated

Withdrawn by NIST.

03.10.04 Not allocated

Withdrawn by NIST.

03.10.05 Not allocated

Withdrawn by NIST.

03.10.06 Alternate work site

ODP:

A.03.10.06.ODP: security requirements to be employed at alternate work sites are defined

Determine if:

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: security requirements>**

Potential 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; privacy 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 and privacy responsibilities]

Test

[Select from: processes for security and privacy at alternate work sites; mechanisms for supporting alternate work sites; security and privacy 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

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 specified information

Potential 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

Determine if:

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

Potential 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

The Risk assessment controls deal with the periodic conduct of risk assessments, including PIAs, resulting from the operation of organizational systems and associated handling, storage, or transmission of data and information.

03.11.01 Risk assessment

ODP:

A.03.11.01.ODP: the frequency at which to update the risk assessment is defined

Determine if:

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

A.03.11.01.B: risk assessments are updated <**A.03.11.01.ODP: frequency**>

Potential assessment methods and objects:**Examine**

[Select from: risk assessment policy and procedures; security and privacy planning policy and procedures; procedures for organizational assessments of risk; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; supply chain risk management (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; privacy plan; other relevant documents or records]

Interview

[Select from: personnel with risk assessment responsibilities; personnel with SCRM responsibilities; personnel with security and privacy 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

ODPs:

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

Determine if:

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

Potential 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 Not allocated

Withdrawn by NIST.

03.11.04 Risk response

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

Potential assessment methods and objects:

Examine

[Select from: risk assessment policy; assessment reports; system audit records; event logs; system security plan; privacy plan; other relevant documents or records]

Interview

[Select from: personnel with assessment and auditing responsibilities; system administrators; personnel with security and privacy 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

The Security assessment and monitoring controls deal with the security assessment and monitoring of the system.

03.12.01 Security assessment

ODP:

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

Determine if:

A.03.12.01: the security requirements for the system and its environment of operation are assessed **<A.03.12.01.ODP: frequency>** to determine if the requirements have been satisfied

Potential 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; privacy plan; other relevant documents or records]

Interview

[Select from: personnel with security assessment responsibilities; personnel with information security and privacy 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

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

Potential 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; privacy plan; other relevant documents or records]

Interview

[Select from: personnel with plans of action and milestones development and implementation responsibilities; personnel with information security and privacy 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

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

Potential 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; privacy assessment report; plan of action and milestones; system monitoring records; configuration management records; impact analyses; status reports; system security plan; privacy plan; other relevant documents or records]

Interview

[Select from: personnel with continuous monitoring responsibilities; personnel with information security and privacy 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 and privacy status reporting]

References:

Source assessment procedure: CA-07

03.12.04 Not allocated

Withdrawn by NIST.

03.12.05 Information exchange

ODPs:

- A.03.12.05.ODP[01]:** 1 or more of the following parameter values are selected: {interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; information sharing arrangements; service-level agreements; user agreements; nondisclosure agreements; other types of agreements}
- A.03.12.05.ODP[02]:** the frequency at which to review and update agreements is defined

Determine if:

A.03.12.05.A[01]: the exchange of specified information 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 specified information 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 and privacy 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>**

Potential 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; information sharing arrangements; nondisclosure agreements; system design documentation; enterprise architecture; security architecture; system configuration settings; system security plan; privacy 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 and privacy responsibilities]

References:

Source assessment procedure: CA-03

3.13 System and communications protection

The System and communications protection controls support the monitoring, control and protection of the systems themselves and of the communications between and within the systems.

03.13.01 Boundary protection

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

Potential 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; enterprise security architecture 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 Not allocated

Withdrawn by NIST.

03.13.03 Not allocated

Withdrawn by NIST.

03.13.04 Information in shared system resources

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

Potential 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 Not allocated

Withdrawn by NIST.

03.13.06 Network communications – deny by default – allow by exception

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

Potential 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 Not allocated

Withdrawn by NIST.

03.13.08 Transmission and storage confidentiality

Determine if:

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

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

Potential 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

ODP:

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

Determine if:

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: time period>** of inactivity

Potential 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

ODP:

A.03.13.10.ODP: requirements for key generation, distribution, storage, access, and destruction are defined

Determine if:

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: 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: requirements>**

Potential 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

ODP:

A.03.13.11.ODP: the types of cryptography for protecting the confidentiality of specified information are defined

Determine if:

A.03.13.11: the following types of cryptography are implemented to protect the confidentiality of specified information:

<A.03.13.11.ODP: types of cryptography>

Potential 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 Federal Information Processing Standards (FIPS) 140-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

ODP:

A.03.13.12.ODP: exceptions where remote activation is to be allowed are defined

Determine if:

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: exceptions>**

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

Potential 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**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

Potential 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 Not allocated

Withdrawn by NIST.

03.13.15 Session authenticity

Determine if:

A.03.13.15: the authenticity of communications sessions is protected

Potential 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 Not allocated

Withdrawn by NIST.

3.14 System and information integrity

The System and information integrity controls support the protection of the integrity of the system components and the data that it processes. They allow an organization to:

- identify, report and correct data and system flaws in a timely manner
- provide protection against malicious code
- monitor system security alerts and advisories
- take appropriate actions in response.

03.14.01 Flaw remediation

ODPs:

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

Determine if:

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

Potential 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; privacy 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 and privacy 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**ODP:**

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

Determine if:

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: 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 or quarantine malicious code, or take other mitigation actions in response to malicious code detection

Potential 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

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

Potential 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 Not allocated

Withdrawn by NIST.

03.14.05 Not allocated

Withdrawn by NIST.

03.14.06 System monitoring**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

Potential 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 Not allocated

Withdrawn by NIST.

03.14.08 Information management and retention

Determine if:

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

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

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

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

Potential assessment methods and objects:

Examine

[Select from: system and information integrity policy and procedures; laws, Orders in Council, directives, policies, regulations, standards, and operational requirements applicable to information management and retention; records retention and disposition policy; records retention and disposition procedures; personal information handling policy; media protection policy; media protection procedures; audit findings; system security plan; privacy plan; privacy program plan; personal information inventory; PIA, privacy risk assessment documentation; other relevant documents or records]

Interview

[Select from: personnel with information and records management, retention, and disposition responsibilities; personnel with information security and privacy 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

The Planning controls and assurance activities deal with the development, documentation, update, and implementation of security and privacy plans for organizational systems. Those plans describe the security and privacy controls and assurance activities in place or planned for the systems, and the rules of behaviour for individuals accessing the systems.

03.15.01 Policy and procedures

ODP:

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

Determine if:

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

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

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

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

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

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

Potential assessment methods and objects:

Examine

[Select from: security policies and procedures associated with the protection of specified information; audit findings; system security plan; privacy plan; other relevant documents or records]

Interview

[Select from: personnel with information security and privacy 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**ODP:**

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

Determine if:

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

A.03.15.02.A.02: a system security plan that 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 specified information is developed

A.03.15.02.B[01]: the system security plan is reviewed <**A.03.15.02.ODP: frequency**>

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

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

Potential assessment methods and objects:**Examine**

[Select from: security planning policy and procedures; procedures for system security and privacy plan development and implementation; procedures for system security and privacy plan reviews and updates; enterprise architecture; system security plan; privacy plan; records of system security and privacy 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 and privacy responsibilities]

Test

[Select from: processes for system security and privacy plan development, review, update, and approval]

References:

Source assessment procedure: PL-02

03.15.03 Rules of behaviour

ODP:

A.03.15.03.ODP: the frequency at which the rules of behaviour are reviewed and updated is defined

Determine if:

A.03.15.03.A: rules that describe responsibilities and expected behaviour for system usage and protecting specified information 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 behaviour is received before authorizing access to specified information and the system

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

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

Potential assessment methods and objects:

Examine

[Select from: security and privacy planning policy and procedures; rules of behaviour for system users; signed acknowledgements of rules of behaviour; records for rules of behaviour reviews and updates; system security plan; privacy plan; information sharing arrangements; other relevant documents or records]

Interview

[Select from: personnel with rules of behaviour 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 behaviour; personnel with information security and privacy responsibilities]

Test

[Select from: processes for establishing, reviewing, disseminating, and updating rules of behaviour; mechanisms for supporting or implementing the establishment, dissemination, review, and update of rules of behaviour]

References:

Source assessment procedure: PL-04

3.16 System and services acquisition

The System and services acquisition controls deal with the contracting of products and services required to support the implementation and operation of organizational systems. They ensure that sufficient resources are allocated for the protection of organizational systems, and they support system development lifecycle processes that incorporate security considerations.

03.16.01 Systems security engineering principles

ODP:

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

Determine if:

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

Potential 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 and privacy requirements and specifications for the system; system security plan; privacy plan; other relevant documents or records]

Interview

[Select from: personnel with acquisition/contracting responsibilities; personnel with information security and privacy 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

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

Potential 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 lifecycle 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

ODP:

A.03.16.03.ODP: security requirements to be satisfied by external system service providers are defined

Determine if:

A.03.16.03.A: the providers of external system services used for the processing, storage, or transmission of specified information comply with the following security requirements: **<A.03.16.03.ODP: 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

Potential 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 and privacy 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

The Supply chain risk management controls support the mitigation of cyber security risks throughout all phases of the supply chain.

03.17.01 Supply chain risk management plan

ODP:

A.03.17.01.ODP: the frequency at which to review and update the SCRM plan is defined

Determine if:

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

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

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

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

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

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

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

A.03.17.01.A[08]: the SCRM plan addresses risks associated with the 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: frequency**>

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

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

Potential 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 lifecycle (SDLC) 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 lifecycle documentation, including research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal; inter-organizational agreements and procedures; system security plan; privacy plan; privacy program plan; other relevant documents or records]

Interview

[Select from: personnel with acquisition responsibilities; personnel with SCRM responsibilities; personnel with information security and privacy responsibilities]

Test

[Select from: organizational processes for defining and documenting the 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

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

Potential 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; privacy plan; other relevant documents or records]

Interview

[Select from: personnel with acquisition responsibilities; personnel with SCRM responsibilities; personnel with information security and privacy 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

ODP:

A.03.17.03.ODP: 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

Determine if:

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: security requirements>**

Potential 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 and privacy 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; privacy plan; other relevant documents or records]

Interview

[Select from: personnel with acquisition responsibilities; personnel with information security and privacy 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

A.1 Organization-defined parameters

This appendix lists the organization-defined parameters (ODPs) that are included in the security requirements in Section 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 1: Organization-defined parameters

Security requirement	Organization-defined parameter
Account management A.03.01.01.ODP[01]	The time period for account inactivity before disabling is defined
Account management 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
Account management 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
Account management 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
Account management A.03.01.01.ODP[05]	The time period of expected inactivity requiring users to log out of the system is defined
Account management A.03.01.01.ODP[06]	Circumstances requiring users to log out of the system are defined
Least privilege A.03.01.05.ODP[01]	Security functions for authorized access are defined
Least privilege A.03.01.05.ODP[02]	Security-relevant information for authorized access is defined
Least privilege A.03.01.05.ODP[03]	The frequency at which to review the privileges assigned to roles or classes of users is defined
Least privilege—privileged accounts A.03.01.06.ODP	Personnel or roles to which privileged accounts on the system are to be restricted are defined
Unsuccessful logon attempts A.03.01.08.ODP[01]	The number of consecutive invalid logon attempts by a user allowed during a time period is defined
Unsuccessful logon attempts 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
Unsuccessful logon attempts A.03.01.08.ODP[03]	1 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}

Unsuccessful logon attempts A.03.01.08.ODP[04]	The time period for an account or node to be locked is defined (if selected)
Device lock 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}
Device lock A.03.01.10.ODP[02]	The time period of inactivity after which a device lock is initiated is defined (if selected)
Session termination A.03.01.11.ODP	Conditions or trigger events that require session disconnect are defined
Use of external systems A.03.01.20.ODP	Security requirements to be satisfied on external systems prior to allowing the use of or access to those systems by authorized individuals are defined
Literacy training and awareness A.03.02.01.ODP[01]	The frequency at which to provide security literacy training to system users after initial training is defined
Literacy training and awareness A.03.02.01.ODP[02]	Events that require security literacy training for system users are defined
Literacy training and awareness A.03.02.01.ODP[03]	The frequency at which to update security literacy training content is defined
Literacy training and awareness A.03.02.01.ODP[04]	Events that require security literacy training content updates are defined
Role-based training A.03.02.02.ODP[01]	The frequency at which to provide role-based security training to assigned personnel after initial training is defined
Role-based training A.03.02.02.ODP[02]	Events that require role-based security training are defined
Role-based training A.03.02.02.ODP[03]	The frequency at which to update role-based security training content is defined
Role-based training A.03.02.02.ODP[04]	Events that require role-based security training content updates are defined
Event logging A.03.03.01.ODP[01]	Event types selected for logging within the system are defined
Event logging A.03.03.01.ODP[02]	The frequency of event types selected for logging are reviewed and updated
Response to audit logging process failures A.03.03.04.ODP[01]	The time period for organizational personnel or roles receiving audit logging process failure alerts is defined
Response to audit logging process failures A.03.03.04.ODP[02]	Additional actions to be taken in the event of an audit logging process failure are defined
Audit record review, analysis, and reporting A.03.03.05.ODP	The frequency at which system audit records are reviewed and analyzed is defined
Time stamps A.03.03.07.ODP	Granularity of time measurement for audit record time stamps is defined

Baseline configuration A.03.04.01.ODP	The frequency of baseline configuration review and update is defined
Configuration settings A.03.04.02.ODP	Configuration settings for the system that reflect the most restrictive mode consistent with operational requirements are defined
Least functionality A.03.04.06.ODP[01]	Functions to be prohibited or restricted are defined
Least functionality A.03.04.06.ODP[02]	Ports to be prohibited or restricted are defined
Least functionality A.03.04.06.ODP[03]	Protocols to be prohibited or restricted are defined
Least functionality A.03.04.06.ODP[04]	Connections to be prohibited or restricted are defined
Least functionality A.03.04.06.ODP[05]	Services to be prohibited or restricted are defined
Least functionality 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
Authorized software – allow by exception A.03.04.08.ODP	The frequency at which to review and update the list of authorized software programs is defined
System component inventory A.03.04.10.ODP	The frequency at which to review and update the system component inventory is defined
System and component configuration for high-risk areas A.03.04.12.ODP[01]	Configurations for systems or system components to be issued to individuals traveling to high-risk locations are defined
System and component configuration for high-risk areas A.03.04.12.ODP[02]	Security requirements to be applied to the system or system components when individuals return from travel are defined
User identification, authentication, and reauthentication A.03.05.01.ODP	Circumstances or situations that require reauthentication are defined
Device identification and authentication A.03.05.02.ODP	Devices or types of devices to be uniquely identified and authenticated before establishing a connection are defined
Identifier management A.03.05.05.ODP[01]	The time period for preventing the reuse of identifiers is defined
Identifier management A.03.05.05.ODP[02]	Characteristics used to identify individual status are defined
Password management A.03.05.07.ODP[01]	The frequency at which to update the list of commonly used, expected, or compromised passwords is defined
Password management A.03.05.07.ODP[02]	Password composition and complexity rules are defined
Authenticator management A.03.05.12.ODP[01]	The frequency for changing or refreshing authenticators is defined
Authenticator management A.03.05.12.ODP[02]	Events that trigger the change or refreshment of authenticators are defined

Incident monitoring, reporting, and response assistance A.03.06.02.ODP[01]	The time period to report suspected incidents to the organizational incident response capability is defined
Incident monitoring, reporting, and response assistance A.03.06.02.ODP[02]	Authorities to whom incident information is to be reported are defined
Incident response testing A.03.06.03.ODP	The frequency at which to test the effectiveness of the incident response capability for the system is defined
Incident response training A.03.06.04.ODP[01]	The time period within which incident response training is to be provided to system users is defined
Incident response training A.03.06.04.ODP[02]	The frequency at which to provide incident response training to users is defined
Incident response training A.03.06.04.ODP[03]	The frequency at which to review and update incident response training content is defined
Incident response training A.03.06.04.ODP[04]	Events that initiate a review of the incident response training content are defined
Media use A.03.08.07.ODP	Types of system media with usage restrictions or that are prohibited from use are defined
Personnel screening A.03.09.01.ODP	Conditions that require the rescreening of individuals are defined
Personnel termination and transfer A.03.09.02.ODP	The time period within which to disable system access is defined
Physical access authorizations A.03.10.01.ODP	The frequency at which to review the access list detailing authorized facility access by individuals is defined
Monitoring physical access A.03.10.02.ODP[01]	The frequency at which to review physical access logs is defined
Monitoring physical access A.03.10.02.ODP[02]	Events or potential indications of events requiring physical access logs to be reviewed are defined
Alternate work site A.03.10.06.ODP	Security requirements to be employed at alternate work sites are defined
Risk assessment A.03.11.01.ODP	The frequency at which to update the risk assessment is defined
Vulnerability monitoring and scanning A.03.11.02.ODP[01]	The frequency at which the system is monitored for vulnerabilities is defined
Vulnerability monitoring and scanning A.03.11.02.ODP[02]	The frequency at which the system is scanned for vulnerabilities is defined
Vulnerability monitoring and scanning A.03.11.02.ODP[03]	Response times to remediate system vulnerabilities are defined

Vulnerability monitoring and scanning A.03.11.02.ODP[04]	The frequency at which to update system vulnerabilities to be scanned is defined
Security assessment A.03.12.01.ODP	The frequency at which to assess the security requirements for the system and its environment of operation is defined
Information exchange A.03.12.05.ODP[01]	1 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}
Information exchange A.03.12.05.ODP[02]	The frequency at which to review and update agreements is defined
Network disconnect A.03.13.09.ODP	The time period of inactivity after which the system terminates a network connection associated with a communications session is defined
Cryptographic key establishment and management A.03.13.10.ODP	Requirements for key generation, distribution, storage, access, and destruction are defined
Cryptographic protection A.03.13.11.ODP	The types of cryptography for protecting the confidentiality of specified information are defined
Collaborative computing devices and applications A.03.13.12.ODP	Exceptions where remote activation is to be allowed are defined
Flaw remediation 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
Flaw remediation 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
Malicious code protection A.03.14.02.ODP	The frequency at which malicious code protection mechanisms perform scans is defined
Policy and procedures A.03.15.01.ODP	The frequency at which the policies and procedures for implementing security requirements are reviewed and updated is defined
System security plan A.03.15.02.ODP	The frequency at which the system security plan is reviewed and updated is defined
Rules of behaviour A.03.15.03.ODP	The frequency at which the rules of behaviour are reviewed and updated is defined
Systems security engineering principles A.03.16.01.ODP	Systems security engineering principles to be applied to the development or modification of the system and system components are defined
External system services A.03.16.03.ODP	Security requirements to be satisfied by external system service providers are defined

Supply chain risk management plan A.03.17.01.ODP	The frequency at which to review and update the supply chain risk management plan is defined
Supply chain requirements and processes A.03.17.03.ODP	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

Foreword

This is an UNCLASSIFIED publication, issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information or to suggest amendments, contact the Cyber Centre:

- by email: contact@cyber.gc.ca
- by phone: [613-949-7048](tel:613-949-7048) or [1-833-CYBER-88](tel:1-833-CYBER-88)

Effective date

This publication takes effect on April 20, 2026.

Revision history

Revision	Amendments	Date
1	First release.	April 20, 2026

D97-3/10-171-01-2026E-PDF

ISBN 978-0-660-99556-4