03.08.07 Media Use

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: MP-07

03.08.08 Withdrawn

Incorporated into 03.08.07.

03.08.09 System Backup – Cryptographic Protection

ASSESSMENT OBJECTIVE

Determine if:

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

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

3.9. Personnel Security

03.09.01 Personnel Screening

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

[SELECT FROM: processes for personnel screening and rescreening]

REFERENCES

Source Assessment Procedure: PS-03

03.09.02 Personnel Termination and Transfer

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

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

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

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

A.03.09.02.b.01[02]: upon individual reassignment or transfer to other positions in the organization, the ongoing operational need for current logical and physical access authorizations to the system and facility is confirmed.

A.03.09.02.b.02: upon individual reassignment or transfer to other positions in the organization, access authorization is modified to correspond with any changes in operational need.

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedures: PS-04, PS-05

3.10. Physical Protection

03.10.01 Physical Access Authorizations

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

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

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: PE-02

03.10.02 Monitoring Physical Access

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: PE-06

03.10.03 Withdrawn

Incorporated into 03.10.07.

03.10.04 Withdrawn

Incorporated into 03.10.07.

03.10.05 Withdrawn

Incorporated into 03.10.07.

03.10.06 Alternate Work Site

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: PE-17

03.10.07 Physical Access Control

ASSESSMENT OBJECTIVE

Determine if:

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

A.03.10.07.a.02: physical access authorizations are enforced at entry and exit points to the facility where the system resides by controlling ingress and egress with physical access control systems, devices, or guards.

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

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

A.03.10.07.c[02]: visitor activity is controlled.

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

A.03.10.07.e: physical access to output devices is controlled to prevent unauthorized individuals from obtaining access to CUI.

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: PE-03, PE-05

03.10.08 Access Control for Transmission

ASSESSMENT OBJECTIVE

Determine if:

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: PE-04

3.11. Risk Assessment

03.11.01 Risk Assessment

ASSESSMENT OBJECTIVE

Determine if:

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

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

A.03.11.01.b: risk assessments are updated ***<A.03.11.01.ODP[01]: frequency>***.

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

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

03.11.02 Vulnerability Monitoring and Scanning

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

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

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

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

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

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

A.03.11.02.b: system vulnerabilities are remediated within ***<A.03.11.02.ODP[03]: response times>***.

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

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

03.11.03 Withdrawn

Incorporated into 03.11.02.

03.11.04 Risk Response

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: RA-07

3.12. Security Assessment and Monitoring

03.12.01 Security Assessment

ASSESSMENT OBJECTIVE

Determine if:

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

A.03.12.01: the security requirements for the system and its environment of operation are assessed ***<A.03.12.01.ODP[01]: frequency>*** to determine if the requirements have been satisfied.

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: CA-02

03.12.02 Plan of Action and Milestones

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: CA-05

03.12.03 Continuous Monitoring

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

A.03.12.03[04]: security assessments are included in the continuous monitoring strategy.

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: CA-07

03.12.04 Withdrawn

Incorporated into 03.15.02.

03.12.05 Information Exchange

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

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

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

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

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

A.03.12.05.c[01]: exchange agreements are reviewed ***<A.03.12.05.ODP[02]: frequency>***.

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

REFERENCES

Source Assessment Procedure: CA-03

3.13. System and Communications Protection

03.13.01 Boundary Protection

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

[SELECT FROM: mechanisms for implementing boundary protection capabilities]

REFERENCES

Source Assessment Procedure: SC-07

03.13.02 Withdrawn

Recategorized as NCO.

03.13.03 Withdrawn

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

03.13.04 Information in Shared System Resources

ASSESSMENT OBJECTIVE

Determine if:

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: SC-04

03.13.05 Withdrawn

Incorporated into 03.13.01.

03.13.06 Network Communications – Deny by Default – Allow by Exception

ASSESSMENT OBJECTIVE

Determine if:

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: SC-07(05)

03.13.07 Withdrawn

Addressed by 03.01.12, 03.04.02 and 03.04.06.

03.13.08 Transmission and Storage Confidentiality

ASSESSMENT OBJECTIVE

Determine if:

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

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

03.13.09 Network Disconnect

ASSESSMENT OBJECTIVE

Determine if:

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: SC-10

03.13.10 Cryptographic Key Establishment and Management

ASSESSMENT OBJECTIVE

Determine if:

A.03.13.10.ODP[01]: ***requirements for key generation, distribution, storage, access, and destruction are defined.***

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: SC-12

03.13.11 Cryptographic Protection

ASSESSMENT OBJECTIVE

Determine if:

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: SC-13

03.13.12 Collaborative Computing Devices and Applications

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: SC-15

03.13.13 Mobile Code

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: SC-18

03.13.14 Withdrawn

Technology-specific.

03.13.15 Session Authenticity

ASSESSMENT OBJECTIVE

Determine if:

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: SC-23

03.13.16 Withdrawn

Incorporated into 03.13.08.

3.14. System and Information Integrity

03.14.01 Flaw Remediation

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

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

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: SI-02

03.14.02 Malicious Code Protection

ASSESSMENT OBJECTIVE

Determine if:

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

A.03.14.02.a[01]: malicious code protection mechanisms are implemented at system entry and exit points to detect malicious code.

A.03.14.02.a[02]: malicious code protection mechanisms are implemented at system entry and exit points to eradicate malicious code.

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

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: SI-03

03.14.03 Security Alerts, Advisories, and Directives

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: SI-05

03.14.04 Withdrawn

Incorporated into 03.14.02.

03.14.05 Withdrawn

Addressed by 03.14.02.

03.14.06 System Monitoring

ASSESSMENT OBJECTIVE

Determine if:

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

A.03.14.06.a.01[02]: the system is monitored to detect indicators of potential attacks.

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

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

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

03.14.07 Withdrawn

Incorporated into 03.14.06.

03.14.08 Information Management and Retention

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: SI-12

3.15. Planning

03.15.01 Policy and Procedures

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

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

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

[SELECT FROM: personnel with information security responsibilities]

REFERENCES

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

03.15.02 System Security Plan

ASSESSMENT OBJECTIVE

Determine if:

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

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

A.03.15.02.a.02: a system security plan that identifies the information types processed, stored, and transmitted by the system is developed.

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

A.03.15.02.a.04: a system security plan that describes the operational environment for the system and any dependencies on or connections to other systems or system components is developed.

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

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

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

A.03.15.02.a.08: a system security plan that includes other relevant information necessary for the protection of CUI is developed.

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: PL-02

03.15.03 Rules of Behavior

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: PL-04

3.16. System and Services Acquisition

03.16.01 Systems Security Engineering Principles

ASSESSMENT OBJECTIVE

Determine if:

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: SA-08

03.16.02 Unsupported System Components

ASSESSMENT OBJECTIVE

Determine if:

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: SA-22

03.16.03 External System Services

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

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

Interview

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

Test

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

REFERENCES

Source Assessment Procedure: SA-09

3.17. Supply Chain Risk Management

03.17.01 Supply Chain Risk Management Plan

ASSESSMENT OBJECTIVE

Determine if:

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

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

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

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

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

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

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

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

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

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

A.03.17.01.a[10]: the SCRM plan addresses risks associated with the disposal of the system, system components, or system services.

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

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

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

ASSESSMENT METHODS AND OBJECTS

Examine

[SELECT FROM: SCRM policy and procedures; SCRM plan; system and services acquisition policy and procedures; system and services acquisition procedures; procedures for supply chain protection; procedures for protecting the SCRM plan from unauthorized disclosure; system development life cycle procedures; procedures for the integration of information security requirements into the acquisition process; acquisition documentation; service-level agreements; acquisition contracts for the system, system components, or system services; list of supply chain threats; list of safeguards for supply chain threats; system life cycle documentation, including research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal; inter-organizational agreements and procedures; system security plan; other relevant documents or records]

Interview

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