| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SC-12** | CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | |
| **SC-12.1**  **SC-12.1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization establishes and manages cryptographic keys for required cryptography employed within the information system.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing cryptographic key management and establishment; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for cryptographic key establishment or management].  **Test**: [*select from:* Automated mechanisms implementing cryptographic key management and establishment within the information system]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: SC-13, SC-17  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions**  **\*\*See “**[**Assessment Case Overview**](http://csrc.nist.gov/groups/SMA/fisma/assessment-cases-overview.html)**” for selecting, tailoring and executing action steps\*\*** |
|  | | *\*\*Assessment Case Assessor Note:* More convincing evidence (i.e., greater assurance) of correct implementation and operating as intended can be obtained through the assessment case actions by:   1. **Replacing bracketed values in action gathering statements to apply greater rigor in the assessment** (e.g, . replacing [“*reviewing*”] with “*studying*” or “*analyzing*”; replacing [“*observing*”] with “*inspecting*” or “*analyzing*”; replacing [“*basic*”] with “*focused*” or “*comprehensive*”); 2. **Replacing bracketed values in action gathering statements to apply greater sample coverage in the assessment** (e.g, . replacing [“*basic”*] sample with “*focused*” or “*sufficiently large”* sample); 3. **Defining additional action steps to the list of action steps suggested herein that exercise additional test methods** (i.e., Examine, Interview or Test) on additional assessment objects. |
| **SC-12.1.1.1** | | **Examine** system and communications protection policy, procedures addressing cryptographic key management and establishment, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed for establishing and managing cryptographic keys for required cryptography employed within the information system.  Note to assessor: Cryptographic key establishment and management can be performed using manual procedures or automated mechanisms with supporting manual procedures. |
| **SC-12.1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-12.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-12.1.1.1. |
| **SC-12.1.1.3** | | **Examine** records resulting from the measures employed to establish and manage cryptographic keys for required cryptography used within the information system; [*reviewing*] for evidence that the measures identified in SC-12.1.1.1 are being applied. |
| **SC-12.1.1.4** | | **Interview** an agreed-upon [*basic*]sample of organizational personnel with responsibilities for cryptographic key establishment or management; conducting [*basic*]discussions for further evidence that the measures identified in SC-12.1.1.1 are being applied. |
| **SC-12.1.1.5** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-12.1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **SC-12(1)** | | CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT |
| **SC-12(1).1**  **SC-12(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the organization maintains availability of information in the event of the loss of cryptographic keys by users.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing cryptographic key management, establishment, and recovery; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CP-2, CP-9, CP-10, SC-13, SC-17  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **SC-12(1).1.1.1** | | **Examine** system and communications protection policy, procedures addressing cryptographic key management, establishment, and recovery, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to maintain availability of information in the event of the loss of cryptographic keys by users. |
| **SC-12(1).1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-12(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-12(1).1.1.1. |
| **SC-12(1).1.1.3** | | **Examine** information system backup and recovery records resulting from the measures employed to maintain availability of information in the event of loss of cryptographic keys by users; [*reviewing*] for evidence that the measures identified in SC-12(1).1.1.1 are being applied. |
| **SC-12(1).1.1.4** | | **Interview** an agreed-upon [*basic*]sample of organizational personnel with responsibilities for cryptographic key establishment or management; conducting [*basic*]discussions for further evidence that the measures identified in SC-12(1).1.1.1 are being applied. |
| **SC-12(1).1.1.5** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-12(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-12(2)** | CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT |
| **SC-12(2).1**  **SC-12(2).1.1**  **SC-12(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines whether it will use NIST-approved or NSA-approved key management technology and processes; and* 2. *the organization produces, controls, and distributes symmetric cryptographic keys using the organization-defined key management technology and processes.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing cryptographic key management, establishment, and recovery; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Interview**:[*select from:* Organizational personnel with responsibilities for cryptographic key establishment or management]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: SC-13, SC-17  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-12(2).1.1.1** | **Examine** system and communications protection policy, procedures addressing cryptographic key management, establishment, and recovery, security plan, or other relevant documents; [*reviewing*] for the key management technology and processes (NIST-approved or NSA-approved) to be employed. |
|  |  |
| **SC-12(2).1.2.1** | **Examine** system and communications protection policy, procedures addressing cryptographic key management, establishment, and recovery, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to produce, control, and distribute symmetric cryptographic keys using the key management technology and processes identified in SC-12(2).1.1.1. |
| **SC-12(2).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-12(2).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-12(2).1.2.1. |
| **SC-12(2).1.2.3** | **Examine** change control records, information system audit records, information system monitoring records, or other relevant records resulting from the processes employed to produce, control, and distribute symmetric cryptographic keys; [*reviewing*] for evidence that the measures identified in SC-12(2).1.2.1 are being applied using the key management technology and processes identified in SC-12(2).1.1.1. |
| **SC-12(2).1.2.4** | **Interview** an agreed-upon [*basic*]sample of organizational personnel with responsibilities for cryptographic key establishment or management; conducting [*basic*]discussions for further evidence the measures identified in SC-12(2).1.2.1 are being employed. |
| **SC-12(2).1.2.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-12(2).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-12(3)** | CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT |
| **SC-12(3).1**  **SC-12(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization produces, controls, and distributes symmetric and asymmetric cryptographic keys using NSA-approved key management technology and processes.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing cryptographic key management, establishment, and recovery; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Interview**:[*select from:* Organizational personnel with responsibilities for cryptographic key establishment or management]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: SC-13, SC-17  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-12(3).1.1.1** | **Examine** system and communications protection policy, procedures addressing cryptographic key management, establishment, and recovery, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the NSA-approved key management technology and processes (including automated mechanisms and their configuration settings) to be employed to produce, control, and distribute symmetric and asymmetric cryptographic keys. |
| **SC-12(3).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-12(3).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-12(3).1.1.1. |
| **SC-12(3).1.1.3** | **Examine** change control records, information system audit records, information system monitoring records, or other relevant records resulting from the processes employed to produce, control, and distribute symmetric and asymmetric cryptographic keys; [*reviewing*] for evidence that the NSA-approved key management technology and processes identified in SC-12(3).1.1.1 are being applied. |
| **SC-12(3).1.1.4** | **Interview** an agreed-upon [*basic*]sample of organizational personnel with responsibilities for cryptographic key establishment or management; conducting [*basic*]discussions for further evidence the measures identified in SC-12(3).1.1.1 are being employed. |
| **SC-12(3).1.1.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-12(3).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-12(4)** | CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT |
| **SC-12(4).1**  **SC-12(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 certificates or prepositioned keying material.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing cryptographic key management, establishment, and recovery; information system design documentation; information system configuration settings and associated documentation; information system cryptographic keys; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: SC-13, SC-17  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-12(4).1.1.1** | **Examine** system and communications protection policy, procedures addressing cryptographic key management, establishment, and recovery, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the approved, PKI Class 3 certificates or prepositioned key material (including automated mechanisms and their configuration settings) to be employed to produce, control, and distribute asymmetric cryptographic keys. |
| **SC-12(4).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-12(4).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-12(4).1.1.1. |
| **SC-12(4).1.1.3** | **Examine** change control records, information system audit records, information system monitoring records, or other relevant records resulting from the processes employed to produce, control, and distribute asymmetric cryptographic keys; [*reviewing*] for evidence that the approved, PKI Class 3 certificates or prepositioned material identified in SC-12(4).1.1.1 are being applied. |
| **SC-12(4).1.1.4** | **Interview** an agreed-upon [*basic*]sample of organizational personnel with responsibilities for cryptographic key establishment or management; conducting [*basic*]discussions for further evidence the measures identified in SC-12(4).1.1.1 are being employed. |
| **SC-12(4).1.1.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-12(4).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-12(5)** | CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT |
| **SC-12(5).1**  **SC-12(5).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user’s private key.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing cryptographic key management, establishment, and recovery; information system design documentation; information system configuration settings and associated documentation; information system cryptographic keys; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: SC-13, SC-17  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-12(5).1.1.1** | **Examine** system and communications protection policy, procedures addressing cryptographic key management, establishment, and recovery, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the approved, PKI Class 3 or Class 4 certificates and hardware security tokens (including automated mechanisms and their configuration settings) to be employed to produce, control, distribute, and protect asymmetric cryptographic keys. |
| **SC-12(5).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-12(5).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-12(5).1.1.1. |
| **SC-12(5).1.1.3** | **Examine** change control records, information system audit records, information system monitoring records, or other relevant records resulting from the processes employed to produce, control, distribute, and protect asymmetric cryptographic keys; [*reviewing*] for evidence that the approved, PKI Class 3 or Class 4 certificates and hardware security tokens identified in SC-12(5).1.1.1 are being applied. |
| **SC-12(5).1.1.4** | **Interview** an agreed-upon [*basic*]sample of organizational personnel with responsibilities for cryptographic key establishment or management; conducting [*basic*]discussions for further evidence the measures identified in SC-12(5).1.1.1 are being employed. |
| **SC-12(5).1.1.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-12(5).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |