| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SC-3** | SECURITY FUNCTION ISOLATION | |
| **SC-3.1**  **SC-3.1.1**  **SC-3.1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the security functions of the information system to be isolated from nonsecurity functions; and* 2. *the information system isolates security functions from nonsecurity functions.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing security function isolation; list of security functions to be isolated from nonsecurity functions; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Separation of security functions from nonsecurity functions within the information system]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, AC-4, AC-5, AC-6, CM-6, CM-7, SA-4, SA-5, SC-2, SC-7  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-3.1.1.1** | | **Examine** system and communications protection policy, procedures addressing security function isolation, security plan, or other relevant documents; [*reviewing*] for the security functions of the information system to be isolated from nonsecurity functions. |
| **SC-3.1.2.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to isolate security functions from nonsecurity functions as identified in SC-3.1.1.1. |
|  | |  |
| **SC-3.1.2.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-3.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-3.1.1.1. |
| **SC-3.1.2.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-3.1.1.1; 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-3(1)** | | SECURITY FUNCTION ISOLATION |
| **SC-3(1).1**  **SC-3(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the information system implements underlying hardware separation mechanisms to facilitate security function isolation.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing security function isolation; information system design documentation; hardware separation mechanisms; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Hardware separation mechanisms facilitating security function isolation]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SA-4, SA-5, SC-2, SC-7, SC-32  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **SC-3(1).1.1.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to implement underlying hardware separation mechanisms to facilitate security function isolation. |
| **SC-3(1).1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-3(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-3(1).1.1.1. |
| **SC-3(1).1.1.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-3(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-3(2)** | SECURITY FUNCTION ISOLATION |
| **SC-3(2).1**  **SC-3(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system isolates security functions enforcing access and information flow control from both nonsecurity functions and other security functions.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing security function isolation; list of critical security functions; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Isolation of security functions enforcing access and information flow control]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, AC-4, AC-5, AC-6, CM-6, SA-4, SA-5, SC-2, SC-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-3(2).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to isolate security functions enforcing access and information flow control from both nonsecurity functions and other security functions. |
| **SC-3(2).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-3(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-3(2).1.1.1. |
| **SC-3(2).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-3(2).1.1.1; 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-3(3)** | SECURITY FUNCTION ISOLATION |
| **SC-3(3).1**  **SC-3(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization implements an information system isolation boundary to minimize the number of nonsecurity functions included within the boundary containing security functions.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing security function isolation; 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: AC-3, AC-4, AC-5, AC-6, CM-6, SA-4, SA-5, SC-7, SC-11  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-3(3).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to implement an information system isolation boundary that minimizes the number of nonsecurity functions included within the boundary containing security functions. |
| **SC-3(3).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SC-3(3).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-3(3).1.1.1. |
| **SC-3(3).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-3(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-3(4)** | SECURITY FUNCTION ISOLATION |
| **SC-3(4).1**  **SC-3(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization implements security functions as largely independent modules that avoid unnecessary interactions between modules.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing security function isolation; 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: CM-6, SA-3, SA-4,SA-13  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-3(4).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to implement security functions as largely independent modules that avoid unnecessary interactions between modules. |
| **SC-3(4).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SC-3(4).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-3(4).1.1.1. |
| **SC-3(4).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-3(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-3(5)** | SECURITY FUNCTION ISOLATION |
| **SC-3(5).1**  **SC-3(5).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing security function isolation; 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: CM-6, SA-3, SA-4, SA-13  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-3(5).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers. |
| **SC-3(5).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SC-3(5).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-3(5).1.1.1. |
| **SC-3(5).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-3(5).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |