| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AC-4** | INFORMATION FLOW ENFORCEMENT | |
| **AC-4.1**  **AC-4.1.1**  **AC-4.1.2**  **AC-4.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines applicable policy for controlling the flow of information within the system and between interconnected systems;* 2. *the organization defines approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy; and* 3. *the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system baseline configuration; list of information flow authorizations; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information flow enforcement policy]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, CA-3, CM-2, IA-2, SA-8  concurrent controls: AC-3, AC-17, AC-18, AC-19, AC-21, CM-6, CM-7, SC-2, SC-5, SC-7,  SC-18  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. |
| **AC-4.1.1.1** | | **Examine** access control policy, procedures addressing information flow enforcement, security plan, or other relevant documents; [*reviewing*] for the applicable policy for controlling the flow of information within the system and between interconnected systems. |
|  | |  |
| **AC-4.1.2.1** | | **Examine** access control policy, procedures addressing information flow enforcement, security plan, or other relevant documents; [*reviewing*] for the approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with the applicable policy identified in AC-4.1.1.1. |
|  | |  |
| **AC-4.1.3.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to enforce the approved authorizations identified in AC-4.1.2.1 within the system and between interconnected systems in accordance with the applicable policy identified in AC-4.1.1.1. |
| **AC-4.1.3.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4.1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4.1.3.1. |
| **AC-4.1.3.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4.1.3.1; 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)** | | |
| **AC-4(1)** | | INFORMATION FLOW ENFORCEMENT |
| **AC-4(1).1**  **AC-4(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the information system enforces information flow control using explicit security attributes on information, source, and destination objects as a basis for flow control decisions.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information flow enforcement policy]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-16, SC-7, SC-16, CM-6  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(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 enforce information flow control using explicit security attributes on information, source and destination objects as a basis for flow control decisions. |
| **AC-4(1).1.1.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(1).1.1.1. |
| **AC-4(1).1.1.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(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)** | |
| **AC-4(2)** | INFORMATION FLOW ENFORCEMENT |
| **AC-4(2).1**  **AC-4(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system enforces information flow control using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information flow enforcement policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-7, SC-32  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(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 enforce information flow control using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions. |
| **AC-4(2).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-4(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(2).1.1.1. |
| **AC-4(2).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(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)** | |
| **AC-4(3)** | INFORMATION FLOW ENFORCEMENT |
| **AC-4(3).1**  **AC-4(3).1.1**  **AC-4(3).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines policy that allows or disallows information flows based on changing conditions or operational consideration; and* 2. *the information system enforces dynamic information flow control based on policy that allows or disallows information flows based on changing conditions or operational considerations.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information flow enforcement policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(3).1.1.1** | **Examine** access control policy, procedures addressing information flow enforcement, security plan, or other relevant documents; [*reviewing*] for the policy that allows or disallows information flows based on changing conditions or operational considerations. |
|  |  |
| **AC-4(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 enforce dynamic information flow control based on the policy identified in AC-4(3).1.1.1 that allows or disallows information flows based on changing conditions or operational considerations. |
| **AC-4(3).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-4(3).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(3).1.2.1. |
| **AC-4(3).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(3).1.2.1; 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)** | |
| **AC-4(4)** | INFORMATION FLOW ENFORCEMENT |
| **AC-4(4).1**  **AC-4(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system prevents encrypted data from bypassing content-checking mechanisms.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information flow enforcement policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-8, SC-9, SC-13  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(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 prevent encrypted data from bypassing content-checking mechanisms. |
| **AC-4(4).1*.*1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(4).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(4).1.1.1. |
| **AC-4(4).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(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)** | |
| **AC-4(5)** | INFORMATION FLOW ENFORCEMENT |
| **AC-4(5).1**  **AC-4(5).1.1**  **AC-4(5).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the limitations on the embedding of data types with other data types; and* 2. *the information system enforces organization-defined limitations on the embedding of data types within other data types.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information flow enforcement policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(5).1.1.1** | **Examine** access control policy, procedures addressing information flow enforcement, security plan, or other relevant documents; [*reviewing*] for the limitations on the embedding of data types with other data types. |
|  |  |
| **AC-4(5).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 enforce limitations on the embedding of data types within other data types as identified in AC-4(5).1.1.1. |
| **AC-4(5).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(5).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(5).1.2.1. |
| **AC-4(5).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(5).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 6** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-4(6)** | INFORMATION FLOW ENFORCEMENT |
| **AC-4(6).1**  **AC-4(6).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system enforces information flow control on metadata.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information flow enforcement policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(6).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 enforce information flow control on metadata. |
| **AC-4(6).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-4(6).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(6).1.1.1. |
| **AC-4(6).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(6).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 7** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-4(7)** | INFORMATION FLOW ENFORCEMENT |
| **AC-4(7).1**  **AC-4(7).1.1**  **AC-4(7).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the one-way information flows to be enforced by the information system; and* 2. *the information system enforces organization-defined one-way information flows using hardware mechanisms.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Hardware mechanisms implementing information flow enforcement policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-7, SC-32  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(7).1.1.1** | **Examine** access control policy, procedures addressing information flow enforcement, security plan, or other relevant documents; [*reviewing*] for the one-way information flows to be enforced by the information system. |
|  |  |
| **AC-4(7).1.2.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the hardware mechanisms and their configuration settings to be employed to enforce the one-way information flows identified in AC-4(7).1.1.1. |
| **AC-4(7).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the hardware mechanisms identified in AC-4(7).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(7).1.2.1. |
| **AC-4(7).1.2.3** | **Test** an agreed-upon [*basic*]sample of the hardware mechanisms and their configuration settings identified in AC-4(7).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 8** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-4(8)** | INFORMATION FLOW ENFORCEMENT |
| **AC-4(8).1**  **AC-4(8).1.1**  **AC-4(8).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the security policy filters to be enforced by the information system; and* 2. *the information system enforces information flow control using organization-defined security policy filters as a basis for flow control decisions.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; list of security policy filters; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information flow enforcement policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-16, CM-6, SC-7, SC-16  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(8).1.1.1** | **Examine** access control policy, procedures addressing information flow enforcement, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the security policy filters to be enforced by the information system. |
|  |  |
| **AC-4(8).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 enforce information flow control using the security policy filters identified in AC-4(8).1.1.1 as a basis for flow control decisions. |
| **AC-4(8).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(8).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(8).1.2.1. |
| **AC-4(8).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(8).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 9** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-4(9)** | INFORMATION FLOW ENFORCEMENT |
| **AC-4(9).1**  **AC-4(9).1.1**  **AC-4(9).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the security policy filters that the information system enforces for the use of human review; and* 2. *the information system enforces the use of human review for the organization-defined security policy filters, when the system is not capable of making an information flow control decision.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for making information flow control decisions when the information system is not capable of doing so]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-16, CM-6, SC-7, SC-16  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(9).1.1.1** | **Examine** access control policy, procedures addressing information flow enforcement, security plan, information system design documentation, or other relevant documents; [*reviewing*] for security policy filters that the system enforces for the use of human review. |
|  |  |
| **AC-4(9).1.2.1** | **Examine** access control policy, procedures addressing information flow enforcement, 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 enforce the use of human review for the security policy filters identified in AC-4(9).1.1.1, when the system is not capable of making an information flow control decision. |
| **AC-4(9).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(9).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(9).1.2.1. |
| **AC-4(9).1.2.3** | **Examine** an agreed-upon [*basic*] sample of security policy filter reviews; [*reviewing*] for evidence that the measures identified in AC-4(9).1.2.1 are being applied. |
| **AC-4(9).1.2.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for reviewing security policy filters; conducting [*basic*] discussions for further evidence that the measures identified in AC-4(9).1.2.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 10** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-4(10)** | INFORMATION FLOW ENFORCEMENT |
| **AC-4(10).1**  **AC-4(10).1.1**  **AC-4(10).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the security policy filters that privileged administrators have the capability to enable/disable; and* 2. *the information system provides the capability for a privileged administrator to enable/disable organization-defined security policy filters.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for enabling/disabling security policy filters].  **Test**: [*select from:* Automated mechanisms implementing information flow enforcement policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-6, AC-16, CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(10).1.1.1** | **Examine** access control policy, procedures addressing information flow enforcement, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the security policy filters that privileged administrators have the capability to enable/disable. |
|  |  |
| **AC-4(10).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 provide the capability for privileged administrators to enable/disable the security policy filters identified in AC-4(10).1.1.1. |
| **AC-4(10).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(10).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(10).1.2.1. |
| **AC-4(10).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(10).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 11** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-4(11)** | INFORMATION FLOW ENFORCEMENT |
| **AC-4(11).1**  **AC-4(11).1.1**  **AC-4(11).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the security policy filters that privileged administrators have the capability to configure; and* 2. *the information system provides the capability for a privileged administrator to configure organization-defined security policy filters to support different security policies.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for configuring security policy filters].  **Test**: [*select from:* Automated mechanisms implementing information flow enforcement policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-6, AC-16, CM-6, SC-16  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(11).1.1.1** | **Examine** access control policy, procedures addressing information flow enforcement, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the security policy filters that privileged administrators have the capability to configure. |
|  |  |
| **AC-4(11).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 provide the capability for privileged administrators to configure the security policy filters identified in AC-4(11).1.1.1 to support different security policies. |
| **AC-4(11).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(11).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(11).1.2.1. |
| **AC-4(11).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(11).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 12** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-4(12)** | INFORMATION FLOW ENFORCEMENT |
| **AC-4(12).1**  **AC-4(12).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system, when transferring information between different security domains, identifies information flows by data type specification and usage.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information flow enforcement policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, CM-6, SC-7, SC-31, SC-32  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(12).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 identify information flows by data type specification and usage, when transferring information between different security domains. |
| **AC-4(12).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(12).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(12).1.1.1. |
| **AC-4(12).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(12).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 13** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-4(13)** | INFORMATION FLOW ENFORCEMENT |
| **AC-4(13).1**  **AC-4(13).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system, when transferring information between different security domains, decomposes information into policy-relevant subcomponents for submission to policy enforcement mechanisms.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information flow enforcement policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, CM-6, SC-7, SC-31, SC-32  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(13).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 decompose information into policy-relevant subcomponents for submission to policy enforcement mechanisms, when transferring information between different security domains. |
| **AC-4(13).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(13).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(13).1.1.1. |
| **AC-4(13).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(13).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 14** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-4(14)** | INFORMATION FLOW ENFORCEMENT |
| **AC-4(14).1**  **AC-4(14).1.1**  **AC-4(14).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the security policy requirements for constraining data structure and content; and* 2. *the information system, when transferring information between different security domains, implements policy filters that constrain data structure and content in accordance with organization-defined information security policy requirements.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; list of policy filters; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information flow enforcement policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, CM-6, SC-7, SC-31, SC-32  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(14).1.1.1** | **Examine** access control policy, procedures addressing information flow enforcement, security plan, or other relevant documents; [*reviewing*] for the security policy requirements for constraining data structure and content. |
|  |  |
| **AC-4(14).1.2.1** | **Examine** security plan, information system design documentation, other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to implement policy filters that constrain data structure and content in accordance with the requirements identified in AC-4(14).1.1.1, when transferring information between different security domains. |
| **AC-4(14).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(14).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(14).1.2.1. |
| **AC-4(14).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(14).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 15** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-4(15)** | INFORMATION FLOW ENFORCEMENT |
| **AC-4(15).1**  **AC-4(15).1.1**  **AC-4(15).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the information system, when transferring information between different security domains, detects unsanctioned information; and* 2. *the information system prohibits the transfer of unsanctioned information in accordance with the security policy.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information flow enforcement policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, CM-6, SC-7, SC-31, SC-32  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(15).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 detect unsanctioned information when transferring information between different security domains. |
| **AC-4(15).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(15).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(15).1.1.1. |
| **AC-4(15).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(15).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **AC-4(15).1.2.1** | **Examine** access control policy, procedures addressing information flow enforcement, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to prohibit the transfer of unsanctioned information in accordance with the security policy. |
| **AC-4(15).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of automated mechanisms identified in AC-4(15).1.2.1; [*reviewing*] for evidence that these automated mechanisms are configured as identified in AC-4(15).1.2.1. |
| **AC-4(15).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(15).1.2.1; conducting [*basic*] testing for evidence that these automated mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 16** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-4(16)** | INFORMATION FLOW ENFORCEMENT |
| **AC-4(16).1**  **AC-4(16).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system enforces security policies regarding information on interconnected systems.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information flow enforcement policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CA-3  concurrent controls: AC-16, CM-6, SC-7, SC-16  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(16).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 enforce security policies regarding information on interconnected systems. |
| **AC-4(16).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(16).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(16).1.1.1. |
| **AC-4(16).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(16).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 17** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-4(17)** | INFORMATION FLOW ENFORCEMENT |
| **AC-4(17).1**  **AC-4(17).1.1**  **AC-4(17).1.2**  **AC-4(17).1.3**  **AC-4(17).1.4**  **AC-4(17).1.5**  **AC-4(17).1.6**  **AC-4(17).1.7** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the information system uniquely identifies source domains for information transfer;* 2. *the information system uniquely authenticates source domains for information transfer;* 3. *the information system uniquely identifies destination domains for information transfer;* 4. *the information system uniquely authenticates destination domains for information transfer;* 5. *the information system binds security attributes to information to facilitate information flow policy enforcement;* 6. *the information system tracks problems associated with the security attribute binding; and* 7. *the information system tracks problems associated with the information transfer.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information flow enforcement; procedures addressing source and destination domain identification and authentication, and information transfer error handling; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information flow enforcement policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-16, AU-2, AU-3, AU-12, CM-6, IR-5, SC-7, SC-20, SC-21  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-4(17).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 uniquely identify source domains for information transfer. |
| **AC-4(17).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(17).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(17).1.1.1. |
| **AC-4(17).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(17).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **AC-4(17).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 uniquely authenticate source domains for information transfer. |
| **AC-4(17).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(17).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(17).1.2.1. |
| **AC-4(17).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(17).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **AC-4(17).1.3.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to uniquely identify destination domains for information transfer. |
| **AC-4(17).1.3.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(17).1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(17).1.3.1. |
| **AC-4(17).1.3.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(17).1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **AC-4(17).1.4.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to uniquely authenticate destination domains for information transfer. |
| **AC-4(17).1.4.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(17).1.4.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(17).1.4.1. |
| **AC-4(17).1.4.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(17).1.4.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **AC-4(17).1.5.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to bind security attributes to information to facilitate information flow policy enforcement. |
| **AC-4(17).1.5.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of automated mechanisms identified in AC-4(17).1.5.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(17).1.5.1. |
| **AC-4(17).1.5.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(17).1.5.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **AC-4(17).1.6.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to track problems associated with the security attribute binding. |
| **AC-4(17).1.6.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of automated mechanisms identified in AC-4(17).1.6.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(17).1.6.1. |
| **AC-4(17).1.6.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(17).1.6.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **AC-4(17).1.7.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to track problems associated with the information transfer. |
| **AC-4(17).1.7.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in AC-4(17).1.7.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-4(17).1.7.1. |
| **AC-4(17).1.7.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-4(17).1.7.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |