| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AC-16** | SECURITY ATTRIBUTES | |
| **AC-16.1**  **AC-16.1.1**  **AC-16.1.1a**  **AC-16.1.1b**  **AC-16.1.1c**  **AC-16.1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the security attributes the information system binds to information:*    * *in storage;*    * *in process; and*    * *in transmission; and* 2. *the information system supports and maintains the binding of the organization-defined security attributes to information in storage, in process, and in transmission.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing the binding of security attributes to information in storage, in process, and in transmission; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms supporting and maintaining the binding of security attributes to information in storage, in process, and in transmission]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, MP-3, SC-16  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-16.1.1.1**  **AC-16.1.1.1.a**  **AC-16.1.1.1.b**  **AC-16.1.1.1.c** | | **Examine** access control policy, procedures addressing the binding of security attributes to information in storage, in process, and in transmission, security plan, or other relevant documents; [*reviewing*] for the security attributes the information system binds to information:   * + in storage,   + in process, and;   + in transmission |
|  | |  |
| **AC-16.1.2.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to support and maintain the binding of the security attributes identified in AC-16.1.1.1 to information in storage, in process, and in transmission. |
| **AC-16.1.2.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-16.1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-16.1.2.1. |
| **AC-16.1.2.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-16.1.2.1; 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-16(1)** | | SECURITY ATTRIBUTES |
| **AC-16(1).1**  **AC-16(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the information system dynamically reconfigures security attributes in accordance with an identified security policy as information is created and combined.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing the dynamic reconfiguration of security attributes; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing the dynamic reconfiguration of security attributes to information]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: none  concurrent controls: CM-6, SC-16  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **AC-16(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 dynamically reconfigure security attributes in accordance with an identified security policy as information is created and combined. |
| **AC-16(1).1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-16(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-16(1).1.1.1. |
| **AC-16(1).1.1.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-16(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-16(2)** | SECURITY ATTRIBUTES |
| **AC-16(2).1**  **AC-16(2).1.1**  **AC-16(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization identifies the entities authorized to change security attributes; and* 2. *the information system allows authorized entities to change security attributes.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing the change of security attributes; information system design documentation; information system configuration settings and associated documentation; list of entities authorized to change security attributes; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for changing security attributes].  **Test**: [*select from:* Automated mechanisms allowing the change of security attributes]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-16  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-16(2).1.1.1** | **Examine** access control policy, procedures addressing the change of security attributes, security plan, or other relevant documents; [*reviewing*] for the entities authorized to change security attributes. |
|  |  |
| **AC-16(2).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 allow the authorized entities identified in AC-16(2).1.1.1 to change security attributes. |
| **AC-16(2).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-16(2).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-16(2).1.2.1. |
| **AC-16(2).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-16(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)** | |
| **AC-16(3)** | SECURITY ATTRIBUTES |
| **AC-16(3).1**  **AC-16(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system maintains the binding of security attributes to information with sufficient assurance that the information-attribute association can be used as the basis for automated policy actions.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing the binding of security attributes to information; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms maintaining the binding of security attributes to information]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-16  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-16(3).1.1.1** | **Examine** security plan, security design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to maintain the binding of security attributes to information with sufficient assurance that the information-attribute association can be used as the basis for automated policy actions. |
| **AC-16(3).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-16(3).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-16(3).1.1.1. |
| **AC-16(3).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-16(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)** | |
| **AC-16(4)** | SECURITY ATTRIBUTES |
| **AC-16(4).1**  **AC-16(4).1.1**  **AC-16(4).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization identifies users authorized to associate security attributes with information; and* 2. *the information system allows authorized users to associate security attributes with information.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing the association of security attributes to information; information system design documentation; information system configuration settings and associated documentation; list of users authorized to associate security attributes with information; information system audit records; other relevant documents or records].  **Interview:** [*select from:* Organizational personnel with responsibilities for associating security attributes with information].  **Test**: [*select from:* Automated mechanisms allowing users to associate security attributes with information]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-16  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-16(4).1.1.1** | **Examine** access control policy, procedures addressing the association of security attributes to information, security plan, or other relevant documents; [*reviewing*] for the users authorized to associate security attributes with information. |
|  |  |
| **AC-16(4).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 allow the authorized users identified in AC-16(4).1.1.1 to associate security attributes with information. |
| **AC-16(4).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-16(4).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-16(4).1.2.1. |
| **AC-16(4).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-16(4).1.2.1; 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-16(5)** | SECURITY ATTRIBUTES |
| **AC-16(5).1**  **AC-16(5).1.1**  **AC-16(5).1.2**  **AC-16(5).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the set of special dissemination, handling, or distribution instructions to be used for each object output from the information system;* 2. *the organization defines standard naming conventions for the security attributes to be displayed in human-readable form on each object output from the system to system output devices; and* 3. *the information system displays security attributes in human-readable form on each object output from the system to system output devices to identify the organization-defined set of special dissemination, handling, or distribution instructions using organization-defined human readable, standard naming conventions.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing display of security attributes in human-readable form; special instructions for the dissemination, handling, or distribution of object output from the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* System output devices displaying security attributes in human-readable form on each object]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: none  concurrent controls: CM-6, SC-16  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-16(5).1.1.1** | **Examine** access control policy, procedures addressing display of security attributes in human-readable form, security plan, or other relevant documents; [*reviewing*] for the set of special dissemination, handling, or distribution instructions to be used for each object output from the information system. |
|  |  |
| **AC-16(5).1.2.1** | **Examine** access control policy, procedures addressing display of security attributes in human-readable form, security plan, or other relevant documents; [*reviewing*] for the human-readable, standard naming conventions for the security attributes to be displayed on each object output from the system to system output devices. |
|  |  |
| **AC-16(5).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 display security attributes in human-readable form on each object output from the system to system output devices to identify the special dissemination, handling, or distribution instructions identified in AC-16(5).1.1.1, using the human readable, standard naming conventions identified in AC-16(5).1.2.1. |
| **AC-16(5).1.3.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-16(5).1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-16(5).1.3.1. |
| **AC-16(5).1.3.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-16(5).1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |