| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **CA-3** | INFORMATION SYSTEM CONNECTIONS | |
| **CA-3.1**  **CA-3.1.1**  **CA-3.1.2**  **CA-3.1.3**  **CA-3.1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization identifies connections to external information systems (i.e., information systems outside of the authorization boundary);* 2. *the organization authorizes connections from the information system to external information systems through the use of Interconnection Security Agreements;* 3. *the organization documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and* 4. *the organization monitors the information system connections on an ongoing basis to verify enforcement of security requirements.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection security agreements; security plan; information system design documentation; security assessment report; plan of action and milestones; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibility for developing, implementing, or approving information system interconnection agreements]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: SC-7  concurrent controls: AC-4, CA-7, SA-9  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. |
| **CA-3.1.1.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for evidence that connections to external information systems (i.e., outside the authorization boundary) are identified. |
|  | |  |
| **CA-3.1.1.2** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for developing, implementing, or approving information system interconnection agreements; conducting [*basic*] discussions for evidence that connections to external information systems have been identified. |
|  | |  |
| **CA-3.1.2.1** | | **Examine** information system interconnection agreements for an agreed-upon [*basic*] sample of connections identified in CA-3.1.1.1; [*reviewing*] for evidence that the organization authorizes all identified connections from the information system to external information systems through the use of interconnection security agreements. |
|  | |  |
| **CA-3.1.3.1** | | **Examine** information system interconnection agreements for an agreed-upon [*basic*] sample of connections identified in CA-3.1.1.1; [*reviewing*] for evidence that the interface characteristics, security requirements, and nature of the information communicated is documented for each connection. |
|  | |  |
| **CA-3.1.4.1** | | **Examine** procedures addressing information system connections, system and communications protection policy, an agreed-upon [*basic*] sample of information system interconnection security agreements, or other relevant documents; [*reviewing*] for the measures to be employed to monitor information system connections on an ongoing basis to verify enforcement of security requirements. |
| **CA-3.1.4.2** | | **Examine** information system monitoring records for an agreed-upon [*basic*] sample of connections identified in CA-3.1.1.1; [*reviewing*] for evidence that the measures identified in CA-3.1.4.1 are being applied to monitor information system connections on an ongoing basis. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **CA-3(1)** | | INFORMATION SYSTEM CONNECTIONS |
| **CA-3(1).1**  **CA-3(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the organization prohibits the direct connection of an unclassified, national security system to an external network.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection security agreements; security plan; information system design documentation; security assessment report; plan of action and milestones; other relevant documents or records]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: SC-7  concurrent controls: AC-4, CA-7, CM-6, SA-9  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **CA-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 prohibit the direct connection of an unclassified, national security system to an external network. |
| **CA-3(1).1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*]sample of automated mechanisms identified in CA-3(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CA-3(1).1.1.1. |
| **CA-3(1).1.1.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in CA-3(1).1.1.1; conducting [*basic*] testing for evidence that the automated mechanisms are operating as intended. |
|  | | |
| **ASSESSMENT – Control Enhancement 2** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **CA-3(2)** | | INFORMATION SYSTEM CONNECTIONS |
| **CA-3(2).1**  **CA-3(2).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the organization prohibits the direct connection of a classified, national security system to an external network.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection agreements; security plan; information system design documentation;; security assessment report; plan of action and milestones; other relevant documents or records]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: SC-7  concurrent controls: AC-4, CA-7, CM-6, SA-9  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **CA-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 prohibit the direct connection of a classified, national security system to an external network. |
| **CA-3(2).1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of automated mechanisms identified in CA-3(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CA-3(2).1.1.1. |
| **CA-3(2).1.1.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in CA-3(2).1.1.1; conducting [*basic*] testing for evidence that the automated mechanisms are operating as intended. |