| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 2 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **CA-2** | SECURITY ASSESSMENTS | |
| **CA-2.1**  **CA-2.1.1**  **CA-2.1.2**  **CA-2.1.2a**  **CA-2.1.2b**  **CA-2.1.2c** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization develops a security assessment plan for the information system; and* 2. *the security assessment plan describes the scope of the assessment including:*    * *security controls and control enhancements under assessment;*    * *assessment procedures to be used to determine security control effectiveness; and*    * *assessment environment, assessment team, and assessment roles and responsibilities.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security assessment and authorization policy; procedures addressing security assessments; security assessment plan; other relevant documents or records]. | |
| **Additional Assessment Case Information** | | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CA-6, CA-7, CM-4, PM-10, RA-3, RA-5, SA-11, SI-2  successor controls: CA-5, PM-4 | |
| **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-2.1.1.1** | **Examine** information system documentation; [*reviewing*] for a security assessment plan for the information system. | |
| **CA-2.1.2.1**  **CA-2.1.2.1.a**  **CA-2.1.2.1.b**  **CA-2.1.2.1.c** | **Examine** the security assessment plan; [*reviewing*] for a description of the scope of the assessment including:  -security controls and control enhancements under assessment;  -assessment procedures to be used to determine security control effectiveness; and  -assessment environment, assessment team, and assessment roles and responsibilities. | |
| ASSESSMENT – Base Control, Part 2 of 2 | | |
| **CA-2.2**  **CA-2.2.1**  **CA-2.2.2**  **CA-2.2.3**  **CA-2.2.4** | | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the frequency of assessing the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;* 2. *the organization assesses the security controls in the information system at the organization-defined frequency;* 3. *the organization produces a security assessment report that documents the results of the security control assessment; and* 4. *the results of the security control assessment are provided, in writing, to the authorizing official or authorizing official designated representative.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security assessment and authorization policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; security assessment evidence; plan of action and milestones; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with security assessment responsibilities]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CA-6, CA-7, CM-4, PM-10, RA-3, RA-5, SA-11, SI-2  successor controls: CA-5, PM-4 |
| **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\*\*** |
| **CA-2.2.1.1** | | **Examine** security assessment and authorization policy, procedures addressing security assessments, security plan, or other relevant documents; [*reviewing*] for the frequency of assessing the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. |
| **CA-2.2.2.1** | | **Examine** an agreed-upon [*basic*] sample of security assessment reports; [*reviewing*] for evidence that security controls in the information system are assessed in accordance with the frequency identified in CA-2.2.1.1. |
| **CA-2.2.3.1** | | **Examine** an agreed-upon [*basic*] sample of security assessment reports; [*reviewing*] for evidence that the results of the security control assessments are documented. |
| **CA-2.2.4.1** | | **Examine** an agreed-upon [*basic*] sample ofsecurity assessment reports; [*reviewing*] for evidence that the results of the security control assessments are to be provided, in writing, to the authorizing official or authorizing official designated representative. |
| **CA-2.2.4.2** | | **Interview** authorizing official and authorizing official designated representative for the information system; conducting [*basic*] discussions for further evidence that the results of security control assessments are provided in writing. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **CA-2(1)** | | SECURITY ASSESSMENTS |
| **CA-2(1).1**  **CA-2(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security assessment and authorization policy; procedures addressing security assessments; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with security assessment responsibilities]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CA-6, CA-7, CM-4, PM-10, RA-3, RA-5, SA-11, SI-2  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **CA-2(1).1.1.1** | | **Examine** security assessment and authorization policy, security assessment plan, security plan, or other relevant documents; [*reviewing*] for authorizing official determination and/or approval of the independence criteria for the assessor or assessment team that assesses the security controls in the information system. |
| **CA-2(1).1.2.2** | | **Examine** an agreed-upon [*basic*] sample of security assessment reports or other relevant documents; [*reviewing*] for evidence that the assessors meet the criteria for independence as documented in CA-2(1).1.1. 1. |
|  | | |
| **ASSESSMENT – Control Enhancement 2** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **CA-2(2)** | | SECURITY ASSESSMENTS |
| **CA-2(2).1**  **CA-2(2).1.1**  **CA-2(2).1.1a**  **CA-2(2).1.1b**  **CA-2(2).1.1c**  **CA-2(2).1.2** | | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines:*    * *the forms of security testing to be included in security control assessments, selecting from in-depth monitoring, malicious user testing, penetration testing, red team exercises, or an organization-defined form of security testing;*    * *the frequency for conducting each form of security testing;*    * *whether the security testing will be announced or unannounced; and* 2. *the organization conducts security control assessments using organization-defined forms of testing in accordance with organization-defined frequency and assessment techniques established for each form of testing.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security assessment and authorization policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; assessment evidence; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with security assessment responsibilities]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CA-6, CA-7, CM-4, PM-10, RA-3, RA-5, SA-11, SI-2  successor controls: CA-5, PM-4 |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **CA-2(2).1.1.1**  **CA-2(2).1.1.1.a   CA-2(2).1.1.1.b**  **CA-2(2).1.1.1.c** | | **Examine** security assessment and authorization policy, procedures addressing security assessments, security plan, or other relevant documents; [*reviewing*] for:   * + the forms of security testing to be included in security control assessments, selecting from in-depth monitoring, malicious user testing, penetration testing, red team exercises, or an organization-defined form of security testing;   + the frequency for conducting each form of security testing; and   + whether the security testing will be announced or unannounced; |
|  | |  |
| **CA-2(2).1.2.1** | | **Examine** an agreed-upon [*basic*] sample of security assessment reports; [*reviewing*] for evidence that security control assessments are conducted in accordance with the frequency identified in CA-2(2).1.1.1.b and assessment techniques established for each form of testing identified in CA-2(2).1.1.1.a. |