| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **CA-7** | CONTINUOUS MONITORING | |
| **CA-7.1**  **CA-7.1.1**  **CA-7.1.2**  **CA-7.1.3**  **CA-7.1.4**  **CA-7.1.4a**  **CA-7.1.4b**  **CA-7.1.4c**  **CA-7.1.4d** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization establishes a continuous monitoring strategy and program;* 2. *the organization defines the frequency for reporting the security state of the information system to appropriate organizational officials;* 3. *the organization defines organizational officials to whom the security state of the information system should be reported; and* 4. *the organization implements a continuous monitoring program that includes:*    * *a configuration management process for the information system and its constituent components;*    * *a determination of the security impact of changes to the information system and environment of operation;*    * *ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and*    * *reporting the security state of the information system to appropriate organizational officials in accordance with organization-defined frequency.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing configuration management; security plan; security assessment report; plan of action and milestones; information system monitoring records; configuration management records, security impact analyses; status reports; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with continuous monitoring responsibilities; organizational personnel with configuration management responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PM-9  concurrent controls: CA-2, CA-3, CA-6, CM-3, 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-7.1.1.1** | **Examine** security assessment and authorization policy, procedures addressing continuous monitoring of security controls, organizational risk management strategy documentation, security plan, or other relevant documents; [*reviewing*] for the establishment of a continuous monitoring strategy and program. |
|  |  |
| **CA-7.1.2.1** | **Examine** security assessment and authorization policy, procedures addressing continuous monitoring of security controls, security plan, or other relevant documents; [*reviewing*] for the frequency for reporting the security state of the information system to appropriate organizational officials as defined in CA-7.1.3.1. |
|  |  |
| **CA-7.1.3.1** | **Examine** security assessment and authorization policy, procedures addressing continuous monitoring of security controls, security plan, or other relevant documents; [*reviewing*] for the officials to whom the security state of the information system should be reported. |
|  |  |
| **CA-7.1.4.1**  **CA-7.1.4.1.a**  **CA-7.1.4.1.b**  **CA-7.1.4.1.c**  **CA-7.1.4.1.d** | **Examine** security assessment and authorization policy, procedures addressing continuous monitoring of security controls, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to implement a continuous monitoring program that includes:   * a configuration management process for the information system and its constituent components; * a determination of the security impact of changes to the information system and environment of operation; * ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and * reporting the security state of the information system to appropriate organizational official in accordance with organization-defined frequency. |
| **CA-7.1.4.2** | **Examine** an agreed-upon [*basic*] sample of configuration management records; [*reviewing*] for evidence that the measures identified in CA-7.1.4.1.a are being applied to include a configuration management process for the information system and its constituent components. |
| **CA-7.1.4.3** | **Examine** an agreed-upon [*basic*] sample of security impact analyses; [*reviewing*] for evidence that the measures identified in CA-7.1.4.1.b are being applied to include a determination of the security impact of changes to the information system and environment of operation. |
| **CA-7.1.4.4** | **Examine** an agreed-upon [*basic*] sample of security assessment reports or other relevant documents; [*reviewing*] for evidence that the measures identified in CA-7.1.4.1.c are being applied to include ongoing security control assessments in accordance with the organizational continuous monitoring strategy. |
| **CA-7.1.4.5** | **Examine** an agreed-upon [*basic*] sample of continuous monitoring status reports or other relevant documents provided to officials identified in CA-7.1.3.1; [*reviewing*] for evidence that the measures identified in CA-7.1.4.1.d are being applied to include reporting the security state of the information system to appropriate organizational officials in accordance with the frequency identified in CA-7.1.2.1. |
|  | |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CA-7(1)** | CONTINUOUS MONITORING |
| **CA-7(1).1**  **CA-7(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with continuous monitoring responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CA-2, CA-3, CA-6, CM-4, PM-10, RA-3, RA-5, SA-11, SI-2  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CA-7(1).1.1.1** | **Examine** security assessment and authorization policy, security assessment plan, continuous monitoring plan, security plan, or other relevant documents; [*reviewing*] for the authorizing official determination and/or approval of the independence criteria for the assessor or assessment team that monitors the security controls on an ongoing basis. |
| **CA-7(1).1.1.2** | **Examine** an agreed-upon [*basic*] sample of security assessment reports, continuous monitoring assessment reports, or other relevant documents; [*reviewing*] for evidence that the assessors meet the criteria for independence as documented in CA-7(1).1.1.1. |
| **CA-7(1).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with continuous monitoring responsibilities; conducting [*basic*] discussions for further evidence that the organization employs an independent assessor or assessment team to conduct the security control assessments for continuous monitoring. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CA-7(2)** | CONTINUOUS MONITORING |
| **CA-7(2).1**  **CA-7(2).1.1**  **CA-7(2).1.1a**  **CA-7(2).1.1b**  **CA-7(2).1.1c**  **CA-7(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines:*    * *the forms of security testing to be included in planning, scheduling, and security control assessments selecting from in-depth monitoring, malicious user testing, penetration testing, red team exercises, or an organization-defined form of security testing to ensure compliance with all vulnerability mitigation procedures;*    * *the frequency for conducting each form of security testing;*    * *whether the security testing will be announced or unannounced; and* 2. *the organization plans, schedules, and conducts assessments using organization-defined forms of security testing in accordance with the organization-defined frequency and assessment techniques established for each form of testing to ensure compliance with all vulnerability mitigation procedures.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing vulnerability mitigation; security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with continuous monitoring responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CA-2, , CA-6, 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-7(2).1.1.1**  **CA-7(2).1.1.1.a**  **CA-7(2).1.1.1.b**  **CA-7(2).1.1.1.c** | **Examine** security assessment and authorization policy, procedures addressing continuous monitoring of security controls, security plan, or other relevant documents; [*reviewing*] for:   * + the forms of security testing to be included in planning, scheduling, and security control assessments selecting from in-depth monitoring, malicious user testing, penetration testing, red team exercises, or an organization-defined form of security testing to ensure compliance with all vulnerability mitigation procedures;   + the frequency for conducting each form of security testing;   + whether the security testing will be announced or unannounced; |
| **CA-7(2).1.2.1** | **Examine** an agreed-upon [*basic*] sample of security assessment reports, continuous monitoring assessment reports, or other relevant documents; [*reviewing*] for evidence that assessments are planned, scheduled, and conducted in accordance with the frequency identified in CA-7(2).1.1.1.b and assessment techniques established for each form of testing identified in CA-7(2).1.1.1.a. |