| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **CM-3** | CONFIGURATION CHANGE CONTROL | |
| **CM-3.1**  **CM-3.1.1**  **CM-3.1.2**  **CM-3.1.3**  **CM-3.1.4**  **CM-3.1.5**  **CM-3.1.6**  **CM-3.1.6a**  **CM-3.1.6b**  **CM-3.1.6c**  **CM-3.1.7** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization determines the types of changes to the information system that are configuration controlled;* 2. *the organization approves configuration-controlled changes to the system with explicit consideration for security impact analyses;* 3. *the organization documents approved configuration-controlled changes to the system;* 4. *the organization retains and reviews records of configuration-controlled changes to the system;* 5. *the organization audits activities associated with configuration-controlled changes to the system;* 6. *the organization defines:*    * *the configuration change control element (e.g., committee, board) responsible for coordinating and providing oversight for configuration change control activities;*    * *the frequency with which the configuration change control element convenes; and/or;*    * *configuration change conditions that prompt the configuration change control element to convene.* 7. *the organization coordinates and provides oversight for configuration change control activities through the organization-defined configuration change control element that convenes at the organization-defined frequency and/or for any organization-defined configuration change conditions.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system architecture and configuration documentation; security plan; change control records; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with configuration change control responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: CM-4, CM-5, CM-6, SA-10, SI-2  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. |
| **CM-3.1.1.1** | **Examine** configuration management policy, procedures addressing information system configuration change control, configuration management plan, or other relevant documents; [*reviewing*] for the types of changes to the information system that are to be configuration controlled. |
|  |  |
| **CM-3.1.2.1** | **Examine** configuration management policy, procedures addressing information system configuration change control, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to approve configuration-controlled changes to the system with explicit consideration for security impact analyses. |
| **CM-3.1.2.2** | **Examine** change control records foran agreed-upon [*basic*] sample of changes identified in the change audit summary report or other relevant documents for the information system; [*reviewing*] for evidence that the measures identified in CM-3.1.2.1 are being applied. |
| **CM-3.1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for security impact analysis and approval of proposed changes to the information system; conducting [*basic*] discussions for further evidence that the measures identified in CM-3.1.2.1 are being applied. |
|  |  |
| **CM-3.1.3.1** | **Examine** configuration management policy, procedures addressing information system configuration change control, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to document approved configuration-controlled changes to the system. |
| **CM-3.1.3.2** | **Examine** change control records foran agreed-upon [*basic*] sample of configuration-controlled changes identified in the change audit summary report or other relevant documents for the information system; [*reviewing*] for evidence that the measures identified in CM-3.1.3.1 are being applied. |
|  |  |
| **CM-3.1.4.1** | **Examine** configuration management policy, procedures addressing information system configuration change control, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to retain and review records of configuration-controlled changes to the system. |
| **CM-3.1.4.2** | **Examine** change control records foran agreed-upon [*basic*] sample of configuration-controlled changes to the information system; [*reviewing*] for evidence that the measures identified in CM-3.1.4.1 are being applied. |
| **CM-3.1.4.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for retaining and reviewing records of configuration-controlled changes to the information system; conducting [*basic*] discussions for further evidence that the measures identified in CM-3.1.4.1 are being applied. |
|  |  |
| **CM-3.1.5.1** | **Examine** configuration management policy, procedures addressing information system configuration change control, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to audit activities associated with configuration-controlled changes to the system. |
| **CM-3.1.5.2** | **Examine** an agreed-upon [*basic*] sample of audit records associated with configuration-controlled changes to the information system; [*reviewing*] for evidence that the measures identified in CM-3.1.5.1 are being applied. |
| **CM-3.1.5.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for auditing activities associated with configuration-controlled changes to the information system; conducting [*basic*] discussions for further evidence that the measures identified in CM-3.1.5.1 are being applied. |
|  |  |
| **CM-3.1.6.1**  **CM-3.1.6.1.a**  **CM-3.1.6.1.b**  **CM-3.1.6.1.c** | **Examine** configuration management policy, procedures addressing information system configuration change control, configuration management plan, or other relevant documents; [*reviewing*] for:   * + the configuration change control element (e.g., committee, board) responsible for coordinating and providing oversight for configuration change control activities;   + the frequency with which the configuration change control element convenes; and/or;   + configuration change conditions that prompt the configuration change control element to convene. |
|  |  |
| **CM-3.1.7.1** | **Examine** configuration management policy, procedures addressing information system configuration change control, configuration change control board charter, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to coordinate and provide oversight for configuration control activities through the configuration change control element identified in CM-3.1.6.1.a that convenes at the frequency identified in CM-3.1.6.1.b and/or for any conditions identified in CM-3.1.6.1.c. |
| **CM-3.1.7.2** | **Examine** an agreed-upon [*basic*] sample of change control records, change control board meeting minutes, information system audit records, or other relevant documents; [*reviewing*] for evidence that the measures identified in CM-3.1.7.1 are being applied. |
| **CM-3.1.7.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for coordinating and providing oversight for configuration change control activities; conducting [*basic*] discussions for further evidence that the measures identified in CM-3.1.7.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CM-3(1)** | CONFIGURATION CHANGE CONTROL |
| **CM-3(1).1**  **CM-3(1).1.1**  **CM-3(1).1.2**  **CM-3(1).1.2a**  **CM-3(1).1.2b**  **CM-3(1).1.2c**  **CM3(1).1.2d**  **CM-3(1).1.2e** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the time period after which approvals that have not been received for proposed changes to the information system are highlighted; and* 2. *the organization employs automated mechanisms to:*  * *document proposed changes to the information system;* * *notify designated approval authorities;* * *highlight approvals that have not been received by the organization-defined time period;* * *inhibit change until designated approvals are received; and* * *document completed changes to the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; automated configuration control mechanisms; change control records; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing configuration change control]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: CM-4, CM-5, CM-6, SA-10, SI-2  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-3(1).1.1.1** | **Examine** configuration management policy, procedures addressing information system configuration change control, configuration management plan, or other relevant documents; [*reviewing*] for the time period after which approvals that have not been received for proposed changes to the information system are highlighted. |
|  |  |
| **CM-3(1).1.2.1**  **CM-3(1).1.2.1.a**  **CM-3(1).1.2.1.b**  **CM-3(1).1.2.1.c**  **CM-3(1).1.2.1.d**  **CM-3(1).1.2.1.e** | **Examine** configuration management plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to:   * document proposed changes to the information system; * notify designated approval authorities; * highlight approvals that have not been received by the time period identified in CM-3(1).1.1.1; * inhibit change until designated approvals are received; and * document completed changes to the information system. |
| **CM-3(1).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in CM-3(1).1.2.1; [*reviewing*] for evidence that these mechanisms are configured to document proposed changes to the information system as identified in CM-3(1).1.2.1.a. |
| **CM-3(1).1.2.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in CM-3(1).1.2.1; [*reviewing*] for evidence that these mechanisms are configured to notify designated approval authorities as identified in CM-3(1).1.2.1.b. |
| **CM-3(1).1.2.4** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in CM-3(1).1.2.1; [*reviewing*] for evidence that these mechanisms are configured to highlight approvals that have not been received by the time period identified in CM-3(1).1.2.1.c. |
| **CM-3(1).1.2.5** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in CM-3(1).1.2.1; [*reviewing*] for evidence that these mechanisms are configured to inhibit change until designated approvals are received as identified in CM-3(1).1.2.1.d. |
| **CM-3(1).1.2.6** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in CM-3(1).1.2.1; [*reviewing*] for evidence that these mechanisms are configured to document completed changes to the information system as identified in CM-3(1).1.2.1.e. |
| **CM-3(1).1.2.7** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in CM-3(1).1.2.1; 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)** | |
| **CM-3(2)** | CONFIGURATION CHANGE CONTROL |
| **CM-3(2).1**  **CM-3(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with configuration change control responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: CM-4, CM-5, CM-6, SA-10, SI-2  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-3(2).1.1.1** | **Examine** configuration management policy, procedures addressing information system configuration change control, configuration management plan, or other relevant documents; [*reviewing*] for measures to be employed to test, validate, and document changes to the information system before implementing the changes on the operational system. |
| **CM-3(2).1.1.2** | **Examine** change control records for an agreed-upon [*basic*] sample of changes identified in the change audit summary report or other relevant documents for the information system; [*reviewing*] for evidence that the measures identified in CM-3(2).1.1.1 are being applied. |
| **CM-3(2).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with configuration change control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in CM-3(2).1.1.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CM-3(3)** | CONFIGURATION CHANGE CONTROL |
| **CM-3(3).1**  **CM-3(3).1.1**  **CM-3(3).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization employs automated mechanisms to implement changes to the current information system baseline; and* 2. *the organization deploys the updated baseline across the installed base.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; automated configuration control mechanisms; change control records; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing changes to the information system baseline]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: CM-2, CM-4, CM-5, CM-6, SA-10, SI-2  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-3(3).1.1.1** | **Examine** configuration management plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to implement changes to the current information system baseline. |
| **CM-3(3).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of automated mechanisms identified in CM-3(3).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CM-3(3).1.1.1. |
| **CM-3(3).1.1.3** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in CM-3(3).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **CM-3(3).1.2.1** | **Examine** configuration management plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to deploy the updated baseline across the installed base. |
| **CM-3(3).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of automated mechanisms identified in CM-3(3).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CM-3(3).1.2.1. |
| **CM-3(3).1.2.3** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in CM-3(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)** | |
| **CM-3(4)** | CONFIGURATION CHANGE CONTROL |
| **CM-3(4).1**  **CM-3(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization requires an information security representative to be a member of the configuration change control element as defined by the organization in CM-3.1.6.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing information system configuration change control; security plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with configuration change control responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: None  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-3(4).1.1.1** | **Examine** configuration management policy, procedures addressing information system configuration change control, configuration management plan, or other relevant documents; [*reviewing*] for the requirement to have an information security representative to be a member of the configuration change control element as defined by the organization in CM-3.1.6. |