| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **CM-2** | BASELINE CONFIGURATION | |
| **CM-2.1**  **CM-2.1.1**  **CM-2.1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization develops and documents a baseline configuration of the information system and* 2. *the organization maintains, under configuration control, a current baseline configuration of the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; enterprise architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: CM-3, CM-4, CM-5, CM-6, CM-7, CM-8  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-2.1.1.1** | | **Examine** information system architecture and configuration documentation, information system design documentation, information system build documentation, or other relevant documents associated with an agreed-upon [*basic*] sample of information system components; [*reviewing*] for a current baseline configuration of the information system.  Note to assessor: Information system components defined in the configuration management plan for the information system should include the configuration items (hardware, software, firmware, and documentation) required to be configuration-managed. |
|  | |  |
| **CM-2.1.2.1** | | **Examine** configuration management policy, procedures addressing the baseline configuration of the information system, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to maintain, under configuration control, a current baseline configuration of the information system. |
| **CM-2.1.2.2** | | **Examine** change control records, configuration audit records, or other relevant documents associated with an agreed-upon [*basic*] sample of information system components; [*reviewing*] for evidence that the measures identified in CM-2.1.2.1 are being applied. |
| **CM-2.1.2.3** | | **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-2.1.2.1 are being applied. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **CM-2(1)** | | BASELINE CONFIGURATION |
| **CM-2(1).1**  **CM-2(1).1.1**  **CM-2(1).1.1a**  **CM-2(1).1.1b**  **CM-2(1).1.2**  **CM-2(1).1.2a**  **CM-2(1).1.2b**  **CM-2(1).1.2c** | | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines:*    * *the frequency of reviews and updates to the baseline configuration of the information system; and*    * *the circumstances that require reviews and updates to the baseline configuration of the information system; and* 2. *the organization reviews and updates the baseline configuration of the information system*    * *in accordance with the organization-defined frequency;*    * *when required due to organization-defined circumstances; and*    * *as an integral part of information system component installations and upgrades.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; 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-3, CM-4, CM-5, CM-6, CM-7, CM-8  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **CM-2(1).1.1.1**  **CM-2(1).1.1.1.a  CM-2(1).1.1.1.b** | | **Examine** configuration management policy, procedures addressing the baseline configuration of the information system, configuration management plan, or other relevant documents; [*reviewing*] for:   * + the frequency of reviews and updates to the baseline configuration of the information system; and   + the circumstances that require reviews and updates to the baseline configuration of the information system. |
|  | |  |
| **CM-2(1).1.2.1**  **CM-2(1).1.2.1.a**  **CM-2(1).1.2.1.b**  **CM-2(1).1.2.1.c** | | **Examine** configuration management policy, procedures addressing the baseline configuration of the information system, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to review and update the baseline configuration of the information system:   * + in accordance with the frequency identified in CM-2(1).1.1.1.a;   + when required due to circumstances identified in CM-2(1).1.1.1.b ; and   + as an integral part of information system component installations and upgrades. |
| **CM-2(1).1.2.2** | | **Examine** an agreed-upon [*basic*] sample of records of baseline configuration reviews and updates for the information system; [*reviewing*] for evidence that the baseline configuration is reviewed and updated in accordance with the frequency identified in CM-2(1).1.2.1.a. |
| **CM-2(1).1.2.3** | | **Examine** an agreed-upon [*basic*] sample of records of baseline configuration reviews and updates for the information system; [*reviewing*] for evidence that the baseline configuration is reviewed and updated due to circumstances identified in CM-2(1).1.2.1.b. |
| **CM-2(1).1.2.4** | | **Examine** an agreed-upon [*basic*] sample of records of baseline configuration reviews and updates associated with component installations or upgrades for the information system; [*reviewing*] for evidence that the measures identified in CM-2(1).1.2.1.c are being applied to review and update the baseline configuration as an integral part of information system component installations and upgrades. |
| **CM-2(1).1.2.5** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with configuration change control responsibilities; reviewing for further evidence that the measures identified in CM-2(1).1.2.1 are being applied to review and update the baseline configuration of the information system. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CM-2(2)** | BASELINE CONFIGURATION |
| **CM-2(2).1**  **CM-2(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization* *employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system design documentation; information system architecture and configuration documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing baseline configuration maintenance]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: CM-3, CM-4, CM-5, CM-6, CM-7, CM-8  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-2(2).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 maintain an up-to-date, complete, accurate, and readily available baseline configuration.  Note to assessor: The automated mechanisms provide the current approved baseline configuration and tracks deviations correctly until the next baseline is approved |
| **CM-2(2).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in CM-2(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CM-2(2).1.1.1. |
| **CM-2(2).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in CM-2(2).1.1.1; 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)** | |
| **CM-2(3)** | BASELINE CONFIGURATION |
| **CM-2(3).1**  **CM-2(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization retains older versions of baseline configurations as deemed necessary to support rollback.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; historical copies of baseline configurations; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: CM-3, CM-4, CM-5, CM-6, CM-7, CM-8  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-2(3).1.1.1** | **Examine** configuration management policy, procedures addressing the baseline configuration of the information system, configuration management plan, or other relevant documents; [*reviewing*] for retention requirements for older versions of baseline configurations to support rollback. |
| **CM-2(3).1.1.2** | **Examine** an agreed-upon [*basic*] sample ofhistorical copies of baseline configurations; [*reviewing*] for evidence that older versions of baseline configurations are retained in accordance with the requirements identified in CM-2(3).1.1.1. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CM-2(4)** | BASELINE CONFIGURATION |
| **CM-2(4).1**  **CM-2(4).1.1**  **CM-2(4).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization develops and maintains a list of software programs not authorized to execute on the information system; and* 2. *the organization employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; list of software programs not authorized to execute on the information system; information system architecture and configuration documentation; security plan; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, SA-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-2(4).1.1.1** | **Examine** configuration management policy, procedures addressing the baseline configuration of the information system, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to develop and maintain a list of software programs not authorized to execute on the information system. |
| **CM-2(4).1.1.2** | **Examine** list of software programs not authorized to execute on the information system; [*reviewing*] for evidence that the measures identified in CM-2(4).1.1.1 are being applied. |
| **CM-2(4).1.2.1** | **Examine** configuration management plan, information system design documentation, information system architecture and configuration documentation, information system build documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to enforce an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system. |
| **CM-2(4).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of automated mechanisms identified in CM-2(4).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CM-2(4).1.2.1. |
| **CM-2(4).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in CM-2(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)** | |
| **CM-2(5)** | BASELINE CONFIGURATION |
| **CM-2(5).1**  **CM-2(5).1.1**  **CM-2(5).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization develops and maintains a list of software programs authorized to execute on the information system; and* 2. *the organization employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; list of software authorized to execute on the information system; information system architecture and configuration documentation; security plan; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, SA-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-2(5).1.1.1** | **Examine** configuration management policy, procedures addressing the baseline configuration of the information system, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to develop and maintain a list of software programs authorized to execute on the information system. |
| **CM-2(5).1.1.2** | **Examine** list of software programs authorized to execute on the information system; [*reviewing*] for evidence that the measures identified in CM-2(5).1.1.1 are being applied. |
| **CM-2(5).1.2.1** | E**xamine** configuration management plan, information system design documentation, information system architecture and configuration documentation, information system build documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to enforce a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system. |
| **CM-2(5).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of automated mechanisms identified in CM-2(5).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CM-2(5).1.2.1. |
| **CM-2(5).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in CM-2(5).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 6** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CM-2(6)** | BASELINE CONFIGURATION |
| **CM-2(6).1**  **CM-2(6).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system design documentation; information system architecture and configuration documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing baseline configuration environments]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, SA-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-2(6).1.1.1** | **Examine** configuration management policy, procedures addressing the baseline configuration of the information system, configuration management plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to maintain a baseline configuration for development and test environments that is managed separately from the operational baseline configuration. |
| **CM-2(6).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of automated mechanisms identified in CM-2(6).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CM-2(6).1.1.1. |
| **CM-2(6).1.1.3** | **Examine** documentation describing the current baseline configurations deployed in the development, test, and operational environments for an agreed-upon [*basic*] sample of information system components; reviewing for evidence that the baseline configuration maintained for development and test environments is managed separately from the operational baseline configuration. |
| **CM-2(6).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with configuration change control responsibilities; reviewing for further evidence that the measures identified in CM-2(6).1.1.1 are being applied. |
| **CM-2(6).1.1.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in CM-2(6).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |