| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **CM-6** | CONFIGURATION SETTINGS | |
| **CM-6.1**  **CM-6.1.1**  **CM-6.1.2**  **CM-6.1.3**  **CM-6.1.4**  **CM-6.1.5**  **CM-6.1.6** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines security configuration checklists to be used to establish and document mandatory configuration settings for the information system technology products employed;* 2. *the organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements;* 3. *the organization establishes and documents mandatory configuration settings for information technology products employed within the information system using organization-defined security configuration checklists;* 4. *the organization implements the security configuration settings;* 5. *the organization identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and* 6. *the organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; security plan; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with security configuration responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: AC-2, AC-3, AC-6, CM-2, CM-3, CM-5, CM-7, CM-8, RA-5, SI-4  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-6.1.1.1** | | **Examine** information system architecture documentation, information system design documentation, information system build documentation, or other relevant documents; [*reviewing*] for the information technology products employed within the information system. |
| **CM-6.1.1.2** | | **Examine** configuration management policy, procedures addressing configuration settings for the information system, configuration management plan, or other relevant documents; [*reviewing*] for the security configuration checklists to be used to establish and document mandatory configuration settings for an agreed-upon [*basic*] sample of information technology products identified in CM-6.1.1.1. |
|  | |  |
| **CM-6.1.2.1** | | **Examine** configuration management policy, procedures addressing configuration settings for the information system, configuration management plan, or other relevant documents; [*reviewing*] for the requirement that security configuration checklists are to reflect the most restrictive mode consistent with operational requirements. |
| **CM-6.1.2.2** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for establishing and documenting mandatory configuration settings for the information technology products identified in CM-6.1.1.2; conducting [*basic*] discussions for evidence that the security configuration checklists identified in CM-6.1.1.2 reflect the most restrictive mode consistent with operational requirements. |
|  | |  |
| **CM-6.1.3.1** | | **Examine** security configuration checklists for an agreed-upon [*basic*] sample of information technology products employed within the information system; [*reviewing*] for the mandatory configuration settings to be employed. |
|  | |  |
| **CM-6.1.4.1** | | **Examine** an agreed-upon [*basic*]sample of security configuration settings implemented for the information technology products identified in CM-6.1.3.1; [*reviewing*] for evidence that the information system is configured in accordance with the mandatory configuration settings identified in CM-6.1.3.1. |
|  | |  |
| **CM-6.1.5.1** | | **Examine** configuration management policy, procedures addressing configuration settings for the information system, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to identify, document, and approve exceptions from the mandatory configurations settings for individual components within the information system based on explicit operational requirements. |
| **CM-6.1.5.2** | | **Examine** documentation approvals for an agreed-upon [*basic*] sample of exceptions from the mandatory configurations settings for an agreed upon [*basic*] sample of information system components; [*reviewing*] for evidence that the measures identified in CM-6.1.5.1 are being applied. |
|  | |  |
| **CM-6.1.6.1** | | **Examine** configuration management policy, procedures addressing configuration settings for the information system, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to monitor and control changes to the configuration settings. |
| **CM-6.1.6.2** | | **Examine** an agreed-upon [*basic*] sample of monitoring records and change control records associated with changes to the configuration settings for the information system; [*reviewing*] for evidence that the measures identified in CM-6.1.6.1 are being applied. |
| **CM-6.1.6.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for monitoring and controlling changes to information system configuration settings; conducting [*basic*] discussions for further evidence that the measures identified in CM-6.1.6.1 are being applied. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CM-6(1)** | CONFIGURATION SETTINGS |
| **CM-6(1).1**  **CM-6(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; information system design documentation; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing the centralized management, application, and verification of configuration settings]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: AC-2, AC-3, CM-2, CM-3, CM-5, CM-7, CM-8, RA-5, SI-4,  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-6(1).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 centrally manage, apply and verify configuration settings. |
| **CM-6(1).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of automated mechanisms identified in CM-6(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CM-6(1).1.1.1. |
| **CM-6(1).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in CM-6(1).1.1.1; 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-6(2)** | CONFIGURATION SETTINGS |
| **CM-6(2).1**  **CM-6(2).1.1**  **CM-6(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines configuration settings that, if modified by unauthorized changes, initiate the automated mechanisms to be employed to respond to such changes; and* 2. *the organization employs automated mechanisms to respond to unauthorized changes to organization-defined configuration settings.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; security plan; information system design documentation; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing responses to unauthorized changes to configuration settings]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: AC-2, AC-3, CM-2, CM-3, CM-5, CM-7, CM-8, RA-5, SI-4, SI-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-6(2).1.1.1** | **Examine** configuration management policy, procedures addressing configuration settings for the information system, configuration management plan, or other relevant documents; [*reviewing*] for the configuration settings that, if modified by unauthorized changes, initiate the automated mechanisms to be employed to respond to such changes. |
|  |  |
| **CM-6(2).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 respond to unauthorized changes to the configuration settings identified in CM-6(2).1.1.1. |
| **CM-6(2).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of automated mechanisms identified in CM-6(2).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CM-6(2).1.2.1. |
| **CM-6(2).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in CM-6(2).1.2.1; 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-6(3)** | CONFIGURATION SETTINGS |
| **CM-6(3).1**  **CM-6(3).1.1**  **CM-6(3).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization incorporates detection of unauthorized, security-relevant configuration changes into the organization’s incident response capability; and* 2. *the organization ensures that such detected events are tracked, monitored, corrected, and available for historical purposes.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; procedures addressing incident response planning; information system design documentation; information system configuration settings and associated documentation; incident response plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with security configuration responsibilities; organization personnel with incident response planning responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: AC-2, AC-3, CM-2, CM-3, IR-4, IR-5, RA-5, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-6(3).1.1.1** | **Examine** configuration management policy, configuration management plan, incident response plan, or other relevant documents; [*reviewing*] for the requirement to incorporate detection of unauthorized, security-relevant configuration changes into the organization’s incident response capability. |
| **CM-6(3).1.1.2** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with incident response planning responsibilities; conducting [*basic*] discussions for evidence that the detection of unauthorized, security-related configurations changes is incorporated into the organization’s incident response capability. |
|  |  |
| **CM-6(3).1.2.1** | **Examine** configuration management policy, configuration management plan, incident response plan, or other relevant documents; [*reviewing*] for the measures to be employed to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. |
| **CM-6(3).1.2.2** | **Examine** incident response records for an agreed-upon [*basic*] sample of unauthorized, security-relevant configuration changes, if any; [*reviewing*] for evidence that the measures identified in CM-6(3).1.2.1 are being applied. |
| **CM-6(3).1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with incident response planning responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in CM-6(3).1.2.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CM-6(4)** | CONFIGURATION SETTINGS |
| **CM-6(4).1**  **CM-6(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system (including modifications to the baseline configuration) demonstrates conformance to security configuration guidance (i.e., security checklists), prior to being introduced into a production environment.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; information system design documentation; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with security configuration responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: CM-2, CM-3, CM-5, CM-7, CM-8, RA-5, SI-4, SI-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-6(4).1.1.1** | **Examine** configuration management policy, procedures addressing configuration settings for the information system, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to ensure the information system (including modifications to the baseline configurations) conforms to security configuration guidance prior to being introduced into a production environment. |
| **CM-6(4).1.1.2** | **Examine** change control records and associated security configuration documentation for an agreed-upon [*basic*] sample of system installations and modifications; [*reviewing*] for evidence that the measures identified in CM-6(4).1.1.1 are being applied. |
| **CM-6(4).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system inventory responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in CM-6(4).1.1.1 are being applied. |