| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **CM-4** | SECURITY IMPACT ANALYSIS | |
| **CM-4.1**  **CM-4.1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization analyzes changes to the information system to determine potential security impacts prior to change implementation.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the information system; security impact analysis 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 responsibilities for determining security impacts prior to implementation of information system changes]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: CA-2, CA-6, CA-7, CM-3, PM-10, RA-3, RA-5, SA-10, 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. |
| **CM-4.1.1.1** | | **Examine** configuration management policy, procedures addressing security impact analysis for changes to the information system, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to analyze changes to the information system to determine potential security impacts prior to change implementation. |
| **CM-4.1.1.2** | | **Examine** security impact analysis documentation for an agreed-upon [*basic*] sample of changes identified in the configuration status accounting report, change audit summary report, or other relevant documents for the information system; [*reviewing*] for evidence that the measures identified in CM-4.1.1.1 are being applied. |
| **CM-4.1.1.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes; conducting [*basic*] discussions for further evidence that the measures identified in CM-4.1.1.1 are being applied. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CM-4(1)** | SECURITY IMPACT ANALYSIS |
| **CM-4(1).1**  **CM-4(1).1.1**  **CM-4(1).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization analyzes new software in a separate test environment before installation in an operational environment; and* 2. *the organization, when analyzing new software in a separate test environment, looks for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the information system; security impact analysis documentation; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; information system test and operational environments; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: CA-2, CA-6, CA-7, CM-3, , PM-10, RA-3, RA-5, SA-10, SA-11, SI-2  successor controls: CA-5, PM-4, SA-6 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-4(1).1.1.1** | **Examine** configuration management policy, procedures addressing security impact analysis for changes to the information system, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to analyze new software in a separate test environment before installation in an operational environment. |
| **CM-4(1).1.1.2** | **Examine** change control records or information system audit records for an agreed-upon [*basic*] sample of software installations; [*reviewing*] for evidence that the measures identified in CM-4(1).1.1.1 are being applied. |
| **CM-4(1).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes; conducting [*basic*] discussions for further evidence that the measures identified in CM-4(1).1.1.1 are being applied. |
|  |  |
| **CM-4(1).1.2.1** | **Examine** configuration management policy, procedures addressing security impact analysis for changes to the information system, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to identify security impacts due to flaws, weaknesses, incompatibility, or intentional malice, when analyzing new software. |
| **CM-4(1).1.2.2** | **Examine** security impact analysis documentation for an agreed-upon [basic] sample of software installations; [*reviewing*] for evidence that the measures identified in CM-4(1).1.2.1 are being applied. |
| **CM-4(1).1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes; conducting [*basic*] discussions for further evidence that the measures identified in CM-4(1).1.2.1 are being applied. |
|  | |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CM-4(2)** | SECURITY IMPACT ANALYSIS |
| **CM-4(2).1**  **CM-4(2).1.1a**  **CM-4(2).1.1b**  **CM-4(2).1.1c** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization, after the information system is changed, checks the security functions to verify that the functions are:*   * *implemented correctly;* * *operating as intended; and* * *producing the desired outcome with regard to meeting the security requirements for the system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the information system; security impact analysis documentation; change control records; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: CA-2, CA-6, CA-7, CM-3, PM-10, RA-3, RA-5, SA-10, SA-11, SI-2, SI-6  successor controls: CA-5, PM-4 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-4(2).1.1**  **CM-4(2).1.1.a**  **CM-4(2).1.1.b**  **CM-4(2).1.1.c** | **Examine** configuration management policy, procedures addressing security impact analysis for changes to the information system, configuration management plan, or other relevant documents; [*reviewing*] for the measures to the employed to check the security functions, after the information system is changed, to verify that the functions are:   * implemented correctly; * operating as intended; and * producing the desired outcome with regard to meeting the security requirements for the system. |
| **CM-4(2).1.2** | **Examine** change control records for an agreed-upon [*basic*] sample of changes identified in the configuration status accounting report, change audit summary report, or other relevant documents for the information system; [*reviewing*] for evidence that measures identified in CM-4(2).1.1.a are being applied to verify that the security functions are implemented correctly. |
| **CM-4(2).1.3** | **Examine** change control records for an agreed-upon [*basic*] sample of changes identified in the configuration status accounting report, change audit summary report, or other relevant documents for the information system; [*reviewing*] for evidence that measures identified in CM-4(2).1.1.b are being applied to verify that the security functions are operating as intended. |
| **CM-4(2).1.4** | **Examine** change control records for an agreed-upon [*basic*] sample of changes identified in the configuration status accounting report, change audit summary report, or other relevant documents for the information system; [*reviewing*] for evidence that measures identified in CM-4(2).1.1.c are being applied to verify that the security functions are producing the desired outcome with regard to meeting the security requirements for the system. |