| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **CM-5** | ACCESS RESTRICTIONS FOR CHANGE | |
| **CM-5.1**  **CM-5.1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities].  **Test**: [*select from:* Change control process and associated restrictions for changes to the information system]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: AC-2, AC-3, AC-6, CM-3, CM-5, CM-6, CM-7, PE-2, PE-3  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-5.1.1.1** | | **Examine** configuration management policy, procedures addressing access restrictions for changes to the information system, configuration management plan, or other relevant documents; [*reviewing*] for the physical and logical access restrictions to be associated with changes to the information system.  Note to assessor: The requirements to satisfy the CM-5 control may be fully implemented by other controls (e.g., AC-3, PE-3), partially implemented by other controls (e.g., AC-3, PE-3), or completely implemented by the CM-5 control. Therefore, assessors will need to understand and isolate these complexities to successfully adapt assessor actions when evaluating this control. |
| **CM-5.1.1.2** | | **Examine** configuration management policy, procedures addressing access restrictions for changes to the information system, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to document and approve the physical and logical access restrictions identified in CM-5.1.1.1. |
| **CM-5.1.1.3** | | **Examine** access approval records and associated documentation of access privileges for an agreed-upon [*basic*] sample of information system users; [*reviewing*] for evidence that the measures identified in CM-5.1.1.2 are being applied to document and approve physical and logical access restrictions. |
| **CM-5.1.1.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with physical access control responsibilities and organizational personnel with logical access control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in CM-5.1.1.2 are being applied to document and approve physical and logical access restrictions. |
| **CM-5.1.1.5** | | **Examine** configuration management policy, procedures addressing access restrictions for changes to 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 enforce the physical and logical access restrictions identified in CM-5.1.1.1. |
| **CM-5.1.1.6** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in CM-5.1.1.5; [*reviewing*] for evidence that these mechanisms are configured to enforce physical and logical access restrictions as intended in CM-5.1.1.5. |
| **CM-5.1.1.7** | | **Examine** access control records for an agreed-upon [*basic*] sample of information system users; [*reviewing*] for further evidence that the measures identified in CM-5.1.1.5 are being applied to enforce physical and logical access restrictions. |
| **CM-5.1.1.8** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with physical access control responsibilities and organizational personnel with logical access control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in CM-5.1.1.5 are being applied to enforce physical and logical access restrictions. |
| **CM-5.1.1.9** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms identified in CM-5.1.5; conducting [*basic*] testing for evidence that these mechanisms are operating to enforce physical and logical access restrictions as intended in CM-5.1.1.5. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CM-5(1)** | ACCESS RESTRICTIONS FOR CHANGE |
| **CM-5(1).1**  **CM-5(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing access restrictions for changes to the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: AC-2, AC-3, AC-6, AU-2, AU-3, AU-12, CM-3, CM-6, CM-7, PE-3  successor controls: AU-6, AU-7 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-5(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 enforce access restrictions and support auditing of the enforcement actions. |
| **CM-5(1).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of automated mechanisms identified in CM-5(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CM-5(1).1.1.1. |
| **CM-5(1).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in CM-5(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-5(2)** | ACCESS RESTRICTIONS FOR CHANGE |
| **CM-5(2).1**  **CM-5(2).1.1**  **CM-5(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the frequency for conducting audits of information system changes; and* 2. *the organization conducts audits of information system changes in accordance with the organization-defined frequency and when indications so warrant to determine whether unauthorized changes have occurred.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system design documentation; information system architecture and configuration documentation; security plan; change control records; information system audit records; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-12, CM-9  concurrent controls: AU-6, AU-7, CM-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-5(2).1.1.1** | **Examine** configuration management policy, procedures addressing auditing of information system changes, configuration management plan, or other relevant documents; [*reviewing*] for the frequency for conducting audits of information system changes. |
|  |  |
| **CM-5(2).1.1.2** | **Examine** configuration management policy, procedures addressing auditing of information system changes, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to conduct audits of information system changes in accordance with the frequency identified in CM-5(2).1.1.1 and when indications so warrant to determine whether unauthorized changes have occurred. |
| **CM-5(2).1.1.3** | **Examine** change control records and associated information system audit records for an agreed-upon [*basic*] sample of information system changes; [*reviewing*] for evidence that the measures identified in CM-5(2).1.1.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CM-5(3)** | ACCESS RESTRICTIONS FOR CHANGE |
| **CM-5(3).1**  **CM-5(3).1.1**  **CM-5(3).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines critical software programs that the information system will prevent from being installed if such software programs are not signed with a recognized and approved certificate; and* 2. *the information system prevents the installation of organization-defined critical software programs that are not signed with a certificate that is recognized and approved by the organization.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; list of critical software programs to be prohibited from installation without an approved certificate; information system design documentation; information system architecture and configuration documentation; security plan; change control records; information system audit records; other relevant documents or records].  **Test**: [*select from:* Information system mechanisms preventing installation of software programs not signed with an organization-approved certificate]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: AC-2, AC-3, AC-6, CM-2, CM-3, CM-6, CM-7, CM-8, SA-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-5(3).1.1.1** | **Examine** configuration management policy, procedures addressing installation restrictions on critical software programs, configuration management plan, or other relevant documents; [*reviewing*] for the critical software programs to be prohibited from installation if these programs are not signed with a recognized and approved certificate. |
|  |  |
| **CM-5(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 prevent the installation of the critical software programs identified in CM-5(3).1.1.1. |
| **CM-5(3).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of automated mechanisms identified in CM-5(3).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CM-5(3).1.2.1. |
| **CM-5(3).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in CM-5(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-5(4)** | ACCESS RESTRICTIONS FOR CHANGE |
| **CM-5(4).1**  **CM-5(4).1.1**  **CM-5(4).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines information system components and system-level information requiring enforcement of a two-person rule for information system changes; and* 2. *the organization enforces a two-person rule for changes to organization-defined information system components and system-level information.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; security plan; 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 responsible for enforcing a two-person rule for system changes]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: AC-2, AC-3, AC-5, AC-6, CM-3, CM-6, CM-7, CM-8, PE-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-5(4).1.1.1** | **Examine** configuration management policy, procedures addressing access restrictions for changes to the information system, configuration management plan, or other relevant documents; [*reviewing*] for the information system components and system-level information requiring enforcement of a two-person rule for information system changes. |
|  |  |
| **CM-5(4).1.2.1** | **Examine** configuration management policy, procedures addressing access restrictions for changes to 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 enforce a two-person rule (dual authorization) for changes to the information system components and system-level information identified in CM-5(4).1.1.1. |
| **CM-5(4).1.2.2** | **Examine** documentation describing the current configuration settings for an-agreed upon [*basic*] sample of the automated mechanisms identified in CM-5(4).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CM-5(4).1.2.1. |
| **CM-5(4).1.2.3** | **Examine** dual authorization records, access control records, change control records, or information system audit records for an agreed-upon [*basic*] sample of system components and system-level information identified in CM-5(4).1.1.1; [*reviewing*] for further evidence that the measures identified in CM-5(4).1.2.1 are being applied. |
| **CM-5(4).1.2.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for enforcing a two-person rule for system changes; conducting [*basic*] discussions for further evidence that the measures identified in CM-5(4).1.2.1 are being applied. |
| **CM-5(4).1.2.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in CM-5(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-5(5)** | ACCESS RESTRICTIONS FOR CHANGE |
| **CM-5(5).1**  **CM-5(5).1.1**  **CM-5(5).1.2**  **CM-5(5).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment;* 2. *the organization defines the frequency for reviews and reevaluations of information system developer/integrator privileges; and* 3. *the organization reviews and reevaluates information system developer/integrator privileges in accordance with the organization-defined frequency.*   *.***POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; security plan; 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 logical access control responsibilities; organizational personnel with physical access control responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: AC-2, AC-3, AC-5, AC-6, CM-2, CM-3, CM-6, CM-7, CM-8, PE-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-5(5).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 limit information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment. |
|  |  |
| **CM-5(5).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of automated mechanisms identified in CM-5(5).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CM-5(5).1.1.1. |
| **CM-5(5).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in CM-5(5).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **CM-5(5).1.2.1** | **Examine** configuration management policy, procedures addressing access restrictions for changes to the information system, configuration management plan, or other relevant documents; [*reviewing*] for the frequency of reviewing and reevaluating information system developer/integrator privileges. |

|  |  |
| --- | --- |
|  |  |
| **CM-5(5).1.3.1** | **Examine** configuration management policy, procedures addressing access restrictions for changes to the information system, configuration management plan, or other relevant documents; [*reviewing*] for the measures to be employed to review and reevaluate information system developer/integrator privileges in accordance with the frequency identified in CM-5(5).1.2.1. |
| **CM-5(5).1.3.2** | **Examine** an agreed-upon [*basic*] sample of reviews and reevaluations of information system developer/integrator privileges; [*reviewing*] for evidence that the measures identified in CM-5(5).1.3.1 are being applied. |
| **CM-5(5).1.3.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for reviewing and reevaluating information system developer/integrator privileges; conducting [*basic*] discussions for further evidence that the measures identified in CM-5(5).1.3.1 are being applied. |
|  | |
| **ASSESSMENT – Control Enhancement 6** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CM-5(6)** | ACCESS RESTRICTIONS FOR CHANGE |
| **CM-5(6).1**  **CM-5(6).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization limits privileges to change software resident within software libraries (including privileged programs).*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: AC-2, AC-3, AC-5, AC-6, CM-2, CM-3, CM-6, CM-7,  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-5(6).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 limit privileges to change software resident within software libraries (including privileged programs). |
| **CM-5(6).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of automated mechanisms identified in CM-5(6).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CM-5(6).1.1.1. |
| **CM-5(6).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in CM-5(6).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 7** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **CM-5(7)** | ACCESS RESTRICTIONS FOR CHANGE |
| **CM-5(7).1**  **CM-5(7).1.1**  **CM-5(7).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines safeguards and countermeasures to be employed by the information system if security functions (or mechanisms) are changed inappropriately; and* 2. *the information system automatically implements organization-defined safeguards and countermeasures if security functions (or mechanisms) are changed inappropriately.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records].  **Test**: [*select from:* Information system implementing safeguards and countermeasures for inappropriate changes to security functions]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9  concurrent controls: CM-2, CM-3, CM-6, CM-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **CM-5(7).1.1.1** | **Examine** configuration management policy, procedures addressing access restrictions for changes to the information system, configuration management plan, or other relevant documents; [*reviewing*] for the safeguards and countermeasures to be employed by the information system if security functions (or mechanisms) are changed appropriately. |
|  |  |
| **CM-5(7).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 ensure the safeguards and countermeasures identified in CM-5(7).1.1.1 are automatically implemented if security functions (or mechanisms) are changed inappropriately. |
| **CM-5(7).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of automated mechanisms identified in CM-5(7).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in CM-5(7).1.2.1. |
| **CM-5(7).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in CM-5(7).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |