| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SI-7** | SOFTWARE AND INFORMATION INTEGRITY | |
| **SI-7.1**  **SI-7.1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system detects unauthorized changes to software and information.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records].  **Test**: [*select from:* Software integrity protection and verification capability]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-2, CM-3, CM-5, CM-6, SA-4, SA-10, SA-11, SA-13, SI-3, 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. |
| **SI-7.1.1.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to detect unauthorized changes to software and information. |
| **SI-7.1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-7.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-7.1.1.1. |
| **SI-7.1.1.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-7.1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-7(1)** | SOFTWARE AND INFORMATION INTEGRITY |
| **SI-7(1).1**  **SI-7(1).1.1**  **SI-7(1).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the frequency of integrity scans to be performed on the information system; and* 2. *the organization reassesses the integrity of software and information by performing integrity scans of the information system in accordance with the organization-defined frequency.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing software and information integrity; security plan; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-2, CM-3, CM-5, CM-6, RA-5, SA-4, SA-10, SA-11, SA-13, SI-3, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-7(1).1.1.1** | **Examine** system and information integrity policy, procedures addressing software and information integrity, security plan, or other relevant documents; [*reviewing*] for the frequency of integrity scans to be performed on the information system. |
|  |  |
| **SI-7(1).1.2.1** | **Examine** system and information integrity policy, procedures software and information integrity, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to reassess the integrity of software and information by performing integrity scans of the information system in accordance with the frequency identified in SI-7(1).1.1.1. |
| **SI-7(1).1.2.2** | **Examine** an agreed-upon [*basic*] sample of integrity scans results, or other relevant records; [*reviewing*] for evidence that the measures identified in SI-7(1).1.2.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-7(2)** | SOFTWARE AND INFORMATION INTEGRITY |
| **SI-7(2).1**  **SI-7(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing software and information integrity; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; automated tools supporting alerts and notifications for integrity discrepancies; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, IR-4, IR-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-7(2).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated tools and their configuration settings to be employed to provide notification to designated individuals upon discovering discrepancies during integrity verification. |
| **SI-7(2).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated tools identified in SI-7(2).1.1.1; [*reviewing*] for evidence that these tools are configured as identified in SI-7(2).1.1.1. |
| **SI-7(2).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated tools and their configuration settings identified in SI-7(2).1.1.1; conducting [*basic*] testing for evidence that these tools are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-7(3)** | SOFTWARE AND INFORMATION INTEGRITY |
| **SI-7(3).1**  **SI-7(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs centrally managed integrity verification tools.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing software and information integrity; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-2, CM-3, CM-5, CM-6, SA-4, SA-10, SA-11, SA-13, SI-3, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-7(3).1.1.1** | **Examine** system and information integrity policy, procedures addressing software and information integrity, security plan, integrity verification tools and applications documentation, or other relevant documents; [*reviewing*] for the centrally managed integrity verification tools and techniques to be employed. |
| **SI-7(3).1.1.2** | **Examine** system and information integrity policy, procedures addressing software and information integrity, security plan, integrity verification tools and applications documentation, or other relevant documents; [*reviewing*] for the measures (including the process and/or the automated mechanisms and their configuration settings) to be employed to centrally manage integrity verification tools. |
| **SI-7(3).1.1.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SI-7(3).1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-7(3).1.1.2. |
| **SI-7(3).1.1.4** | **Examine** the process employed to centrally manage integrity verification tools; [*reviewing*] for evidence that the process identified in SI-7(3).1.1.2 is being applied. |
| **SI-7(3).1.1.5** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in SI-7(3).1.1.2; 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)** | |
| **SI-7(4)** | SOFTWARE AND INFORMATION INTEGRITY |
| **SI-7(4).1**  **SI-7(4).1.1**  **SI-7(4).1.2**  **SI-7(4).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines information system components that require use of tamper-evident packaging;* 2. *the organization defines the conditions (i.e., transportation from vendor to operational site, during operation, both) under which tamper-evident packaging must be used for organization-defined information system components; and* 3. *the organization requires use of tamper-evident packaging for organization-defined information system components during organization-defined conditions.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing software and information integrity; information system component packaging; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: IR-4, MP-5, SI-3, SA-4, SA-10, SA-11, SA-13, SI-3, SI-4, SC-34  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-7(4).1.1.1** | **Examine** system and information integrity policy, procedures addressing software and information integrity, security plan, or other relevant documents; [*reviewing*] for the information system components that require use of tamper-evident packaging. |
|  |  |
| **SI-7(4).1.2.1** | **Examine** system and information integrity policy, procedures addressing software and information integrity, security plan, or other relevant documents; [*reviewing*] for the conditions (i.e., transportation from vendor to operational site, during operation, both) under which tamper-evident packaging must be used for the components identified in SI-7(4).1.1.1. |
|  |  |
| **SI-7(4).1.3.1** | **Examine** system and information integrity policy, procedures addressing software and information integrity, security plan, or other relevant documents; [*reviewing*] for the requirement of the use of tamper-evident packaging for the information system components identified in SI-7(4).1.1.1 during the conditions identified in SI-7(4).1.2.1. |