| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SA-6** | SOFTWARE USAGE RESTRICTIONS | |
| **SA-6.1**  **SA-6.1.1**  **SA-6.1.2**  **SA-6.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization uses software and associated documentation in accordance with contract agreements and copyright laws;* 2. *the organization employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and* 3. *the organization controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: SA-4, SA-5  concurrent controls: AC-17, AC-18, AC-19, AU-6, CM-3, IR-5, IR-6, PL-4, SA-7  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. |
| **SA-6.1.1.1** | | **Examine** system and services acquisition policy, procedures addressing software usage restrictions, site license documentation, software usage restrictions, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to use software and associated documentation in accordance with contract agreements and copyright laws. |
| **SA-6.1.1.2** | | **Examine** an agreed-upon [*basic*] sample of information system audit records, configuration change control records, information system monitoring records, or other relevant records; [*reviewing*] for evidence that the measures identified in SA-6.1.1.1 are being applied. |
| **SA-6.1.1.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system administration responsibilities and/or organizational personnel operating, using, and/or maintaining the information system; conducting [*basic*] discussions for further evidence that the measures identified in SA-6.1.1.1 are being applied. |
|  | |  |
| **SA-6.1.2.1** | | **Examine** system and services acquisition policy, procedures addressing software usage restrictions, security plan, or other relevant documents; [*reviewing*] for the tracking systems to be employed to control copying and distribution of software and associated documentation protected by quality licenses. |
| **SA-6.1.2.2** | | **Examine** an agreed-upon [*basic*] sample of information system audit records, configuration change control records, information system monitoring records, or other relevant records for an agreed-upon [*basic*] sample of tracking systems identified in SA-6.1.2.1; [*reviewing*] for evidence that these tracking systems are being applied. |
| **SA-6.1.2.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel operating, using, and/or maintaining the information system; conducting [*basic*] discussions for further evidence that the tracking systems identified in SA-6.1.2.1 are being applied. |
|  | |  |
| **SA-6.1.3.1** | | **Examine** system and services acquisition policy, procedures addressing software usage restrictions, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. |
| **SA-6.1.3.2** | | **Examine** an agreed-upon [*basic*] sample of information system audit records, configuration change control records, information system monitoring records, or other relevant records associated with the use of peer-to-peer file sharing technology; [*reviewing*] for evidence that the measures identified in SA-6.1.3.1 are being applied. |
| **SA-6.1.3.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel operating, using, and/or maintaining the information system; conducting [*basic*] discussions for further evidence that the measures identified in SA-6.1.3.1 are being applied. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-6(1)** | SOFTWARE USAGE RESTRICTIONS |
| **SA-6(1).1**  **SA-6(1).1.1**  **SA-6(1).1.2**  **SA-6(1).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization prohibits the use of binary or machine executable code from sources with limited or no warranty without accompanying source code;* 2. *the organization provides exceptions to the source code requirement only when no alternative solutions are available to support compelling mission/operational requirements; and* 3. *the organization obtains express written consent of the authorizing official for exceptions to the source code requirement.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records].  **Interview:** [*select from:* Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: SA-4, SA-5  concurrent controls: SA-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-6(1).1.1.1** | **Examine** system and services acquisition policy, procedures addressing the integration of information security requirements and/or security specifications into the acquisition process, solicitation documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the source code requirement that prohibits the use of binary or machine executable code without accompanying source code from sources with limited or no warranty. |
| **SA-6(1).1.1.2** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system administration responsibilities or organizational personnel operating, using, and/or maintaining the information system; conducting [*basic*] discussions for further evidence of the requirement identified in SA-6(1).1.1.1. |
|  |  |
| **SA-6(1).1.2.1** | **Examine** system and services acquisition policy, procedures addressing the integration of information security requirements and/or security specifications into the acquisition process, security plan, or other relevant documents; [*reviewing*] for the exceptions to be provided to the source code requirement identified in SA-6(1).1.1.1 only when no alternative solutions are available to support compelling mission/operational requirements. |
| **SA-6(1).1.2.2** | **Examine** exceptions provided to the source code requirement identified in SA-6(1).1.1.1 for an agreed-upon [*basic*] sample of acquisition contracts or other relevant acquisition-related documentation obtained for information system services; [*reviewing*] for evidence that these exceptions were provided only when no alternative solutions are available to support compelling mission/operational requirements.  Note to assessor: Execution of this assessor action may depend on the organization’s verbal confirmation and records regarding the existence or nonexistence of exceptions to the source code requirement during the acquisition approval and contractual process to obtain software products without accompanying source code. |
| **SA-6(1).1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system administration responsibilities or organizational personnel operating, using, and/or maintaining the information system; conducting [*basic*] discussions for further evidence that exceptions to the source code requirement identified in SA-6(1).1.1.1 are provided only when no alternative solutions are available to support compelling mission/operational requirements. |
|  |  |
| **SA-6(1).1.3.1** | **Examine** system and services acquisition policy, procedures addressing the integration of information security requirements and/or security specifications into the acquisition process, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to obtain express written consent of the authorizing official for exceptions to the source code requirement identified in SA-6(1).1.1.1. |
| **SA-6(1).1.3.2** | **Examine** express written consent of the authorization official for the exceptions identified in SA-6(1).1.1.1; [*reviewing*] for evidence that the measures identified in SA-6(1).1.3.1 are being applied. |
| **SA-6(1).1.3.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system administration responsibilities or organizational personnel operating, using, and/or maintaining the information system; conducting [*basic*] discussions for further evidence that the measures identified in SA-6(1).1.3.1. |