| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SA-7** | USER-INSTALLED SOFTWARE | |
| **SA-7.1**  **SA-7.1.1**  **SA-7.1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization identifies and documents (as appropriate) explicit rules to be enforced when governing the installation of software by users; and* 2. *the organization (or information system) enforces explicit rules governing the installation of software by users.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; 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].  **Test**: [*select from:* Enforcement of rules for user installed software on the information system; information system for prohibited software]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: SA-4, SA-5  concurrent controls: CM-2, CM-5, CM-6, CM-7, SA-6  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-7.1.1.1** | | **Examine** system and services acquisition policy, procedures addressing user installed software, security plan, or other relevant documents; [*reviewing*] for the explicit rules governing the installation of software by users. |
|  | |  |
| **SA-7.1.2.1** | | **Examine** system and services acquisition policy, procedures addressing user installed software, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration setting) to be employed to enforce the rules identified in SA-7.1.1.1. |
| **SA-7.1.2.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SA-7.1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SA-7.1.2.1. |
| **SA-7.1.2.3** | | **Examine** the software installation rules and audit records enforced by an agreed-upon [*basic*] sample of the automated mechanisms identified in SA-7.1.2.1; [*reviewing*] for evidence that the rules identified in SA-7.1.1.1 are being applied. |
| **SA-7.1.2.4** | | **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-7.1.2.1 are being applied. |
| **SA-7.1.2.5** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in SA-7.1.2.1; conducting [*basic*] testing using simulated events or conditions for evidence that these mechanisms are operating as intended. |
|  | | |