| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SA-14** | CRITICAL INFORMATION SYSTEM COMPONENTS | |
| **SA-14.1**  **SA-14.1.1**  **SA-14.1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the critical information system components that require re-implementation; and* 2. *the organization re-implements organization-defined critical information system components.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; configuration management plan; list of critical information system components requiring re-implementation; configuration baseline for critical information system components; configuration management records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel implementing, operating, and/or maintaining the information system]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: SA-12, SA-13  concurrent controls: None  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-14.1.1.1** | | **Examine** system and services acquisition policy, configuration management plan, security plan, or other relevant documents; [*reviewing*] for the critical information system components that require re-implementation. |
|  | |  |
| **SA-14.1.2.1** | | **Examine** system and services acquisition policy, configuration management plan, configuration baseline for critical information system components, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to re-implement or custom develop the critical information system components identified in SA-14.1.1.1. |
| **SA-14.1.2.2** | | **Examine** an agreed-upon [*basic*] sample of configuration management records for the critical information system components identified in SA-14.1.1.1; [*reviewing*] for evidence that the measures identified in SA-14.1.2.1 are being applied. |
| **SA-14.1.2.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel implementing, operating, and/or maintaining the information system; conducting [*basic*] discussions for further evidence that the measures identified in SA-14.1.2.1 are being applied. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **SA-14(1)** | | CRITICAL INFORMATION SYSTEM COMPONENTS |
| **SA-14(1).1**  **SA-14(1).1.1**  **SA-14(1).1.2**  **SA-14(1).1.3** | | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization identifies information system components for which alternative sourcing is not viable;* 2. *the organization defines the measures to be employed to prevent critical security controls for information system components from being compromised; and* 3. *the organization employs organization-defined measures to ensure that critical security controls for information system components are not compromised.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; information system design documentation; information system configuration settings and associated documentation; list of information system components; security requirements and security specifications for the information system; penetration test and vulnerability scan reports; security test and evaluation results; other relevant documents or records]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: RA-3, SA-12, SA-13  concurrent controls: CA-2  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **SA-14(1).1.1.1** | | **Examine** configuration management plan, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the information system components for which alternative sourcing is not viable. |
| **SA-14(1).1.1.2** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel implementing, operating, and/or maintaining the information system; conducting [*basic*] discussions for further evidence of the information system components identified in SA-14(1).1.1.1 for which alternative sourcing is not viable. |
|  | |  |
| **SA-14(1).1.2.1** | | **Examine** configuration management plan, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to prevent critical security controls for the information system components identified in SA-14(1).1.1.1 from being compromised. |
| **SA-14(1).1.2.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SA-14(1).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SA-14(1).1.2.1. |
| **SA-14(1).1.2.3** | | **Examine** access authorization records, access control records, audit records, or other relevant records for an agreed-upon [*basic*] sample of the information system components identified in SA-14(1).1.1.1; [*reviewing*] for evidence that the measures identified in SA-14(1).1.2.1 are being applied. |
|  | |  |
| **SA-14(1).1.3.1** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel implementing, operating, and/or maintaining the information system; conducting [*basic*] discussions for further evidence that the measures identified in SA-14(1).1.2.1 are being applied to ensure that critical security controls for the information system components identified in SA-14(1).1.1.1 are not compromised. |