| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SA-8** | SECURITY ENGINEERING PRINCIPLES | |
| **SA-8.1**  **SA-8.1.1**  **SA-8.1.2**  **SA-8.1.3**  **SA-8.1.4**  **SA-8.1.5** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *The organization applies information system security engineering principles in the specification of the information system;* 2. *the organization applies information system security engineering principles in the design of the information system;* 3. *the organization applies information system security engineering principles in the development of the information system;* 4. *the organization applies information system security engineering principles in the implementation of the information system; and* 5. *the organization applies information system security engineering principles in the modification of the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; information system design documentation; security requirements and security specifications for the information system; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system design, development, implementation, and modification responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: PM-3, PM-7, PM-9, PM-11, SI-3  successor controls: SA-2, SA-3, SA-4, SA-5, SA-10, SA-11, SA-12, SA-13 |
| **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-8.1.1.1** | | **Examine** system and services acquisition policy, procedures addressing security engineering principles used in the development and implementation of the information system, system development life cycle methodology, security plan, or other relevant documents; [*reviewing*] for the information system security engineering principles to be applied in the specification of the information system. |
| **SA-8.1.1.2** | | **Examine** system and services acquisition policy, procedures addressing security engineering principles used in the development and implementation of the information system, system development life cycle methodology, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to apply the information system security engineering principles identified in SA-8.1.1.1 during the specification of the information system. |
| **SA-8.1.1.3** | | **Examine** an agreed-upon [*basic*] sample of acquisition contracts, security requirements and specifications documentation, or other relevant documents for the information system; [*reviewing*] for evidence that the measures identified in SA-8.1.1.2 are being applied. |
| **SA-8.1.1.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system design, development, implementation, and/or modification responsibilities; [*reviewing*] for further evidence that the measures identified in SA-8.1.1.2 are being applied. |
|  | |  |
| **SA-8.1.2.1** | | **Examine** system and services acquisition policy, procedures addressing security engineering principles used in the development and implementation of the information system, system development life cycle methodology, security plan, or other relevant documents; [*reviewing*] for the information system security engineering principles to be applied in the design of the information system. |
| **SA-8.1.2.2** | | **Examine** system and services acquisition policy, procedures addressing security engineering principles used in the development and implementation of the information system, system development life cycle methodology, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to apply the information system security engineering principles identified in SA-8.1.2.1 during the design of the information system. |
| **SA-8.1.2.3** | | **Examine** an agreed-upon [*basic*] sample of acquisition contracts, information system design documentation, or other relevant documents for the information system; [*reviewing*] for evidence that the measures identified in SA-8.1.2.2 are being applied. |
| **SA-8.1.2.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system design, development, implementation, and/or modification responsibilities; [*reviewing*] for further evidence that the measures identified in SA-8.1.2.2 are being applied. |
|  | |  |
| **SA-8.1.3.1** | | **Examine** system and services acquisition policy, procedures addressing security engineering principles used in the development and implementation of the information system, system development life cycle methodology, security plan, or other relevant documents; [*reviewing*] for the information system security engineering principles to be applied in the development of the information system. |
| **SA-8.1.3.2** | | **Examine** system and services acquisition policy, procedures addressing security engineering principles used in the development and implementation of the information system, system development life cycle methodology, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to apply the information system security engineering principles identified in SA-8.1.3.1 during the development of the information system. |
| **SA-8.1.3.3** | | **Examine** an agreed-upon [*basic*] sample of acquisition contracts, information system test and development documentation, or other relevant documents for the information system; [*reviewing*] for evidence that the measures identified in SA-8.1.3.2 are being applied. |
| **SA-8.1.3.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system design, development, implementation, and/or modification responsibilities; [*reviewing*] for further evidence that the measures identified in SA-8.1.3.2 are being applied. |
|  | |  |
| **SA-8.1.4.1** | | **Examine** system and services acquisition policy, procedures addressing security engineering principles used in the development and implementation of the information system, system development life cycle methodology, security plan, or other relevant documents; [*reviewing*] for the information system security engineering principles to be applied in the implementation of the information system. |
| **SA-8.1.4.2** | | **Examine** system and services acquisition policy, procedures addressing security engineering principles used in the development and implementation of the information system, system development life cycle methodology, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to apply the information system security engineering principles identified in SA-8.1.4.1 during the implementation of the information system. |
| **SA-8.1.4.3** | | **Examine** an agreed-upon [*basic*] sample of acquisition contracts, information system implementation documentation, or other relevant documents for the information system; [*reviewing*] for evidence that the measures identified in SA-8.1.4.2 are being applied.  Note to assessor: Examples of information system implementation documentation may include system administrator manuals, user manuals, installation manuals, configuration manuals, operations manuals, and training manuals. |
| **SA-8.1.4.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system design, development, implementation, and/or modification responsibilities; [*reviewing*] for further evidence that the measures identified in SA-8.1.4.2 are being applied. |
|  | |  |
| **SA-8.1.5.1** | | **Examine** system and services acquisition policy, procedures addressing security engineering principles used in the development and implementation of the information system, system development life cycle methodology, security plan, or other relevant documents; [*reviewing*] for the information system security engineering principles to be applied in the modification of the information system. |
| **SA-8.1.5.2** | | **Examine** system and services acquisition policy, procedures addressing security engineering principles used in the development and implementation of the information system, system development life cycle methodology, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to apply the information system security engineering principles identified in SA-8.1.5.1 during the modification of the information system. |
| **SA-8.1.5.3** | | **Examine** an agreed-upon [*basic*] sample of acquisition contracts, change control documentation, system maintenance documentation, or other relevant documents for the information system; [*reviewing*] for evidence that the measures identified in SA-8.1.5.2 are being applied. |
| **SA-8.1.5.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system design, development, implementation, and/or modification responsibilities; [*reviewing*] for further evidence that the measures identified in SA-8.1.5.2 are being applied. |
|  | | |