| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SA-3** | LIFE CYCLE SUPPORT | |
| **SA-3.1**  **SA-3.1.1**  **SA-3.1.2**  **SA-3.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization manages the information system using a system development life cycle methodology that includes information security considerations;* 2. *the organization defines and documents information system security roles and responsibilities throughout the system development life cycle; and* 3. *the organization identifies individuals having information system security roles and responsibilities.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; information system development life cycle documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information security and system development life cycle responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PM-7, PM-11, SA-8  concurrent controls: AT-3, SA-9, SA-10, SA-11, SA-12  successor controls: SA-2, SA-4 |
| **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-3.1.1.1** | | **Examine** information system engineering documentation; [*reviewing*] for the system development life cycle methodology. |
| **SA-3.1.1.2** | | **Examine** system development life cycle methodology; [*reviewing*] for evidence that the methodology includes information security considerations. |
| **SA-3.1.1.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information security and system development life cycle responsibilities; conducting [*basic*] discussions for evidence that the methodology identified in SA-3.1.1.1 is being applied to manage the information system. |
|  | |  |
| **SA-3.1.2.1** | | **Examine** system and services acquisition policy, procedures addressing the integration of information security into the system development life cycle process, system development life cycle methodology documentation, security plan, or other relevant documents; [*reviewing*] for the information system security roles and responsibilities throughout the system development life cycle. |
|  | |  |
| **SA-3.1.3.1** | | **Examine** system and services acquisition policy, procedures addressing the integration of information security into the system development life cycle process, system development life cycle methodology documentation, security plan, or other relevant documents; [*reviewing*] for the individuals (identified by name and/or by role) with information system security roles and responsibilities. |
|  | | |