| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **RA-2** | SECURITY CATEGORIZATION | |
| **RA-2.1**  **RA-2.1.1**  **RA-2.1.2**  **RA-2.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;* 2. *the organization documents the security categorization results (including supporting rationale) in the security plan for the information system; and* 3. *the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; security plan; security categorization documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with security categorization and risk assessment responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PM-9  concurrent controls: PE-19, PL-2, PL-5, PM-7, PM-11, RA-3  successor controls: CA-2, CA-6, CA-7, CM-4, MP-4, MP-6, RA-5, SA-13, SC-8, SC-9, SC-28 |
| **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. |
| **RA-2.1.1.1** | | **Examine** risk assessment policy, security planning policy, procedures addressing security categorization of organizational information and information systems, security plan, or other relevant documents; [*reviewing*] for the applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance to be employed to categorize information and the information system. |
| **RA-2.1.1.2** | | **Examine** risk assessment policy, security planning policy, procedures addressing security categorization of organizational information and information systems, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to categorize information and the information system in accordance with the applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance identified in RA-2.1.1.1. |
| **RA-2.1.1.3** | | **Examine** an agreed-upon [*basic*] sample of security categorizations for the information system; [*reviewing*] for evidence that the measures identified in RA-2.1.1.2 are being applied. |
| **RA-2.1.1.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with security categorization and risk assessment responsibilities for the information system; conducting [*basic*] discussions for further evidence that the measures identified in RA-2.1.1.2 are being applied. |
|  | |  |
| **RA-2.1.2.1** | | **Examine** security plan for the information system; [*reviewing*] for the security categorization results, including supporting rationale. |
|  | |  |
| **RA-2.1.3.1** | | **Examine** risk assessment policy, security planning policy, procedures addressing security categorization of organizational information and information systems, security plan, or other relevant documents; [*reviewing*] for the measures to be employed by the authorizing official or authorizing official designated representative(s) to review and approve the security categorization decision. |
| **RA-2.1.3.2** | | **Examine** an agreed-upon [*basic*] sample of security categorization reviews and approvals for the information system; [*reviewing*] for evidence that the measures identified in RA-2.1.3.1 are being applied. |
| **RA-2.1.3.3** | | **Interview** authorizing official or an agreed-upon [*basic*] sample of authorizing official designated representatives for the information system; conducting [*basic*] discussions for further evidence that the measures identified in RA-2.1.3.1 are being applied. |
|  | | |