| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 2 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **RA-1** | RISK ASSESSMENT POLICY AND PROCEDURES | |
| **RA-1.1**  **RA-1.1.1**  **RA-1.1.2**  **RA-1.1.2a**  **RA-1.1.2b**  **RA-1.1.2c**  **RA-1.1.2d**  **RA-1.1.2e**  **RA-1.1.2f**  **RA-1.1.3**  **RA-1.1.4**  **RA-1.1.5**  **RA-1.1.6** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization develops and formally documents risk assessment* *policy;* 2. *the organization risk assessment policy addresses:*    * *purpose;*    * *scope;*    * *roles and responsibilities;*    * *management commitment;*    * *coordination among organizational entities; and*    * *compliance;* 3. *the organization disseminates formal documented risk assessment policy to elements within the organization having associated risk assessment roles and responsibilities;* 4. *the organization develops and formally documents risk assessment* *procedures;* 5. *the organization risk assessment procedures facilitate implementation of the risk assessment policy and associated risk assessment controls; and* 6. *the organization disseminates formal documented risk assessment procedures to elements within the organization having associated risk assessment roles and responsibilities.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* risk assessment policy and procedures; information security program documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with risk assessment responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PM-9  concurrent controls: None  successor controls: All other controls in this family |

|  |  |  |
| --- | --- | --- |
| **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-1.1.1.1** | **Examine** information security program documentation; [*reviewing*] for the organization risk assessment policy. | |
|  |  | |
| **RA-1.1.2.1**  **RA-1.1.2.1.a**  **RA-1.1.2.1.b**  **RA-1.1.2.1.c**  **RA-1.1.2.1.d**  **RA-1.1.2.1.e**  **RA-1.1.2.1.f** | **Examine** organization risk assessment policy; [*reviewing*] for evidence that the policy addresses:   * + purpose;   + scope;   + roles and responsibilities;   + management commitment;   + coordination among organizational entities; and   + compliance. | |
|  |  | |
| **RA-1.1.3.1** | **Examine** organization risk assessment policy and procedures, or other relevant documents; [*reviewing*] for the organization elements having associated risk assessment roles and responsibilities and to which the risk assessment policy is to be disseminated or otherwise made available. | |
| **RA-1.1.3.2** | **Interview** an agreed-upon [*basic*] sample of key organizational personnel within the organization elements identified in RA-1.1.3.1; conducting [*basic*] discussions for evidence that the risk assessment policy identified in RA-1.1.1.1 was disseminated to the organizational elements identified in RA-1.1.3.1. | |
|  |  | |
| **RA-1.1.4.1** | **Examine** information security program documentation; [*reviewing*] for the organization risk assessment procedures. | |
|  |  | |
| **RA-1.1.5.1** | **Examine** organization risk assessment procedures; [*reviewing*] for evidence that the procedures facilitate implementation of the risk assessment policy and associated risk assessment controls. | |
|  |  | |
| **RA-1.1.6.1** | **Examine** organization risk assessment policy and procedures, or other relevant documents; [*reviewing*] for the organization elements having associated risk assessment roles and responsibilities and to which the risk assessment procedures are to be disseminated or otherwise made available. | |
| **RA-1.1.6.2** | **Interview** an agreed-upon [*basic*] sample of key organizational personnel within the organization elements identified in RA-1.1.6.1; conducting [*basic*] discussions for evidence that the risk assessment procedures identified in RA-1.1.4.1 were disseminated to the organizational elements identified in RA-1.1.6.1. | |
| ASSESSMENT – Base Control, Part 2 of 2 | | |
| **RA-1.2**  **RA-1.2.1**  **RA-1.2.2**  **RA-1.2.3**  **RA-1.2.4** | | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the frequency of risk assessment policy reviews/updates;* 2. *the organization reviews/updates risk assessment policy in accordance with organization-defined frequency;* 3. *the organization defines the frequency of risk assessment procedure reviews/updates; and* 4. *the organization reviews/updates risk assessment procedures in accordance with organization-defined frequency.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* risk assessment policy and procedures; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with risk assessment responsibilities]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PM-9  concurrent controls: None  successor controls: All other controls in this family |
| **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\*\*** |
| **RA-1.2.1.1** | | **Examine** organization risk assessmentpolicy and procedures, or other relevant documents; [*reviewing*] for the frequency for risk assessment policyreviews and updates. |
|  | |  |
| **RA-1.2.2.1** | | **Examine** change control records or other relevant records for organization risk assessmentpolicy reviews and updates; [*reviewing*] for evidence that the risk assessmentpolicy identified in RA-1.1.1.1 is reviewed and updated in accordance with the frequency identified in RA-1.2.1.1. |
|  | |  |
| **RA-1.2.3.1** | | **Examine** organization risk assessmentpolicy and procedures, or other relevant documents; [*reviewing*] for the frequency for risk assessmentprocedurereviews and updates. |
|  | |  |
| **RA-1.2.4.1** | | **Examine** change control records or other relevant records for an agreed-upon [*basic*] sample ofrisk assessment procedure reviews and updates; [*reviewing*] for evidence that the risk assessment procedures identified in RA-1.1.4.1 are reviewed and updated in accordance with the frequency identified in RA-1.2.3.1. |
|  | | |