| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **RA-3** | RISK ASSESSMENT | |
| **RA-3.1**  **RA-3.1.1**  **RA-3.1.1a**  **RA-3.1.1b**  **RA-3.1.1c**  **RA-3.1.1d**  **RA-3.1.1e**  **RA-3.1.1f**  **RA-3.1.2**  **RA-3.1.3**  **RA-3.1.4**  **RA-3.1.5**  **RA-3.1.6**  **RA-3.1.7** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm, from the unauthorized:*    * *access;*    * *use;*    * *disclosure;*    * *disruption;*    * *modification; or*    * *destruction;* 2. *the organization defines the document in which risk assessment results are documented, selecting from the security plan, risk assessment report, or other organization-defined document;* 3. *the organization documents risk assessment results in the organization-defined document;* 4. *the organization defines the frequency for review of the risk assessment results;* 5. *the organization reviews risk assessment results in accordance with the organization-defined frequency;* 6. *the organization defines the frequency that risk assessments are updated; and* 7. *the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system or environment of operation, or other conditions that may impact the security state of the system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; 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: CA-2, CA-6, CA-7, CM-4, RA-2, RA-5, PL-2, PL-5, PM-8, SI-4  successor controls: AC-6, AU-2, CA-5, CP-6, CP-7, IA-8, MP-2, MP-3, MP-4, MP-5, MP-6,  PL-6 |

|  |  |
| --- | --- |
| **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-3.1.1.1**  **RA-3.1.1.1.a**  **RA-3.1.1.1.b**  **RA-3.1.1.1.c**  **RA-3.1.1.1.d**  **RA-3.1.1.1.e**  **RA-3.1.1.1.f** | **Examine** risk assessment policy, security planning policy, procedures addressing organizational assessments of risk, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to conduct an assessment of risk for the information system and the information it processes, stores, or transmits, to determine the likelihood and magnitude of harm resulting from unauthorized:   * + access;   + use;   + disclosure;   + disruption;   + modification; or   + destruction. |
| **RA-3.1.1.2** | **Examine** an agreed-upon [*basic*] sample of risk assessments for the information system; [*reviewing*] for evidence that the measures identified in RA-3.1.1.1.a are being applied to determine the likelihood and magnitude of harm resulting from unauthorized access to the information system or its information. |
| **RA-3.1.1.3** | **Examine** an agreed-upon [*basic*] sample of risk assessments for the information system; [*reviewing*] for evidence that the measures identified in RA-3.1.1.1.b are being applied to determine the likelihood and magnitude of harm resulting from unauthorized use of the information system or its information. |
| **RA-3.1.1.4** | **Examine** an agreed-upon [*basic*] sample of risk assessments for the information system; [*reviewing*] for evidence that the measures identified in RA-3.1.1.1.c are being applied to determine the likelihood and magnitude of harm resulting from unauthorized disclosure of information on the information system. |
| **RA-3.1.1.5** | **Examine** an agreed-upon [*basic*] sample of risk assessments for the information system; [*reviewing*] for evidence that the measures identified in RA-3.1.1.1.d are being applied to determine the likelihood and magnitude of harm resulting from unauthorized disruption to the information system or its information. |
| **RA-3.1.1.6** | **Examine** an agreed-upon [*basic*] sample of risk assessments for the information system; [*reviewing*] for evidence that the measures identified in RA-3.1.1.1.e are being applied to determine the likelihood and magnitude of harm resulting from unauthorized modification to the information system or its information. |
| **RA-3.1.1.7** | **Examine** an agreed-upon [*basic*] sample of risk assessments for the information system; [*reviewing*] for evidence that the measures identified in RA-3.1.1.1.f are being applied to determine the likelihood and magnitude of harm resulting from unauthorized destruction of the information system or its information. |
| **RA-3.1.1.8** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with risk assessment responsibilities for the information system; conducting [*basic*] discussions for further evidence that the measures identified in RA-3.1.1.1.a are being applied to determine the likelihood and magnitude of harm resulting from unauthorized access to the information system or its information. |
| **RA-3.1.1.9** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with risk assessment responsibilities for the information system; conducting [*basic*] discussions for further evidence that the measures identified in RA-3.1.1.1.b are being applied to determine the likelihood and magnitude of harm resulting from authorized use of the information system or its information. |
| **RA-3.1.1.10** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with risk assessment responsibilities for the information system; conducting [*basic*] discussions for further evidence that the measures identified in RA-3.1.1.1.c are being applied to determine the likelihood and magnitude of harm resulting from unauthorized disclosure of information on the information system. |
| **RA-3.1.1.11** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with risk assessment responsibilities for the information system; conducting [*basic*] discussions for further evidence that the measures identified in RA-3.1.1.1.d are being applied to determine the likelihood and magnitude of harm resulting from unauthorized disruption to the information system or its information. |
| **RA-3.1.1.12** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with risk assessment responsibilities for the information system; conducting [*basic*] discussions for further evidence that the measures identified in RA-3.1.1.1.e are being applied to determine the likelihood and magnitude of harm resulting from unauthorized modification to the information system or its information. |
| **RA-3.1.1.13** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with risk assessment responsibilities for the information system; conducting [*basic*] discussions for further evidence that the measures identified in RA-3.1.1.1.f are being applied to determine the likelihood and magnitude of harm resulting from unauthorized destruction of the information system or its information. |
|  |  |
| **RA-3.1.2.1** | **Examine** risk assessment policy, security planning policy, procedures addressing organizational assessments of risk, security plan, or other relevant documents; [*reviewing*] for the document in which risk assessment results are to be documented. |
|  |  |
| **RA-3.1.3.1** | **Examine** security plan, an agreed-upon [*basic*] sample of risk assessment reports, or other relevant information system documents identified in RA-3.1.2.1; [*reviewing*] for evidence that the documentation identified in RA-3.1.2.1 is being used to document risk assessment results. |
|  |  |
| **RA-3.1.4.1** | **Examine** risk assessment policy, security planning policy, procedures addressing organizational assessments of risk, security plan, or other relevant documents; [*reviewing*] for the frequency in which risk assessment results are to be reviewed. |
|  |  |
| **RA-3.1.5.1** | **Examine** an agreed-upon [*basic*] sample of risk assessment reviews; [*reviewing*] for evidence that risk assessment results are reviewed in accordance with the frequency identified in RA-3.1.4.1. |
|  |  |
| **RA-3.1.6.1** | **Examine** risk assessment policy, security planning policy, procedures addressing organizational assessments of risk, security plan, or other relevant documents; [*reviewing*] for the frequency in which risk assessments are to be updated. |
|  |  |
| **RA-3.1.7.1** | **Examine** risk assessment policy, security planning policy, procedures addressing organizational assessments of risk, security plan, or other relevant documents; [*reviewing*] for the types of significant changes and/or other conditions that require risk assessment updates for the information system or environment of operation in addition to the frequency identified in RA-3.1.6.1. |
| **RA-3.1.7.2** | **Examine** an agreed-upon [*basic*] sample of risk assessment updates; [*reviewing*] for evidence that risk assessments are updated in accordance with the frequency identified in RA-3.1.6.1, the significant changes identified in RA-3.1.7.1, and/or the other conditions identified in RA-3.1.7.1. |
|  | |