| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **IR-5** | INCIDENT MONITORING | |
| **IR-5.1**  **IR-5.1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization tracks and documents information system security incidents.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident monitoring; incident response records and documentation; incident response plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident monitoring responsibilities].  **Test**: [*select from:* Incident monitoring capability for the organization]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8  concurrent controls: AU-6, AU-7, AU-11, IR-4, IR-6, PE-6, SC-7, SI-4  successor controls: None |
| **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. |
| **IR-5.1.1.1** | | **Examine** incident response policy, procedures addressing incident monitoring, incident response plan, or other relevant documents; [*reviewing*] for the measures to be employed to track and document information system security incidents. |
| **IR-5.1.1.2** | | **Examine** an agreed-upon [*basic*] sample of incident monitoring records, information system monitoring records, information system audit records, or other relevant documents; [*reviewing*] for evidence that the measures identified in IR-5.1.1.1 are being applied. |
| **IR-5.1.1.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with incident monitoring responsibilities; conducting [*basic*] discussions for evidence that the measures identified in IR-5.1.1.1 are being applied. |
| **IR-5.1.1.4** | | **Test** incident monitoring capability for the information system using an agreed-upon [*basic*] sample of simulated events or conditions; conducting [*basic*] testing for evidence that the measures identified in IR-5.1.1.1 are being applied as intended. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IR-5(1)** | INCIDENT MONITORING |
| **IR-5(1).1**  **IR-5(1).1.1**  **IR-5(1).1.2**  **IR-5(1).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization employs automated mechanisms to assist in the tracking of security incidents;* 2. *the organization employs automated mechanisms to assist in the collection of security incident information; and* 3. *the organization employs automated mechanisms to assist in the analysis of security incident information.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident monitoring; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting incident monitoring; incident response plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident monitoring responsibilities].  **Test**: [*select from:* Automated mechanisms assisting in tracking of security incidents and in the collection and analysis of incident information]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8  concurrent controls: AU-6, AU-7, AU-11, CM-6, IR-4, IR-6, PE-6, SC-7, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IR-5(1).1.1.1** | **Examine** incident response plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to assist in the tracking of security incidents. |
| **IR-5(1).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in IR-5(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-5(1).1.1.1. |
| **IR-5(1).1.1.3** | **Examine** an agreed-upon [*basic*] sample of information system output records generated by the automated mechanisms identified in IR-5(1).1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-5(1).1.1.1. |
| **IR-5(1).1.1.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in IR-5(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **IR-5(1).1.2.1** | **Examine** incident response plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to assist in the collection of security incident information. |
| **IR-5(1).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in IR-5(1).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-5(1).1.2.1. |
| **IR-5(1).1.2.3** | **Examine** an agreed-upon [*basic*] sample of information system output records generated by the automated mechanisms identified in IR-5(1).1.2.2; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-5(1).1.2.1. |
| **IR-5(1).1.2.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in IR-5(1).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **IR-5(1).1.3.1** | **Examine** incident response plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to support the analysis of security incident information. |
| **IR-5(1).1.3.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in IR-5(1).1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-5(1).1.3.1. |
| **IR-5(1).1.3.3** | **Examine** an agreed-upon [*basic*] sample of information system output records generated by the automated mechanisms identified in IR-5(1).1.3.2; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-5(1).1.3.1. |
| **IR-5(1).1.3.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in IR-5(1).1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |