| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **IR-6** | INCIDENT REPORTING | |
| **IR-6.1**  **IR-6.1.1**  **IR-6.1.2**  **IR-6.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines in the time period required to report suspected security incidents to the organizational incident response capability;* 2. *the organization requires personnel to report suspected security incidents to the organizational incident response capability within the organization-defined time period; and* 3. *the organization reports security incident information to designated authorities.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; security plan; incident response plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident reporting responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8, SI-4  concurrent controls: AU-6, AU-7, AU-11, IR-4, IR-5, IR-7, SI-5  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-6.1.1.1** | | **Examine** incident response policy, procedures addressing incident reporting, incident response plan, or other relevant documents; [*reviewing*] for the time period required to report suspected security incidents to the organizational incident response capability. |
|  | |  |
| **IR-6.1.2.1** | | **Examine** incident response policy, procedures addressing incident reporting, incident response plan, or other relevant documents; [*reviewing*] for the requirement that personnel are to report suspected security incidents to the organizational incident response capability within the time period identified in IR-6.1.1.1. |
| **IR-6.1.2.2** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with incident reporting responsibilities; conducting [*basic*] discussions for further evidence that personnel are required to report suspected security incidents to the organizational response capability within the time period identified in IR-6.1.1.1. |
|  | |  |
| **IR-6.1.3.1** | | **Examine** incident response policy, procedures addressing incident reporting, incident response plan, or other relevant documents; [*reviewing*] for the designated authorities to whom security incident information should be reported. |
| **IR-6.1.3.2** | | **Examine** incident response policy, procedures addressing incident reporting, incident response plan, or other relevant documents; [*reviewing*] for the measures to be employed to report security incident information to the authorities identified in IR-6.1.3.1. |
| **IR-6.1.3.3** | | **Examine** an agreed-upon [*basic*] sample of security incident reports or other relevant security incident information provided to the authorities identified in IR-6.1.3.1; [*reviewing*] for evidence that the measures identified in IR-6.1.3.2 are being applied. |
| **IR-6.1.3.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with incident reporting responsibilities and the authorities identified in IR-6.1.3.1; conducting [*basic*] discussions for evidence that the measures identified in IR-6.1.3.2 are being applied. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IR-6(1)** | INCIDENT REPORTING |
| **IR-6(1).1**  **IR-6(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated mechanisms to assist in the reporting of security incidents.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; incident response plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident reporting responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8, SI-4  concurrent controls: AU-6, AU-7, AU-11, CM-6, IR-4, IR-5, IR-7, SI-5  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IR-6(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 support the incident reporting process. |
| **IR-6(1).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in IR-6(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-6(1).1.1.1. |
| **IR-6(1).1.1.3** | **Examine** an agreed-upon [*basic*] sample of information system reports generated by the automated mechanisms identified in IR-6(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-6(1).1.1.1. |
| **IR-6(1).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with incident reporting responsibilities; conducting [*basic*] discussions for further evidence that the mechanisms and configurations identified in IR-6(1).1.1.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IR-6(2)** | INCIDENT REPORTING |
| **IR-6(2).1**  **IR-6(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; incident response plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident reporting responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8, SI-4  concurrent controls: AU-6, AU-7, AU-11, IR-4, IR-5, IR-7, SI-5  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IR-6(2).1.1.1** | **Examine** incident response policy, procedures addressing incident reporting, incident response plan, or other relevant documents; [*reviewing*] for the organizational officials to whom information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents are to be reported. |
| **IR-6(2).1.1.2** | **Examine** incident response policy, procedures addressing incident reporting, incident response plan, or other relevant documents; [*reviewing*] for the measures to be employed to report information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to the organizational officials identified in IR-6(2).1.1.1. |
| **IR-6(2).1.1.3** | **Examine** an agreed-upon [*basic*] sample of security assessment reports, security vulnerability reports, security audit reports, or other relevant documents associated with security incidents reported to the organizational officials identified in IR-6(2).1.1.1 ; [*reviewing*] for evidence that the measures identified in IR-6(2).1.1.2 are being applied. |
| **IR-6(2).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with incident reporting responsibilities and organizational officials identified in IR-6(2).1.1.1; conducting [*basic*] discussions for evidence that the measures identified in IR-6(2).1.1.2 are being applied. |