| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **IR-4** | INCIDENT HANDLING | |
| **IR-4.1**  **IR-4.1.1**  **IR-4.1.1a**  **IR-4.1.1b**  **IR-4.1.1c**  **IR-4.1.1d**  **IR-4.1.1e**  **IR-4.1.2**  **IR-4.1.3**  **IR-4.1.3a**  **IR-4.1.3b**  **IR-4.1.3c**  **IR-4.1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization implements an incident handling capability for security incidents that includes:*    * *preparation;*    * *detection and analysis;*    * *containment;*    * *eradication; and*    * *recovery;* 2. *the organization coordinates incident handling activities with contingency planning activities; and* 3. *the organization incorporates lessons learned from ongoing incident handling activities into:*    * *incident response procedures;*    * *training; and*    * *testing/exercises; and* 4. *the organization implements the resulting changes to incident response procedures, training and testing/exercise accordingly.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident handling; incident response plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities].  **Test**: [*select from:* Incident handling capability for the organization]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8, SC-7  concurrent controls: AU-6, AU-7, AU-11, CP-2, CP-4, IR-2, IR-3, IR-5, IR-6, IR-7, PE-6, 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-4.1.1.1**  **IR-4.1.1.1.a**  **IR-4.1.1.1.b**  **IR-4.1.1.1.c**  **IR-4.1.1.1.d**  **IR-4.1.1.1.e** | **Examine** incident response policy, procedures addressing incident handling, incident response plan, or other relevant documents; [*reviewing*] for the measures to be employed to implement an incident handling capability for security incidents that includes:   * + preparation;   + detection and analysis;   + containment;   + eradication; and   + recovery. |
| **IR-4.1.1.2** | **Examine** incident handling records and any problem records, change control records, incident response test/exercise records, or other relevant documents associated with an agreed-upon [*basic*] sample of security incidents for the information system; [reviewing] for evidence that the measures identified in IR-4.1.1.1.a are being applied to prepare for security incidents. |
| **IR-4.1.1.3** | **Examine** incident handling records and any problem records, change control records, incident response test/exercise records, or other relevant documents associated with an agreed-upon [*basic*] sample of security incidents identified for the information system; [*reviewing*] for evidence that the measures identified in IR-4.1.1.1.b are being applied to detect and analyze security incidents. |
| **IR-4.1.1.4** | **Examine** incident handling records and any problem records, change control records, incident response test/exercise records, or other relevant documents associated with an agreed-upon [*basic*] sample of security incidents identified for the information system; [*reviewing*] for evidence that the measures identified in IR-4.1.1.1.c are being applied to contain security incidents. |
| **IR-4.1.1.5** | **Examine** incident handling records and any problem records, change control records, incident response test/exercise records, or other relevant documents associated with an agreed-upon [*basic*] sample of security incidents identified for the information system; [*reviewing*] for evidence that the measures identified in IR-4.1.1.1.d are being applied to eradicate security incidents. |
| **IR-4.1.1.6** | **Examine** incident handling records and any problem records, change control records, incident response test/exercise records, or other relevant documents associated with an agreed-upon [*basic*] sample of security incidents for the information system; [reviewing] for evidence that the measures identified in IR-4.1.1.1.e are being applied to recover from security incidents. |
| **IR-4.1.1.7** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with incident handling responsibilities; conducting [*basic*] discussions for evidence that the measures identified in IR-4.1.1.1 are being applied. |
| **IR-4.1.1.8** | **Test** the incident handling capability identified in IR-4.1.1.1 using an agreed-upon [*basic*] sample of simulated events or conditions; conducting [*basic*] testing for evidence that the measures identified in IR-4.1.1.1.a are being applied as intended to prepare for security incidents. |
| **IR-4.1.1.9** | **Test** the incident handling capability identified in IR-4.1.1.1 using an agreed-upon [*basic*] sample of simulated events or conditions; conducting [*basic*] testing for evidence that the measures identified in IR-4.1.1.1.b are being applied as intended to detect and analyze security incidents. |
| **IR-4.1.1.10** | **Test** the incident handling capability identified in IR-4.1.1.1 using an agreed-upon [*basic*] sample of simulated events or conditions; conducting [*basic*] testing for evidence that the measures identified in IR-4.1.1.1.c are being applied as intended to contain security incidents. |
| **IR-4.1.1.11** | **Test** the incident handling capability identified in IR-4.1.1.1 using an agreed-upon [*basic*] sample of simulated events or conditions; conducting [*basic*] testing for evidence that the measures identified in IR-4.1.1.1.d are being applied as intended to eradicate security incidents. |
| **IR-4.1.1.12** | **Test** the incident handling capability identified in IR-4.1.1.1 using an agreed-upon [*basic*] sample of simulated events or conditions; conducting [*basic*] testing for evidence that the measures identified in IR-4.1.1.1.e are being applied as intended to recover from security incidents. |
|  |  |
| **IR-4.1.2.1** | **Examine** incident response policy, contingency planning policy, procedures addressing incident handling, procedures addressing contingency operations, incident response plan, contingency plan, or other relevant documents; [*reviewing*] for the measures to be employed to coordinate incident handling activities with contingency planning activities. |
| **IR-4.1.2.2** | **Examine** an agreed-upon [*basic*] sample of meeting minutes, meeting agendas, status reports, or other relevant documents associated with coordinating incident handling and contingency planning activities; [*reviewing*] for evidence that the measures identified in IR-4.1.2.1 are being applied. |
| **IR-4.1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with incident handling responsibilities and organizational personnel with contingency planning responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in IR-4.1.2.1 are being applied to coordinate incident handling activities with contingency planning activities. |
|  |  |
| **IR-4.1.3.1**  **IR-4.1.3.1.a**  **IR-4.1.3.1.b**  **IR-4.1.3.1.c** | **Examine** incident response policy, procedures addressing incident handling, incident response plan, or other relevant documents; [*reviewing*] for the measures to be employed to incorporate lessons learned from ongoing incident handling activities into:   * + incident response procedures;   + training; and   + testing/exercises. |
| **IR-4.1.3.2** | **Examine** incident response procedures and an agreed-upon [*basic*] sample of change control records addressing lessons learned from ongoing incident response activities; [*reviewing*] for evidence that the measures identified in IR-4.1.3.1.a are being applied to incorporate lessons learned from ongoing incident handling activities into incident response procedures.  Note to assessor: Change control records addressing revisions to incident response procedures may be maintained in the incident response plan, or maintained in change management software or document management software used by the organization. |
| **IR-4.1.3.3** | **Examine** incident response training materials and an agreed-upon [*basic*] sample of change control records addressing lessons learned from ongoing incident response activities; [*reviewing*] for evidence that the measures identified in IR-4.1.3.1.b are being applied to incorporate lessons learned from ongoing incident handling activities into incident response training.  Note to assessor: Change control records addressing revisions to incident response training may be maintained in the incident response plan, or maintained in change management software or document management software used by the organization. |
| **IR-4.1.3.4** | **Examine** incident response tests/exercises and an agreed-upon [*basic*] sample of change control records addressing lessons learned from ongoing incident response activities; [*reviewing*] for evidence that the measures identified in IR-4.1.3.1.c are being applied to incorporate lessons learned from ongoing incident handling activities into incident response testing/exercises.  Note to assessor: Change control records addressing revisions to incident response tests/exercises may be maintained in the incident response plan, or maintained in change management software or document management software used by the organization. |
|  |  |
| **IR-4.1.4.1** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with incident handling responsibilities; [*reviewing*] for evidence that the organization implements the resulting changes identified in IR-4.1.3.2, IR-4.1.3.3, and IR-4.1.3.4 to incident response procedures, training, and testing/exercises accordingly. |
|  | |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IR-4(1)** | INCIDENT HANDLING |
| **IR-4(1).1**  **IR-4(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated mechanisms to support the incident handling process.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident handling responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8, SC-7  concurrent controls: AU-6, AU-7, AU-11, CM-6, CP-2, IR-2, IR-3, IR-5, IR-6, IR-7, PE-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IR-4(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 handling process. |
| **IR-4(1).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic* ] sample of the automated mechanisms identified in IR-4(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-4(1).1.1.1. |
| **IR-4(1).1.1.3** | **Examine** an agreed-upon [*basic*] sample of information system output records generated by the automated mechanisms identified in IR-4(1).1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-4(1).1.1.1. |
| **IR-4(1).1.1.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in IR-4(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IR-4(2)** | INCIDENT HANDLING |
| **IR-4(2).1**  **IR-4(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization includes dynamic reconfiguration of the information system as part of the incident response capability.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident handling responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8, SC-7  concurrent controls: CM-6, IR-2, IR-3, IR-5, IR-6, IR-7, PE-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IR-4(2).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 include dynamic reconfiguration of the information system as part of the incident response capability. |
| **IR-4(2).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample the automated mechanisms identified in IR-4(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-4(2).1.1.1. |
| **IR-4(2).1.1.3** | **Examine** incident handling records, configuration change control records, incident response test/exercise records, contingency plan test/exercise records, or other relevant documents associated with an agreed-upon [*basic*] sample of the automated mechanisms identified in IR-4(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-4(2).1.1.1. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IR-4(3)** | INCIDENT HANDLING |
| **IR-4(3).1**  **IR-4(3).1.1**  **IR-4(3).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization identifies classes of incidents; and* 2. *the organization defines the appropriate actions to take in response to each class of incidents to ensure continuation of organizational missions and business functions.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; security plan; incident response plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident handling responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8, SC-7  concurrent controls: AU-6, AU-7, AU-11, CM-6, CP-2, IR-2, IR-3, IR-5, IR-6, IR-7, PE-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IR-4(3).1.1.1** | **Examine** incident response policy, procedures addressing incident handling, incident response plan, or other relevant documents; [*reviewing*] for the classes of incidents. |
|  |  |
| **IR-4(3).1.2.1** | **Examine** incident response policy, procedures addressing incident handling, incident response plan, or other relevant documents; [*reviewing*] for the actions to be taken in response to the classes of incidents identified in IR-4(3).1.1.1 to ensure continuation of organizational missions and business functions. |
| **IR-4(3).1.2.2** | **Examine** an agreed-upon [*basic*] sample of incident handling records; [*reviewing*] for evidence of the classes of incidents identified in IR-4(3).1.1.1 and the actions taken in response to these incidents as identified in IR-4(3).1.2.1. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IR-4(4)** | INCIDENT HANDLING |
| **IR-4(4).1**  **IR-4(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident handling; incident response plan; automated mechanisms supporting incident handling; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident handling responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8, SC-7  concurrent controls: AU-6, AU-7, AU-11, CM-6, CP-2, IR-2, IR-3, IR-5, IR-6, IR-7, PE-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IR-4(4).1.1.1** | **Examine** incident response policy, procedures addressing incident handling, incident response plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including the process and/or the automated mechanisms and their configuration settings) to be employed to correlate incident information and individual responses to achieve an organization-wide perspective on incident awareness and response. |
| **IR-4(4).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in IR-4(4).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-4(4).1.1.1. |
| **IR-4(4).1.1.3** | **Examine** the process identified in IR-4(4).1.1.1 to correlate incident information and individual incident responses; [*observing*] for evidence that the process identified in IR-4(4).1.1.1 is being applied |
| **IR-4(4).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with incident handling responsibilities; conducting [*basic*] discussions for further evidence that measures identified in IR-4(4).1.1.1 are being applied. |
| **IR-4(4).1.1.5** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in IR-4(4).1.1.1 using an agreed-upon [*basic*] sample of simulated events or conditions; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IR-4(5)** | INCIDENT HANDLING |
| **IR-4(5).1**  **IR-4(5).1.1**  **IR-4(5).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines a list of security violations that, if detected, initiate a configurable capability to automatically disable the information system; and* 2. *the organization implements a configurable capability to automatically disable the information system if any of the organization-defined security violations are detected.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; security plan; incident response plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident handling responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8, SC-7  concurrent controls: AU-2, AU-6, CM-6, CP-2, IR-2, IR-3, IR-5, IR-6, IR-7, PE-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IR-4(5).1.1.1** | **Examine** incident response policy, procedures addressing incident handling, incident response plan, or other relevant documents; [*reviewing*] for the list of security violations that, if detected, initiate a configurable capability to automatically disable the information system. |
|  |  |
| **IR-4(5).1.2.1** | **Examine** incident response plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configurations to be employed to automatically disable the information system if any of the security violations identified in IR-4(5).1.1.1 are detected. |
| **IR-4(5).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in IR-4(5).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-4(5).1.2.1. |
| **IR-4(5).1.2.3** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in IR-4(5).1.2.1 using an agreed-upon [*basic*] sample of simulated events or conditions; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |