| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 2 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **IR-8** | INCIDENT RESPONSE PLAN | |
| **IR-8.1**  **IR-8.1.1**  **IR-8.1.1a**  **IR-8.1.1b**  **IR-8.1.1c**  **IR-8.1.1d**  **IR-8.1.1e**  **IR-8.1.1f**  **IR-8.1.1g**  **IR-8.1.1h** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization develops an incident response plan that:*   * *provides the organization with a roadmap for implementing its incident response capability;* * *describes the structure and organization of the incident response capability;* * *provides a high-level approach for how the incident response capability fits into the overall organization;* * *meets the unique requirements of the organization, which relate to mission, size, structure, and functions;* * *defines reportable incidents;* * *provides metrics for measuring the incident response capability within the organization;* * *defines the resources and management support needed to effectively maintain and mature an incident response capability; and* * *is reviewed and approved by designated officials within the organization.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident response planning responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: None  successor controls: IR-2, IR-3, IR-4, IR-5, IR-6, IR-7 |
| **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-8.1.1.1** | | **Examine** incident response documentation; [*reviewing*] for an incident response plan. |
| **IR-8.1.1.2**  **IR-8.1.1.2a**  **IR-8.1.1.2b**  **IR-8.1.1.2c**  **IR-8.1.1.2d**  **IR-8.1.1.2e**  **IR-8.1.1.2f**  **IR-8.1.1.2g**  **IR-8.1.1.2h** | | **Examine** incident response plan; [*reviewing*] for evidence that the plan:   * + provides the organization with a roadmap for implementing its incident response capability;   + describes the structure and organization of the incident response capability;   + provides a high-level approach for how the incident response capability fits into the overall organization;   + meets the unique requirements of the organization, which relate to mission, size, structure, and functions;   + defines reportable incidents;   + provides metrics for measuring the incident response capability within the organization;   + defines the resources and management support needed to effectively maintain and mature an incident response capability; and   + is reviewed and approved by designated officials within the organization. |
| ASSESSMENT – Base Control, Part 2 of 2 | | |
| **IR-8.2**  **IR-8.2.1**  **IR-8.2.2**  **IR-8.2.3**  **IR-8.2.4**  **IR-8.2.5**  **IR-8.2.6** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines, in the incident response plan, incident response personnel (identified by name and/or role) and organizational elements;* 2. *the organization distributes copies of the incident response plan to incident response personnel and organizational elements identified in the plan;* 3. *the organization defines, in the incident response plan, the frequency to review the plan;* 4. *the organization reviews the incident response plan in accordance with the organization-defined frequency;* 5. *the organization revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and* 6. *the organization communicates incident response plan changes to incident response personnel and organizational elements identified in the plan.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident response planning responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: None  successor controls: IR-2, IR-3, IR-4, IR-5, IR-6, IR-7 |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **IR-8.2.1.1** | | **Examine** incident response plan or other relevant documents; [*reviewing*] for the incident response personnel (identified by name and/or by role) and organizational elements designated to receive copies of the incident response plan. |
|  | |  |
| **IR-8.2.2.1** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel and organizational elements identified in IR-8.2.1.1; conducting [*basic*] discussions for evidence that these individuals received copies of the incident response plan. |
|  | |  |
| **IR-8.2.3.1** | | **Examine** incident response plan or other relevant documents; [*reviewing*] for the frequency of incident response plan reviews. |
|  | |  |
| **IR-8.2.4.1** | | **Examine** incident response plan and other relevant documents resulting from incident response plan reviews; [*reviewing*] for evidence that the plan is reviewed in accordance with the frequency identified in IR-8.2.3.1. |
|  | |  |
| **IR-8.2.5.1** | | **Examine** incident response policy, procedures addressing incident response assistance, incident response plan, or other relevant documents; [*reviewing*] for the measures to be employed to revise the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing. |
| **IR-8.2.5.2** | | **Examine** incident response plan and an agreed-upon [*basic*] sample of change control records addressing incident response plan revisions from system/organizational changes; [*reviewing*] for evidence that the measures identified in IR-8.2.5.1 are being applied.  Note to assessor: Change control records addressing incident response plan revisions may be maintained in the incident response plan, or maintained in change management software or document management software used by the organization. |
| **IR-8.2.5.3** | | **Examine** incident response plan and an agreed-upon [*basic*] sample of change control records addressing incident response plan revisions from problems encountered during plan implementation, execution, or testing; [*reviewing*] for evidence that the measures identified in IR-8.2.5.1 are being applied. |
|  | |  |
| **IR-8.2.6.1** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel and organizational elements identified in IR-8.2.1.1; conducting [*basic*] discussions for evidence that incident response plan changes are communicated to organizational personnel and organizational elements. |