| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **IR-3** | INCIDENT RESPONSE TESTING AND EXERCISES | |
| **IR-3.1**  **IR-3.1.1**  **IR-3.1.2**  **IR-3.1*.*3**  **IR-3.1*.*4**  **IR-3.1*.*5** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines incident response tests/exercises;* 2. *the organization defines the frequency of incident response tests/exercises;* 3. *the organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency;* 4. *the organization documents the results of incident response tests/exercises; and* 5. *the organization determines the effectiveness of the incident response capability.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident response testing and exercises; security plan; incident response testing material; incident response test results; incident response plan; other relevant documents or records].  **Interview:** [*select from:* Organizational personnel with incident response testing responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8  concurrent controls: IR-2, IR-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-3.1.1.1** | | **Examine** incident response policy, procedures addressing incident response testing/exercises, incident response plan, or other relevant documents; [*reviewing*] for the incident response tests/exercises to be conducted for the information system. |
|  | |  |
| **IR-3.1.2.1** | | **Examine** incident response policy, procedures addressing incident response testing/exercises, incident response plan, or other relevant documents; [*reviewing*] for the frequency of incident response tests/exercises. |
|  | |  |
| **IR-3.1.3.1** | | **Examine** an agreed-upon [*basic*] sample of incident response tests/exercises conducted for the information system; [*reviewing*] for evidence that the organization tests/exercises the incident response capability using the tests/exercises identified in IR-3.1.1.1, in accordance with the frequency identified in IR-3.1.2.1, to document the results and determine incident response effectiveness. |
|  | |  |
| **IR-3.1.4.1** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for testing/exercising the incident response capability for the information system; conducting [*basic*] discussions for further evidence that the organization documents the results of incident response tests/exercises using the tests/exercises identified in IR.3.1.1.1 in accordance with the frequency identified in IR-3.1.2.1. |
|  | |  |
| **IR-3.1.5.1** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for testing/exercising the incident response capability for the information system; conducting [*basic*] discussions for further evidence that the organization determines the effectiveness of the incident response capability using the tests/exercises identified in IR-3.1.1.1 in accordance with the frequency identified in IR-3.1.2.1. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **IR-3(1)** | | INCIDENT RESPONSE TESTING AND EXERCISES |
| **IR-3(1).1**  **IR-3(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability for the information system.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident response testing and exercises; security plan; incident response testing documentation; automated mechanisms supporting incident response tests/exercises; incident response plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident response testing responsibilities]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8  concurrent controls: CM-6, IR-2, IR-4  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **IR-3(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 more thoroughly and effectively test/exercise the incident response capability for the information system. |
| **IR-3(1).1.1.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in IR-3(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-3(1).1.1.1. |
| **IR-3(1).1.1.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with incident response test/exercise responsibilities; conducting [*basic*] discussions for evidence that the mechanisms identified in IR-3(1).1.1 are employed to more thoroughly and effectively test/exercise the incident response capability for the information system. |