| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **IR-2** | INCIDENT RESPONSE TRAINING | |
| **IR-2.1**  **IR-2.1.1**  **IR-2.1.2**  **IR-2.1.3**  **IR-2.1.4**  **IR-2.1.5** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization identifies personnel with incident response roles and responsibilities with respect to the information system;* 2. *the organization provides incident response training to personnel with incident response roles and responsibilities with respect to the information system;* 3. *incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities;* 4. *the organization defines the frequency of refresher incident response training; and* 5. *the organization provides refresher incident response training in accordance with the organization-defined frequency.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident response training; incident response training material; security plan; incident response plan; incident response training records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident response training and operational responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8  concurrent controls: IR-3, 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-2.1.1.1** | | **Examine** incident response policy, procedures addressing incident response training, incident response plan, or other relevant documents; [*reviewing*] for organizational personnel (identified by name and/or by role) with incident response roles and responsibilities with respect to the information system. |
|  | |  |
| **IR-2.1.2.1** | | **Examine** incident response policy, procedures addressing incident response training, incident response plan, or other relevant documents; [*reviewing*] for the measures to be employed to provide incident response training to the organizational personnel identified in IR-2.1.1.1. |
| **IR-2.1.2.2** | | **Examine** training records for an agreed-upon [*basic*] sample of organizational personnel identified in IR-2.1.1.1; [*reviewing*] for evidence that the measures identified in IR-2.1.2.1 are being applied. |
| **IR-2.1.2.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel identified in IR-2.1.2.2; conducting [*basic*] discussions for further evidence that the measures identified in IR-2.1.2.1 are being applied. |
|  | |  |
| **IR-2.1.3.1** | | **Examine** incident response policy, procedures addressing incident response training, incident response plan, or other relevant documents; [*reviewing*] for organizational incident response roles and responsibilities. |
| **IR-2.1.3.2** | | **Examine** incident response policy, procedures addressing incident response training, incident response plan, or other relevant documents; [*reviewing*] for the procedures and activities necessary to fulfill the organizational incident response roles and responsibilities identified in IR-2.1.3.1. |
| **IR-2.1.3.3** | | **Examine** an agreed-upon [*basic*] sample of incident response training material; [*reviewing*] for evidence that the material addresses the procedures and activities identified in IR-2.1.3.2 necessary to fulfill the organizational incident response roles and responsibilities identified in IR-2.1.3.1. |
|  | |  |
| **IR-2.1.4.1** | | **Examine** incident response policy, procedures addressing incident response training, incident response plan, or other relevant documents; [*reviewing*] for the frequency of refresher incident response training. |
| **IR-2.1.5.1** | | **Examine** training records for an agreed-upon [*basic*] sample of the organizational personnel identified in IR-2.1.1.1; [*reviewing*] for evidence that refresher incident response training is provided in accordance with the frequency identified in IR-2.1.4.1. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IR-2(1)** | INCIDENT RESPONSE TRAINING |
| **IR-2(1).1**  **IR-2(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident response training; incident response training material; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident response training and operational responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8  concurrent controls: IR-3, IR-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IR-2(1).1.1.1** | **Examine** incident response policy, procedures addressing incident response training, incident response plan, or other relevant documents; [*reviewing*] for the measures to be employed to incorporate simulated events into incident response training. |
| **IR-2(1).1.1.2** | **Examine** incident response training curriculum, incident response training material, or other relevant documents; [*reviewing*] for evidence that the measures identified in IR-2(1).1.1.1 are being applied. |
| **IR-2(1).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with incident response training and operational responsibilities; conducting [*basic*] discussions for evidence that the measures identified in IR-2(1).1.1.1 facilitate effective response to crisis situations. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IR-2(2)** | INCIDENT RESPONSE TRAINING |
| **IR-2(2).1**  **IR-2(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident response training; incident response training material; automated mechanisms supporting incident response training; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident response training and operational responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8  concurrent controls: CM-6, IR-3, IR-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IR-2(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 provide a more thorough and realistic incident response training environment. |
| **IR-2(2).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in IR-2(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-2(2).1.1.1. |
| **IR-2(2).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel who received incident response training and organizational personnel with incident response training responsibilities; conducting [*basic*] discussions for further evidence that the mechanisms identified in IR-2(2).1.1.1 are being employed to provide a more thorough and realistic training environment for the information system. |