| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **IR-7** | INCIDENT RESPONSE ASSISTANCE | |
| **IR-7.1**  **IR-7.1.1**  **IR-7.1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents; and* 2. *the incident response support resource is an integral part of the organization’s incident response capability.*   **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 assistance and support responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8  concurrent controls: IR-4, IR-6  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-7.1.1.1** | | **Examine** incident response policy, procedures addressing incident response assistance, incident response plan, or other relevant documents; [*reviewing*] for an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. |
| **IR-7.1.1.2** | | **Examine** an agreed-upon [*basic*] sample of incident response records; [*reviewing*] for the information system users associated with the security incidents and for the incident response support personnel providing the resource identified in IR-7.1.1.1. |
| **IR-7.1.1.3** | | **Interview** an agreed-upon [*basic*] sample of information system users and incident response support personnel identified in IR-7.1.1.2; conducting [*basic*] discussions for evidence that the incident response support resource provides advice and assistance for the handling and reporting of security incidents. |
|  | |  |
| **IR-7.1.2.1** | | **Examine** incident response policy, procedures addressing incident response assistance, incident response plan, or other relevant documents; [*reviewing*] for evidence that the incident response support resource is an integral part of the organization’s incident response capability. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **IR-7(1)** | | INCIDENT RESPONSE ASSISTANCE |
| **IR-7(1).1**  **IR-7(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated mechanisms to increase the availability of incident response-related information and support.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident response assistance; automated mechanisms supporting incident response support and assistance; incident response plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident response support and assistance responsibilities; organizational personnel that require incident response support and assistance]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8  concurrent controls: CM-6, IR-4, IR-6  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **IR-7(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 increase the availability of incident response-related information and support. |
| **IR-7(1).1.1.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in IR-7(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IR-7(1).1.1.1. |
| **IR-7(1).1.1.3** | | **Examine** an agreed-upon [*basic*] sample of information system reports generated by the automated mechanisms identified in IR-7(1).1.1.1; [*reviewing*] for the information system users previously supported or assisted by these mechanisms and for evidence that these mechanisms are configured as identified in IR-7(1).1.1.1. |
| **IR-7(1).1.1.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with incident response support and assistance responsibilities and information system users identified in IR-7(1).1.1.3; conducting [*basic*] discussions for evidence that the mechanisms and configurations identified in IR-7(1).1.1.1 are being applied. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IR-7(2)** | INCIDENT RESPONSE ASSISTANCE |
| **IR-7(2).1**  **IR-7(2).1.1**  **IR-7(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and* 2. *the organization identifies organizational incident response team members to the external providers.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Incident response policy; procedures addressing incident response assistance; automated mechanisms supporting incident response support and assistance; incident response plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with incident response support and assistance responsibilities; external providers of information system protection capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IR-8  concurrent controls: IR-4, IR-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IR-7(2).1.1.1** | **Examine** incident response plan or other relevant documents; [*reviewing*] for external providers of information system protection capability. |
| **IR-7(2).1.1.2** | **Examine** incident response policy, procedures addressing incident response assistance, incident response plan, or other relevant documents; [*reviewing*] for the measures to be employed to establish a direct, cooperative relationship between the organization’s incident response capability and the external providers identified in IR-7(2).1.1.1. |
| **IR-7(2).1.1.3** | **Examine** memorandums of agreement between the organization and an agreed-upon [*basic*] sample of external service providers identified in IR-7(2).1.1.1; [*reviewing*] for evidence that the measures identified in IR-7(2).1.1.2 are being applied. |
| **IR-7(2).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with incident response support and assistance responsibilities and/or external service providers identified in IR-7(2).1.1.1; conducting [*basic*] discussions for further evidence that the measures identified in IR-7(2).1.1.2 are being applied. |
|  |  |
| **IR-7(2).1.2.1** | **Examine** memorandums of agreement identified in IR-7(2).1.1.3, or other relevant documents; [*reviewing*] for evidence that the organization identifies incident response team members to the external providers. |