| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SI-5** | SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | |
| **SI-5.1**  **SI-5.1.1**  **SI-5.1.2**  **SI-5.1.3**  **SI-5.1.4**  **SI-5.1.5** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;* 2. *the organization generates internal security alerts, advisories, and directives;* 3. *the organization defines personnel (identified by name and/or by role) who should receive security alerts, advisories, and directives;* 4. *the organization disseminates security alerts, advisories, and directives to organization-identified personnel; and* 5. *the organization implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing security alerts and advisories; records of security alerts and advisories; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the information system]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AT-5  successor controls: RA-5, SI-2 |
| **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. |
| **SI-5.1.1.1** | | **Examine** system and information integrity policy, procedures addressing security alerts and advisories, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to receive information system security alerts, advisories, and directives from designated external organizations on an ongoing basis. |
| **SI-5.1.1.2** | | **Examine** an agreed-upon [*basic*] sample of security alerts, advisories, and directives received from external organizations; [*reviewing*] for evidence that the measures identified in SI-5.1.1.1 are being applied. |
|  | |  |
| **SI-5.1.2.1** | | **Examine** system and information integrity policy, procedures addressing security alerts and advisories, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to generate internal security alerts, advisories, and directives. |
| **SI-5.1.2.2** | | **Examine** an agreed-upon [*basic*] sample of records of internal security alerts, advisories, and directives generated; [*reviewing*] for evidence that the measures identified in SI-5.1.2.1 are being applied. |
|  | |  |
| **SI-5.1.3.1** | | **Examine** system and information integrity policy, procedures addressing security alerts and advisories, security plan, or other relevant documents; [*reviewing*] for the designated personnel (identified by name and/or by role) who should receive security alerts, advisories, and directives. |
|  | |  |
| **SI-5.1.4.1** | | **Examine** system and information integrity policy, procedures addressing security alerts and advisories, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to disseminate security alerts, advisories, and directives to the personnel identified in SI-5.1.3.1. |
| **SI-5.1.4.2** | | **Examine** an agreed-upon [*basic*] sample of security alerts, advisories, and directives disseminated to the designated personnel identified in SI-5.1.3.1; [*reviewing*] for evidence that the measures identified in SI-5.1.4.1 are being applied. |
|  | |  |
| **SI-5.1.5.1** | | **Examine** system and information integrity policy, procedures addressing security alerts and advisories, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to implement security directives in accordance with established time frames, or to notify the issuing organization of the degree of noncompliance. |
| **SI-5.1.5.2** | | **Examine** security directive implementation reports or email notifying organization of noncompliance for an agreed-upon [*basic*] sample of security directives; [*reviewing*] for evidence that the measures identified in SI-5.1.5.1 are being applied. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-5(1)** | SECURITY ALERTS, ADVISORIES, AND DIRECTIVES |
| **SI-5(1).1**  **SI-5(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated mechanisms to make security alert and advisory information available throughout the organization.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing security alerts and advisories; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting the distribution of security alert and advisory information; records of security alerts and advisories; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing the distribution of security alert and advisory information]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AT-5, CM-6  successor controls: RA-5, SI-2 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-5(1).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to make security alert and advisory information available throughout the organization. |
| **SI-5(1).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-5(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-5(1).1.1.1. |
| **SI-5(1).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-5(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |