| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SI-11** | ERROR HANDLING | |
| **SI-11.1**  **SI-11.1.1**  **SI-11.1.2**  **SI-11.1.3**  **SI-11.1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the information system identifies potentially security-relevant error conditions;* 2. *the organization defines sensitive or potentially harmful information that should not be contained in error logs and administrative messages;* 3. *the information system generates error messages that provide information necessary for corrective actions without revealing organization-defined sensitive or potentially harmful information in error logs and administrative messages that could be exploited by adversaries; and* 4. *the information system reveals error messages only to authorized personnel.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system error handling; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Information system error handling capability]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AU-2, AU-3, AU-9, AC-5, AC-6, CM-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. |
| **SI-11.1.1.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to identify potentially security-relevant error conditions. |
| **SI-11.1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-11.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-11.1.1.1. |
| **SI-11.1.1.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-11.1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |  |
| **SI-11.1.2.1** | | **Examine** system and information integrity policy, procedures addressing information system error handling, security plan, or other relevant documents; [*reviewing*] for the sensitive or potentially harmful information that should not be contained in error logs and administrative messages. |
|  | |  |
| **SI-11.1.3.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to generate error messages that provide information necessary for corrective actions without revealing the sensitive or potentially harmful information identified in SI-11.1.2.1 in error logs and administrative messages that could be exploited by adversaries. |
| **SI-11.1.3.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-11.1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-11.1.3.1. |
| **SI-11.1.3.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-11.1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |  |
| **SI-11.1.4.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to reveal error messages only to authorized personnel. |
| **SI-11.1.4.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-11.1.4.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-11.1.4.1. |
| **SI-11.1.4.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-11.1.4.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | | |