| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SC-24** | FAIL IN KNOWN STATE | |
| **SC-24.1**  **SC-24.1.1**  **SC-24.1.2**  **SC-24.1.3**  **SC-24.1.4**  **SC-24.1.5** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the known-states the information system should fail to in the event of a system failure;* 2. *the organization defines types of failures for which the information system should fail to an organization-defined known-state;* 3. *the organization defines the system state information that should be preserved in the event of a system failure;* 4. *the information system fails to an organization-defined known-state for an organization-defined type of failure; and* 5. *the information system preserves organization-defined system state information in the event of a system failure.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing information system failure; information system design documentation; information system configuration settings and associated documentation; list of failures requiring information system to fail in a known state; state information to be preserved in system failure; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing fail-in-known-state capability]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, CP-2, CP-10, SC-7, SI-13  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. |
| **SC-24.1.1.1** | | **Examine** system and communications protection policy, procedures addressing information system failure, security plan, or other relevant documents; [*reviewing*] for the known-states the information system should fail to in the event of a system failure. |
|  | |  |
| **SC-24.1.2.1** | | **Examine** system and communications protection policy, procedures addressing information system failure, security plan, or other relevant documents; [*reviewing*] for the types of failures for which the information system should fail to the known-states identified in SC-24.1.1.1. |
|  | |  |
| **SC-24.1.3.1** | | **Examine** system and communications protection policy, procedures addressing information system failure, security plan, or other relevant documents; [*reviewing*] for the system state information that should be preserved in the event of a system failure. |
|  | |  |
| **SC-24.1.4.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to fail to one of the known states identified in SC-24.1.1.1 for one of the failures identified in SC-24.1.2.1. |
| **SC-24.1.4.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-24.1.4.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-24.1.4.1. |
| **SC-24.1.4.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-24.1.4.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |  |
| **SC-24.1.5.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to preserve the system state information identified in SC-24.1.3.1 in the event of a system failure. |
| **SC-24.1.5.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-24.1.5.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-24.1.5.1. |
| **SC-24.1.5.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-24.1.5.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | | |