| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SI-13** | PREDICTABLE FAILURE PREVENTION | |
| **SI-13.1**  **SI-13.1.1**  **SI-13.1.2**  **SI-13.1.3**  **SI-13.1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines information system components for which mean time to failure rates should be considered to protect the information system from harm;* 2. *the organization protects the information system from harm by considering mean time to failure rates for organization-defined information system components in specific environments of operation;* 3. *the organization provides substitute information system components, when needed; and* 4. *the organization provides a mechanism to exchange active and standby roles of the components.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing predictable failure prevention; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Interview:** [*select from:* Organizational personnel with predictable failure prevention responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CP-2  concurrent controls: AU-5, CM-2, CP-10, SC-24  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-13.1.1.1** | | **Examine** system and information integrity policy, procedures addressing predictable failure prevention, contingency plan, security plan, or other relevant documents; [*reviewing*] for the information system components for which mean time to failure rates should be considered to protect the information system from harm. |
|  | |  |
| **SI-13.1.2.1** | | **Examine** system and information integrity policy, procedures addressing predictable failure prevention, contingency plan, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to protect the information system from harm by considering mean time to failure rates for system components identified in SI-13.1.1.1 via specific environments of operation. |
| **SI-13.1.2.2** | | **Examine** mean time to failure rates for an agreed-upon [*basic*] sample of information system components; [*reviewing*] for evidence that the measures identified in SI-13.1.2.1 are being applied. |
| **SI-13.1.2.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with predictable failure prevention responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in SI-13.1.2.1 are being applied. |
|  | |  |
| **SI-13.1.3.1** | | **Examine** system and information integrity policy, procedures addressing predictable failure prevention, contingency plan, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to provide substitute information components when needed. |
| **SI-13.1.3.2** | | **Examine** an agreed-upon [*basic*] sample of service level agreements, information system component inventory, records of substitute information system components, or other relevant documents; [*reviewing*] for evidence that the measures identified in SI-13.1.3.1 are being applied. |
|  | |  |
| **SI-13.1.4.1** | | **Examine** contingency plan, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to exchange active and standby roles of components. |
| **SI-13.1.4.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-13.1.4.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-13.1.4.1. |
| **SI-13.1.4.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-13.1.4.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-13(1)** | PREDICTABLE FAILURE PREVENTION |
| **SI-13(1).1**  **SI-13(1).1.1**  **SI-13(1).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the maximum fraction or percentage of mean time to failure in order to transfer the responsibilities of an information system component that is out of service to a substitute component; and* 2. *the organization takes the information system component out of service by transferring component responsibilities to a substitute component no later than the organization-defined fraction or percentage of mean time to failure.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing predictable failure prevention; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Interview:** [*select from:* Organization personnel with predictable failure prevention responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CP-2  concurrent controls: AU-5, CM-2, CP-10, SC-24  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-13(1).1.1.1** | **Examine** system and information integrity policy, procedures addressing predictable failure prevention, contingency plan, security plan, or other relevant documents; [*reviewing*] for the maximum fraction or percentage of mean time to failure in order to transfer the responsibilities of an information system component that is out of service to a substitute component. |
|  |  |
| **SI-13(1).1.2.1** | **Examine** contingency plan, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the mechanisms and their configuration settings to be employed to take the information system component out of service by transferring component responsibilities to a substitute component no later than the fraction or percentage of mean time to failure identified in SI-13(1).1.1.1. |
| **SI-13(1).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the mechanisms identified in SI-13(1).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-13(1).1.2.1. |
| **SI-13(1).1.2.3** | **Test** an agreed-upon [*basic*]sample of the mechanisms and their configuration settings identified in SI-13(1).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-13(2)** | PREDICTABLE FAILURE PREVENTION |
| **SI-13(2).1**  **SI-13(2).1.1**  **SI-13(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the time period that a process is allowed to execute without supervision; and* 2. *the organization does not allow a process to execute without supervision for more than the organization-defined time period.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing predictable failure prevention; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Information system predictable failure prevention capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: None  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-13(2).1.1.1** | **Examine** system and information integrity policy, procedures addressing predictable failure prevention, security plan, or other relevant documents; [*reviewing*] for the time period that a process is allowed to execute without supervision. |
|  |  |
| **SI-13(2).1.2.1** | **Examine** system and information integrity policy, procedures addressing predictable failure prevention, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including the process and/or the automated mechanisms and their configuration settings) to be employed to not allow a process to execute without supervision for more than the time period identified in SI-13(2).1.1.1. |
| **SI-13(2).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SI-13(2).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-13(2).1.2.1. |
| **SI-13(2).1.2.3** | **Examine** the measures (process) employed to not allow a process to execute without supervision for more than the time period identified in SI-13(2).1.1.1; [*reviewing*] for evidence that the measures (process) identified in SI-13(2).1.2.1 is being applied. |
| **SI-13(2).1.2.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in SI-13(2).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-13(3)** | PREDICTABLE FAILURE PREVENTION |
| **SI-13(3).1**  **SI-13(3).1.1**  **SI-13(3).1.2**  **SI-13(3).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the minimum frequency with which the organization manually initiates a transfer between active and standby information system components if the mean time to failure exceeds the organization-defined time period;* 2. *the organization defines the time period that the mean time to failure must exceed before the organization manually initiates a transfer between active and standby information system components; and* 3. *the organization manually initiates a transfer between active and standby information system components at least once per the organization-defined frequency if the mean time to failure exceeds the organization-defined time period.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing predictable failure prevention; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Interview:** [*select from:* Organizational personnel with predictable failure prevention responsibilities].  **Test**: [*select from:* Information system predictable failure prevention capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CP-2  concurrent controls: AU-5, CM-2, CP-10, SC-24  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-13(3).1.1.1** | **Examine** system and information integrity policy, procedures addressing predictable failure prevention, contingency plan, security plan, or other relevant documents; [*reviewing*] for the time period that the mean time to failure must exceed before the organization manually initiates a transfer between active and standby information system components. |
|  |  |
| **SI-13(3).1.2.1** | **Examine** system and information integrity policy, procedures addressing predictable failure prevention, contingency plan, security plan, or other relevant documents; [*reviewing*] for the minimum frequency with which the organization manually initiates a transfer between active and standby information system component if the mean time to failure exceeds the time period identified in SI-13(3).1.1.1. |
|  |  |
| **SI-13(3).1.3.1** | **Examine** system and information integrity policy, procedures addressing predictable failure prevention, contingency plan, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to manually initiate a transfer between active and standby information system components at least once per the frequency identified in SI-13(3).1.2.1 if the mean time to failure exceeds the time period identified in SI-13(3).1.1.1. |
| **SI-13(3).1.3.2** | **Examine** an agreed-upon [*basic*] sample of records documenting transfer between active and standby system components; [*reviewing*] for evidence that the measures identified in SI-13(3).1.3.1 are being applied. |
| **SI-13(3).1.3.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with predictable failure prevention responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in SI-13(3).1.3.1 are being applied. |
|  | |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-13(4)** | PREDICTABLE FAILURE PREVENTION |
| **SI-13(4).1**  **SI-13(4).1.1**  **SI-13(4).1.2**  **SI-13(4).1.3**  **SI-13(4).1.3a**  **SI-13(4).1.3b** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the time period for a standby information system component to successfully and transparently assume the role of an information system component that has failed;* 2. *the organization defines the organization-defined alarm when an information system component failure is detected; and* 3. *the organization, if an information system component failure is detected:*    * *ensures that the standby information system component successfully and transparently assumes its role within the organization-defined time period; and*    * *activates the organization-defined alarm and/or automatically shuts down the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing predictable failure prevention; information system design documentation; information system configuration settings and associated documentation; list of actions to be taken once information system component failure is detected; other relevant documents or records].  **Test**: [*select from:* Information system predictable failure prevention capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CP-2  concurrent controls: AU-5, CM-2, CM-6, CP-10, SC-24  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-13(4).1.1.1** | **Examine** system and information integrity policy, procedures addressing predictable failure prevention, contingency plan, security plan, or other relevant documents; [*reviewing*] for the time period for a standby information system component to successfully and transparently assume the role of an information system component that has failed. |
|  |  |
| **SI-13(4).1.2.1** | **Examine** system and information integrity policy, procedures addressing predictable failure prevention, contingency plan, security plan, or other relevant documents; [*reviewing*] for the alarm when an information system component failure is detected. |
|  |  |
| **SI-13(4).1.3.1**  **SI-13(4).1.3.1.a**  **SI-13(4).1.3.1.b** | **Examine** contingency plan, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed, if an information system component failure is detected, to:   * + ensure that the standby information system component successfully and transparently assumes its role within the time period identified in SI-13(4).1.1.1; and   + activate the alarm identified in SI-13(4).1.2.1 and/or automatically shuts down the information system. |
| **SI-13(4).1.3.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-13(4).1.3.1.a; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-13(4).1.3.1.a to ensure that the standby information system components successfully and transparently assumes its role within the time period identified in SI-13(4).1.1.1. |
| **SI-13(4).1.3.3** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-13(4).1.3.1.b; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-13(4).1.3.1.b to activate the alarm identified in SI-13(4).1.2.1 and/or automatically shut down the information system. |
| **SI-13(4).1.3.4** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-13(4).1.3.1.a; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in SI-13(4).1.3.1.a to ensure that the standby information system components successfully and transparently assumes its role within the time period identified in SI-13(4).1.1.1. |
| **SI-13(4).1.3.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-13(4).1.3.1.b; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in SI-13(4).1.3.1.b to activate the alarm and/or automatically shut down the information system. |