| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AU-5** | RESPONSE TO AUDIT PROCESSING FAILURES | |
| **AU-5.1**  **AU-5.1.1**  **AU-5.1.2**  **AU-5.1.3**  **AU-5.1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines designated organizational officials to be alerted in the event of an audit processing failure;* 2. *the information system alerts designated organizational officials in the event of an audit processing failure;* 3. *the organization defines additional actions to be taken in the event of an audit processing failure; and* 4. *the information system takes the additional organization-defined actions in the event of an audit processing failure.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information system response to audit processing failures]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: AU-4, AU-6, AU-7, AU-11, AU-12, CM-6, SI-4  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. |
| **AU-5.1.1.1** | | **Examine** audit and accountability policy, procedures addressing response to audit processing failures, security plan, or other relevant documents; [*reviewing*] for the organizational officials (identified by name or job position) to be alerted in the event of an audit processing failure. |
|  | |  |
| **AU-5.1.2.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to alert the organization officials identified in AU-5.1.1.1 in the event of an audit processing failure. |
| **AU-5.1.2.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-5.1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-5.1.2.1. |
| **AU-5.1.2.3** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-5.1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended.  Note to assessor: This test must be coordinated with all responsible personnel associated with the information system. Testing of this nature may impose risk to the information system and, as such, the testing of any specific auditing mechanism should be carefully planned and executed. |
|  | |  |
| **AU-5.1.3.1** | | **Examine** audit and accountability policy, procedures addressing response to audit processing failures, security plan, or other relevant documents; [*reviewing*] for the additional actions to be taken in the event of an audit processing failure. |
|  | |  |
| **AU-5.1.4.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to initiate the additional actions identified in AU-5.1.3.1 in the event of an audit processing failure. |
| **AU-5.1.4.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-5.1.4.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-5.1.4.1. |
| **AU-5.1.4.3** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-5.1.4.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended.  Note to assessor: This test must be coordinated with all responsible personnel associated with the information system. Testing of this nature may impose risk to the information system and, as such, the testing of any specific auditing mechanism should be carefully planned and executed. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-5(1)** | RESPONSE TO AUDIT PROCESSING FAILURES |
| **AU-5(1).1**  **AU-5(1).1.1**  **AU-5(1).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the percentage of maximum audit record storage capacity that, if reached, requires a warning to be provided; and* 2. *the information system provides a warning when the allocated audit record storage volume reaches the organization-defined percentage of maximum audit record storage capacity.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing audit storage limit warnings]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: AU-4, AU-6, AU-7, AU-11, AU-12, CM-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-5(1).1.1.1** | **Examine** audit and accountability policy, procedures addressing response to audit processing failures, security plan, or other relevant documents; [*reviewing*] for the percentage threshold(s) of the maximum audit record storage capacity identified in AU-5.1.1.1for the information system that, if reached, requires a warning to be provided. |
|  |  |
| **AU-5(1).1.2.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to provide a warning when the allocated record storage volume reaches the organization percentage threshold(s) of maximum audit record storage capacity as identified in AU-5(1).1.1.1. |
| **AU-5(1).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-5(1).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-5(1).1.2.1. |
| **AU-5(1).1.2.3** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-5(1).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended.  Note to assessor: This test must be coordinated with all responsible personnel associated with the information system. Testing of this nature may impose risk to the information system and, as such, the testing of any specific auditing mechanism should be carefully planned and executed. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-5(2)** | RESPONSE TO AUDIT PROCESSING FAILURES |
| **AU-5(2).1**  **AU-5(2).1.1**  **AU-5(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines audit failure events requiring real-time alerts; and* 2. *the information system provides a real-time alert when organization-defined audit failure events occur.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing real time audit alerts when organization-defined audit failure events occur]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: AU-4, AU-6, AU-7, AU-11, AU-12, CM-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-5(2).1.1.1** | **Examine** audit and accountability policy, procedures addressing response to audit processing failures, security plan, or other relevant documents; [*reviewing*] for the audit failure events requiring real-time alerts. |
|  |  |
| **AU-5(2).1.2.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to provide a real-time alert when the audit failure events defined in AU-5(2).1.1.1 occur. |
| **AU-5(2).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic* ] sample of the automated mechanisms identified in AU-5(2).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-5(2).1.2.1. |
| **AU-5(2).1.2.3** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-5(2)1.2.1; conducting [*basic*] testing using an agreed-upon [*basic*] of the audit failure events identified in AU-5(2).1.1.1 for evidence that these mechanisms are operating as intended.  Note to assessor: This test must be coordinated with all responsible personnel associated with the information system. Testing of this nature may impose risk to the information system and, as such, the testing of any specific auditing mechanism should be carefully planned and executed. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-5(3)** | RESPONSE TO AUDIT PROCESSING FAILURES |
| **AU-5(3).1**  **AU-5(3).1.1**  **AU-5(3).1.2**  **AU-5(3).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic;* 2. *the organization defines if the network traffic above configurable traffic volume thresholds are rejected or delayed; and* 3. *the information system rejects or delays, as defined by the organization, network traffic generated above configurable traffic volume thresholds.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Information system capability implementing configurable traffic volume thresholds]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: AU-4, AU-6, AU-7, AU-11, AU-12, CM-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-5(3).1.1.1** | **Examine** procedures addressing response to audit processing failures, security plan, or other relevant documents; [*reviewing*] for the configurable traffic volume thresholds representing auditing capacity for network traffic. |
| **AU-5(3).1.1.2** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to enforce the traffic volume thresholds identified in AU-5(3)1.1.1. |
| **AU-5(3).1.1.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-5(3).1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-5(3).1.1.2. |
| **AU-5(3).1.1.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-5(3).1.1.2; conducting [*basic*] testing for evidence that these mechanisms are operating as intended.  Note to assessor: This test must be coordinated with all responsible personnel associated with the information system. Testing of this nature may impose risk to the information system and, as such, the testing of any specific auditing mechanism should be carefully planned and executed. |
|  |  |
| **AU-5(3).1.2.1** | **Examine** audit and accountability policy, procedures addressing response to audit processing failures, security plan, or other relevant documents; [*reviewing*] for the organization determination as to whether the network traffic generated above the configurable traffic volume thresholds identified in AU-5(3).1.1.1 should be rejected or delayed. |
|  |  |
| **AU-5(3).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 reject or delay, as determined by the organization in AU-5(3)1.2.1, network traffic generated above the traffic volume thresholds identified in AU-5(3).1.1.1. |
| **AU-5(3).1.3.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-5(3).1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-5(3).1.3.1. |
| **AU-5(3).1.3.3** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-5(3)1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended.  Note to assessor: This test must be coordinated with all responsible personnel associated with the information system. Testing of this nature may impose risk to the information system and, as such, the testing of any specific auditing mechanism should be carefully planned and executed. |
|  | |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-5(4)** | RESPONSE TO AUDIT PROCESSING FAILURES |
| **AU-5(4).1**  **AU-5(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Information system capability invoking system shutdown in the event of an audit failure]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: AU-4, AU-6, AU-7, AU-11, AU-12, CM-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-5(4).1.1.1** | **Examine** audit and accountability policy, procedures addressing response to audit processing failures, security plan, or other relevant documents; [*reviewing*] for the existence of an alternative audit capability to be invoked in the event of an audit failure from the primary audit capability. |
| **AU-5(4).1.1.2** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to invoke a system shutdown in the event of an audit failure, unless an alternative audit capability exists as determined in AU-5(4).1.1.1. |
| **AU-5(4).1.1.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-5(4).1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-5(4).1.1.2, unless an alternative audit capability exists as determined in AU-5(4).1.1.1. |
| **AU-5(4).1.1.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-5(4).1.1.2; conducting [*basic*] testing for evidence that these mechanisms are operating as intended, unless an alternative audit capability exists as determined in AU-5(4).1.1.1.  Note to assessor: This test must be coordinated with all responsible personnel associated with the information system. Testing of this nature may impose risk to the information system and, as such, the testing of any specific auditing mechanism should be carefully planned and executed. |