| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AU-3** | CONTENT OF AUDIT RECORDS | |
| **AU-3.1**  **AU-3.1.1**  **AU-3.1.1a**  **AU-3.1.1b**  **AU-3.1.1c**  **AU-3.1.1d**  **AU-3.1.1e**  **AU-3.1.1f** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system produces audit records that contain sufficient information to, at a minimum, establish:*   * *what type of event occurred;* * *when (date and time) the event occurred;* * *where the event occurred;* * *the source of the event;* * *the outcome (success or failure) of the event; and* * *the identity of any user/subject associated with the event.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information system auditing of auditable events]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2  concurrent controls: AU-8, AU-14, CM-6, SI-4  successor controls: AU-4, AU-5, AU-6, AU-7, AU-10, AU-11, AU-12 |
| **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-3.1.1.1**  **AU-3.1.1.1.a**  **AU-3.1.1.1.b**  **AU-3.1.1.1.c**  **AU-3.1.1.1.d**  **AU-3.1.1.1.e**  **AU-3.1.1.1.f** | | **Examine** audit and accountability policy, procedures addressing content of audit records, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to produce audit records that contain information to, at a minimum, establish:   * what type of event occurred; * when (date and time) the event occurred; * where the event occurred; * the source of the event; * the outcome (success or failure) of the event; and * the identity of any user/subject associated with the event. |
| **AU-3.1.1.2** | | **Examine** documentation describing the configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-3.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-3.1.1.1.a to establish what type of event occurred. |
| **AU-3.1.1.3** | | **Examine** documentation describing the configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-3.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-3.1.1.1.b to establish when (date and time) the event occurred. |
| **AU-3.1.1.4** | | **Examine** documentation describing the configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-3.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-3.1.1.1.c to establish where the event occurred. |
| **AU-3.1.1.5** | | **Examine** documentation describing the configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-3.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-3.1.1.1.d to establish the source of the event. |
| **AU-3.1.1.6** | | **Examine** documentation describing the configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-3.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-3.1.1.1.e to establish the outcome (success of failure) of the event. |
| **AU-3.1.1.7** | | **Examine** documentation describing the configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-3.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-3.1.1.1.f to establish the identity of any user/subject associated with the event. |
| **AU-3.1.1.8** | | **Examine** an agreed-upon [*basic*] sample of information system audit records; [*reviewing*] for evidence that the measures identified in AU-3.1.1.1.a are being applied to establish what type of event occurred. |
| **AU-3.1.1.9** | | **Examine** an agreed-upon [*basic*] sample of information system audit records; [*reviewing*] for evidence that the measures identified in AU-3.1.1.1.b are being applied to establish when (date and time) the event occurred. |
| **AU-3.1.1.10** | | **Examine** an agreed-upon [*basic*] sample of information system audit records; [*reviewing*] for evidence that the measures identified in AU-3.1.1.1.c are being applied to establish where the event occurred. |
| **AU-3.1.1.11** | | **Examine** an agreed-upon [*basic*] sample of information system audit records; [*reviewing*] for evidence that the measures identified in AU-3.1.1.1.d are being applied to establish the source of the event. |
| **AU-3.1.1.12** | | **Examine** an agreed-upon [*basic*] sample of information system audit records; [*reviewing*] for evidence that the measures identified in AU-3.1.1.1.e are being applied to establish the outcome (success or failure) of the event. |
| **AU-3.1.1.13** | | **Examine** an agreed-upon [*basic*] sample of information system audit records; [*reviewing*] for evidence that the measures identified in AU-3.1.1.1.f are being applied to establish the identity of any user/subject associated with the event. |
| **AU-3.1.1.14** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-3.1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in AU-3.1.1.1.a to establish what type of event occurred. |
| **AU-3.1.1.15** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-3.1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in AU-3.1.1.1.b to establish when (date and time) the event occurred. |
| **AU-3.1.1.16** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-3.1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in AU-3.1.1.1.c to establish where the event occurred. |
| **AU-3.1.1.17** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-3.1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in AU-3.1.1.1.d to establish the source of the event. |
| **AU-3.1.1.18** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-3.1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in AU-3.1.1.1.e to establish the outcome (success of failure) of the event. |
| **AU-3.1.1.19** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-3.1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in AU-3.1.1.1.f to establish the identity of any user/subject associated with the event. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-3(1)** | CONTENT OF AUDIT RECORDS |
| **AU-3(1).1**  **AU-3(1).1.1**  **AU-3(1).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the additional, more detailed information to be included in audit records for audit events identified by type, location, or subject; and* 2. *the information system includes the organization-defined additional, more detailed information in the audit records for audit events identified by type, location, or subject.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Information system audit capability to include more detailed information in audit records for audit events identified by type, location, or subject]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2  concurrent controls: AU-8, AU-14, CM-6, SI-4  successor controls: AU-4, AU-5, AU-6, AU-7, AU-10, AU-11, AU-12 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-3(1).1.1.1** | **Examine** audit and accountability policy, procedures addressing content of audit records, security plan, or other relevant documents; [*reviewing*] for additional, more detailed information to be included in audit records for audit events identified by type, location, or subject. |
|  |  |
| **AU-3(1).1.2.1** | **Examine** audit and accountability policy, procedures addressing content of audit records, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to include the detailed information identified in AU-3(1).1.1.1 in audit records for audit events identified by type, location, or subject. |
| **AU-3(1).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-3(1).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-3(1).1.2.1. |
| **AU-3(1).1.2.3** | **Examine** an agreed-upon [*basic*] sample of information system audit records; [*reviewing*] for evidence that the measures identified in AU-3(1).1.2.1 are being applied. |
| **AU-3(1).1.2.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-3(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)** | |
| **AU-3(2)** | CONTENT OF AUDIT RECORDS |
| **AU-3(2).1**  **AU-3(2).1.1**  **AU-3(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the information system components for which the content of audit records generated is centrally managed; and* 2. *the organization centrally manages the content of audit records generated by organization-defined information system components.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing content of audit records; information system design documentation; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing centralized management of audit record content]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2  concurrent controls: AU-8, AU-14, CM-6, SI-4  successor controls: AU-4, AU-5, AU-6, AU-7, AU-10, AU-11, AU-12 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-3(2).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the information system components whose audit record content is to be centrally managed. |
|  |  |
| **AU-3(2).1.2.2** | **Examine** audit and accountability policy, procedures addressing content of audit records, 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 centrally manage the content of audit records generated by the information system components identified in AU-3(2).1.1.1. |
| **AU-3(2).1.2.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-3(2).1.2.2; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-3(2).1.2.2. |
| **AU-3(2).1.2.4** | **Examine** the process identified in AU-3(2).1.2.2 to centrally manage the content of audit records generated by an agreed-upon [*basic*] sample of information system components identified in AU-3(2).1.1.1; reviewing for evidence that the process identified in AU-3(2).1.2.2 is being applied. |
| **AU-3(2).1.2.5** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-3(2).1.2.2; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |