| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AU-12** | AUDIT GENERATION | |
| **AU-12.1**  **AU-12.1.1**  **AU-12.1.2**  **AU-12.1.3**  **AU-12.1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the information system components that provide audit record generation capability for the list of auditable events defined in AU-2;* 2. *the information system provides audit record generation capability, at organization-defined information system components, for the list of auditable events defined in AU-2;* 3. *the information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and* 4. *the information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing audit record generation; security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system audit record generation responsibilities].  **Test**: [*select from:* Automated mechanisms implementing audit record generation capability]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: AU-4, AU-5, AU-6, AU-7, AU-11, 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-12.1.1.1** | | **Examine** procedures addressing audit record generation, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the information system components that provide audit record generation capability for the list of auditable events defined in AU-2.1.1.1. |
|  | |  |
| **AU-12.1.2.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed within the information system components identified in AU-12.1.1.1 to generate audit records for the list of auditable events identified in AU-2.1.1.1. |
| **AU-12.1.2.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-12.1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-12.1.2.1. |
| **AU-12.1.2.3** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-12.1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |  |
| **AU-12.1.3.1** | | **Examine** audit and accountability policy, procedures addressing audit record generation, security plan, or other relevant documents; [*reviewing*] for the organizational personnel (by name or role) designated to select which events are to be audited by the information system components identified in AU-12.1.1.1. |
| **AU-12.1.3.2** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to permit the organizational personnel identified in AU-12.1.3.1 to select the events to be audited by the information system components identified in AU-12.1.1.1. |
| **AU-12.1.3.3** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-12.1.3.2; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-12.1.3.2. |
| **AU-12.1.3.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel identified in AU-12.1.3.1; conducting [*basic*] discussions for evidence that the mechanisms and configurations identified in AU-12.1.3.2 are being applied. |
| **AU-12.1.3.5** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-12.1.3.2; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |  |
| **AU-12.1.4.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed within the information system components identified in AU-12.1.1.1 to generate audit records for the list of audited events identified in AU-2.1.4.1 with the content identified in AU-3.1.1. |
| **AU-12.1.4.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-12.1.4.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-12.1.4.1. |
| **AU-12.1.4.3** | | **Examine** an agreed-upon [*basic*] sample of information system audit records generated from an agreed-upon [*basic*] sample of the information system components identified in AU-12.1.1.1; [*reviewing*] for evidence that the mechanisms and configurations identified in AU-12.1.4.1 are being applied. |
| **AU-12.1.4.4** | | **Test** an agreed-upon [*basic* ] of the automated mechanisms and their configuration settings identified in AU-12.1.4.1; 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)** | |
| **AU-12(1)** | AUDIT GENERATION |
| **AU-12(1).1**  **AU-12(1).1.1**  **AU-12(1).1.2**  **AU-12(1).1.3**  **AU-12(1).1.4**  **AU-12(1).1.5** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the information system produces a system-wide (logical or physical) audit trail of information system audit records;* 2. *the organization defines the information system components from which audit records are to be compiled into the system-wide audit trail;* 3. *the information system compiles audit records from organization-defined information system components into the system-wide audit trail;* 4. *the organization defines the acceptable level of tolerance for relationship between time stamps of individual records in the system-wide audit trail; and* 5. *the system-wide audit trail is time-correlated to within the organization-defined level of tolerance to achieve a time ordering of audit records.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing audit record generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing audit record generation capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: AU-4, AU-5, AU-6, AU-7, AU-11, CM-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-12(1).1.1.1** | **Examine** audit and accountability policy, procedures addressing audit record generation, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the system-wide (logical or physical) audit trail of information system audit records. |
| **AU-12(1).1.1.2** | **Examine** system-wide audit trail identified in AU-12(1).1.1.1; [*reviewing*] for evidence of information system audit records. |
|  |  |
| **AU-12(1).1.2.1** | **Examine** audit and accountability policy, procedures addressing audit record generation, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the information system components from which audit records are to be compiled into the system-wide audit trail identified in AU-12(1).1.1.1. |
|  |  |
| **AU-12(1).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 compile audit records from the information system components identified in AU-12(1).1.2.1 into the system wide audit trail. |
| **AU-12(1).1.3.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-12(1).1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-12(1).1.3.1. |
| **AU-12(1).1.3.3** | **Examine** agreed-upon [*basic*] sample of information system audit records compiled in the system-wide audit trail identified in AU-12(1).1.1.1; [*reviewing*] for evidence that the mechanisms and configurations identified AU-12(1).1.3.1 are being applied to compile audit records from the information system components identified in AU-12(1).1.3.1 |
| **AU-12(1).1.3.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-12(1).1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **AU-12(1).1.4.1** | **Examine** audit and accountability policy, procedures addressing audit record generation, security plan, or other relevant documents; [*reviewing*] for the acceptable level of tolerance within which the information system should correlate audit events to achieve a time ordering of audit records for the system-wide audit trail identified in AU-12(1).1.1.1. |
| **AU-12(1).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 time-correlate the system-wide audit trail within the acceptable level of tolerance identified in AU-12(1).1.4.1. |
| **AU-12(1).1.5.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-12(1).1.5.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-12(1).1.5.1. |
| **AU-12(1).1.5.3** | **Examine** an agreed-upon [*basic*] sample of information system audit records compiled in the system-wide audit trail identified in AU-12(1).1.4.1; [*reviewing*] for evidence that the audit trail is time-correlated to within the level of tolerance identified in AU-12(1).1.4.1 |
| **AU-12(1).1.5.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-12(1).1.5.1; 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-12(2)** | AUDIT GENERATION |
| **AU-12(2).1**  **AU-12(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing audit record generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing audit record generation capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: AU-4, AU-5, AU-6, AU-7, AU-11, CM-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-12(2).1.1.1** | **Examine** audit and accountability policy, procedures addressing audit record generation, security plan, or other relevant documents; [*reviewing*] for the standard format to be employed when the information system produces audit records for the system-wide audit trail identified in AU-12(1).1.1.1. |
| **AU-12(2).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 produce audit records in the standard format identified in AU-12(2).1.1.1 for the system-wide audit trail. |
| **AU-12(2).1.1.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-12(2).1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-12(2).1.1.2. |
| **AU-12(2).1.1.4** | **Examine** an agreed-upon [*basic*] sample of information system audit records compiled in the system-wide audit trail identified in AU-12(2).1.1.1; [*reviewing*] for evidence that audit records are produced in the standard format identified in AU-12(2).1.1.1. |
| **AU-12(2).1.1.5** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-12(2).1.1.2; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |