| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AU-2** | AUDITABLE EVENTS | |
| **AU-2.1**  **AU-2.1.1**  **AU-2.1.2**  **AU-2.1.3**  **AU-2.1.4**  **AU-2.1.5** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the list of events the information system must be capable of auditing based on a risk assessment and mission/business needs;* 2. *the organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and help guide the selection of auditable events;* 3. *the organization provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents;* 4. *the organization defines the subset of auditable events defined in (i) that are to be audited within the information system and the frequency of (or situation requiring) auditing for each identified event; and* 5. *the organization determines, based on current threat information and ongoing assessment of risk, the subset of auditable events defined in (i) to be audited within the information system, and the frequency of (or situation requiring) auditing for each identified event .*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing auditable events; security plan; information system configuration settings and associated documentation; information system audit records; list of information system auditable events; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with auditing and accountability responsibilities].  **Test**: [*select from:* Automated mechanisms implementing information system auditing of organization-defined auditable events]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: RA-3  concurrent controls: CM-6, SI-4  successor controls: AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-10, AU-11, AU-12, AU-14 |
| **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-2.1.1.1** | | **Examine** audit and accountability policy, procedures addressing auditable events, security plan, or other relevant documents; [*reviewing*] for the list of events the information system must be capable of auditing. |
| **AU-2.1.1.2** | | **Examine** an agreed-upon [*basic*] sample of risk assessments for the information system; [*reviewing*] for evidence that risk assessments are used to determine the list of auditable events identified in AU-2.1.1.1. |
| **AU-2.1.1.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for determining the auditable events identified in AU-2.1.1.1; conducting [*basic*] discussions for evidence that these events are determined based on a risk assessment and mission/business needs. |
|  | |  |
| **AU-2.1.2.1** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with security audit responsibilities and other organizational entities requiring audit-related information; conducting [*basic*] discussions for evidence that the security audit function coordinates with other organizational entities requiring audit-related information to enhance mutual support and help guide the selection of auditable events. |
|  | |  |
| **AU-2.1.3.1** | | **Examine** audit and accountability policy, procedures addressing auditable events, security plan, or other relevant documents; [*reviewing*] for the rationale expressing why the list of auditable events identified in AU-2.1.1.1 is adequate to support after-the-fact investigations of security incidents. |
|  | |  |
| **AU-2.1.4.1** | | **Examine** audit and accountability policy, procedures addressing auditable events, security plan, or other relevant documents; [*reviewing*] for the subset of auditable events identified in AU-2.1.1.1 that are to be audited within the information system. |
| **AU-2.1.4.2** | | **Examine** audit and accountability policy, procedures addressing auditable events, security plan, or other relevant documents; [*reviewing*] for the frequency of (or situation requiring) auditing for the subset of auditable events identified in AU-2.1.4.1. |
|  | |  |
| **AU-2.1.5.1** | | **Examine** an agreed-upon [*basic*] sample of risk assessments for the information system; [*reviewing*] for evidence that current threat information and risk assessments are used to determine the subset of events to be audited as identified in AU-2.1.4.1 and the frequency of (or situation requiring) auditing as identified in AU-2.1.4.2. |
| **AU-2.1.5.2** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for determining events to be audited within the information system; conducting [*basic*] discussions for further evidence that current threat information and risk assessments are used to determine the subset of events to be audited as identified in AU-2.1.4.1 and the frequency of (or situation requiring) auditing as identified in AU-2.1.4.2. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **AU-2(1)** | | AUDITABLE EVENTS  [Withdrawn: Incorporated into AU-12]. |
| **AU-2(1).1** | | **ASSESSMENT OBJECTIVE:**  [Withdrawn: Incorporated into AU-12].  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  [Withdrawn: Incorporated into AU-12]. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-2(2)** | AUDITABLE EVENTS  [Withdrawn: Incorporated into AU-12]. |
| **AU-2(2).1** | **ASSESSMENT OBJECTIVE:**  [Withdrawn: Incorporated into AU-12].  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  [Withdrawn: Incorporated into AU-12]. |
|  | |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-2(3)** | AUDITABLE EVENTS |
| **AU-2(3).1**  **AU-2(3).1.1**  **AU-2(3).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the frequency of reviews and updates to the list of organization-defined auditable events; and* 2. *the organization reviews and updates the list of organization-defined auditable events in accordance with the organization-defined frequency.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing auditable events; security plan; list of organization-defined auditable events; auditable events review and update records; information system audit records; information system incident reports; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with auditing and accountability responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-2(3).1.1.1** | **Examine** audit and accountability policy, procedures addressing auditable events, security plan, or other relevant documents; [*reviewing*] for the frequency of reviews and updates to the list of auditable events identified in AU-2.1.1.1. |
|  |  |
| **AU-2(3).1.2.1** | **Examine** an agreed-upon [*basic*] sample of records of organizational reviews and updates to the list of auditable events identified in AU-2.1.1.1; [*reviewing*] for evidence that these events are reviewed and updated in accordance with the frequency identified in AU-2(3).1.1.1. |
| **AU-2(3).1.2.2** | **Interview** an agreed upon [*basic*] sample of organizational personnel responsible for reviewing and updating the auditable events identified in AU-2.1.1.1; conducting [*basic*] discussions for further evidence that these events are reviewed and updated in accordance with the frequency identified in AU-2(3).1.1.1. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-2(4)** | AUDITABLE EVENTS |
| **AU-2(4).1**  **AU-2(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization includes execution of privileged functions in the list of events to be audited by the information system.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing auditable events; information system configuration settings and associated documentation; list of organization-defined auditable events; list of privileged security functions; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-2(4).1.1.1** | **Examine** procedures addressing auditable events, security plan and referenced risk assessment(s), information system architecture and configuration documentation, information system design documentation, or other relevant documents; [*reviewing*] for the privileged functions to be audited by the information system. |
| **AU-2(4).1.1.2** | **Examine** list of events to be audited as identified in AU-2.1.4.1; [*reviewing*] for evidence of the privileged functions identified in AU-2(4).1.1.1. |
|  | |