| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AU-11** | AUDIT RECORD RETENTION | |
| **AU-11.1**  **AU-11.1.1**  **AU-11.1.2**  **AU-11.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the retention period for audit records;* 2. *the retention period for audit records is consistent with the records retention policy; and* 3. *the organization retains audit records for the organization-defined time period consistent with the records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing audit record retention; security plan; organization-defined retention period for audit records; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system audit record retention responsibilities]. | |
| **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-9, AU-12, CM-6, IR-4, IR-5, IR-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-11.1.1.1** | | **Examine** audit and accountability policy, procedures addressing audit record retention, security plan, or other relevant documents; [*reviewing*] for the retention period for audit records. |
|  | |  |
| **AU-11.1.2.1** | | **Examine** organization’s records retention policy; [*reviewing*] for the records retention period and for evidence that this period is consistent with the retention period identified in AU-11.1.1.1 for audit records. |
|  | |  |
| **AU-11.1.3.1** | | **Examine** audit and accountability policy, procedures addressing audit record retention, security plan, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to retain audit records in accordance with the frequency identified in AU-11.1.1.1 |
| **AU-11.1.3.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-11.1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-11.1.3.1. |
| **AU-11.1.3.3** | | **Examine** information system audit records for an agreed-upon [*basic*] sample of audit logs retained for the information system; [*reviewing*] for evidence that the mechanisms and configurations identified in AU-11.1.3.1 are being applied. |
| **AU-11.1.3.4** | | **Interview** an agreed-upon [*basic*] of sample organizational personnel responsible for audit record retention; conducting [*basic*] discussions for evidence that information system audit records are retained in accordance with the time period identified in AU-11.1.1.1 to support after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. |