| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AU-9** | PROTECTION OF AUDIT INFORMATION | |
| **AU-9.1**  **AU-9.1.1**  **AU-9.1.1a**  **AU-9.1.1b**  **AU-9.1.1c** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system protects audit information and audit tools from unauthorized:*   * *access;* * *modification; and* * *deletion.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; audit tools; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing audit information protection]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, AC-6, AU-11, CM-6  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-9.1.1.1**  **AU-9.1.1.1.a**  **AU-9.1.1.1.b**  **AU-9.1.1.1.c** | | **Examine** security plan, information system design documentation, and other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to protect audit information and audit tools from unauthorized:   * access; * modification; and * deletion. |
| **AU-9.1.1.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic* ] sample of the automated mechanisms identified in AU-9.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-9.1.1.1.a to protect audit information and audit tools from unauthorized access. |
| **AU-9.1.1.3** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-9.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-9.1.1.1.b to protect audit information and audit tools from unauthorized modification. |
| **AU-9.1.1.4** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-9.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-9.1.1.1.c to protect audit information and audit tools from unauthorized deletion. |
| **AU-9.1.1.5** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-9.1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in AU-9.1.1.1.a to protect audit information and audit tools from unauthorized access. |
| **AU-9.1.1.6** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-9.1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in AU-9.1.1.1.b to protect audit information and audit tools from unauthorized modification. |
| **AU-9.1.1.7** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-9.1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in AU-9.1.1.1.c to protect audit information and audit tools from unauthorized deletion. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-9(1)** | PROTECTION OF AUDIT INFORMATION |
| **AU-9(1).1**  **AU-9(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system produces audit records on hardware-enforced, write-once media.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system hardware settings; information system configuration settings and associated documentation, information system audit records; other relevant documents or records].  **Test**: [*select from:* Media storage devices to hold audit records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, AC-6, AU-11, CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-9(1).1.1.1** | **Examine** procedures addressing protection of audit information, security plan, information system design documentation, and other relevant documents; [*reviewing*] for the hardware-enforced, write-once media to be used to store audit information. |
| **AU-9(1).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 on the media identified in AU-9(1).1.1.1. |
| **AU-9(1).1.1.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-9(1).1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-9(1).1.1.2 |
| **AU-9(1).1.1.4** | **Examine** information system audit records produced on an agreed-upon [*basic*] sample of the media identified in AU-9(1).1.1.1; [*reviewing*] for evidence that the mechanisms and configurations identified in AU-9(1).1.1.2 are being applied. |
| **AU-9(1).1.1.5** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-9(1).1.1.2 using an agreed-upon [*basic*] sample of the media identified in AU-9(1).1.1.1; conducting [*basic*] testing for evidence that audit information is produced on hardware-enforced, write-once media. |
| **AU-9(1).1.1.6** | **Test** an agreed-upon [*basic*] sample of the media identified in AU-9(1).1.1.5; conducting [*basic*] testing for further evidence that the media is hardware-enforced, write-once. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-9(2)** | PROTECTION OF AUDIT INFORMATION |
| **AU-9(2).1**  **AU-9(2).1.1**  **AU-9(2).1.2**  **AU-9(2).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the system or media for storing back up audit records that is a different system or media than the system being audited;* 2. *the organization defines the frequency of information system backups of audit records; and* 3. *the information system backs up audit records, in accordance with the organization-defined frequency, onto organization-defined system or media.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing protection of audit information; security plan; information system design documentation; information system configuration settings and associated documentation, system or media storing backups of information system audit records; information system audit records; 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: AU-11, CM-6, CP-9, CP-10  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-9(2).1.1.1** | **Examine** audit and accountability policy, procedures addressing protection of audit information, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the system or media storing back up audit records and for evidence that this system or media is different from the system being audited. |
|  |  |
| **AU-9(2).1.2.1** | **Examine** audit and accountability policy, procedures addressing protection of audit information, security plan, or other relevant documents; [*reviewing*] for the frequency of information system backups of audit records. |
|  |  |
| **AU-9(2).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 backup audit records in accordance with the frequency identified in AU-9(2).1.2.1 and onto the system or media identified in AU-9(2).1.1.1. |
| **AU-9(2).1.3.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-9(2).1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-9(2).1.3.1 |
| **AU-9(2).1.3.3** | **Examine** an agreed-upon [*basic*] sample of information system backups of audit records stored on the system or media identified in AU-9(2).1.1.1; [*reviewing*] for evidence that the mechanisms and configurations identified in AU-9(2).1.3.1 are being applied. |
| **AU-9(2).1.3.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for conducting audit record backups on the system or media identified in AU-9(2).1.1.1; conducting [*basic*] discussions for further evidence that the mechanisms and configurations identified in AU-9(2).1.3.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-9(3)** | PROTECTION OF AUDIT INFORMATION |
| **AU-9(3).1**  **AU-9(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system uses cryptographic mechanisms to protect the integrity of audit information and audit tools.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system hardware settings; information system configuration settings and associated documentation, information system audit records; 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: AC-3, AU-11, CM-6, SC-13  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-9(3).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [reviewing] for the cryptographic mechanisms and their configuration settings to be employed to protect the integrity of audit information and audit tools. |
| **AU-9(3).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the cryptographic mechanisms identified in AU-9(3).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-9(3).1.1.1. |
| **AU-9(3).1.1.3** | **Test** an agreed-upon [*basic*] sample of the cryptographic mechanisms and their configuration settings identified in AU-9(3).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-9(4)** | PROTECTION OF AUDIT INFORMATION |
| **AU-9(4).1**  **AU-9(4).1.1**  **AU-9(4).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if :*   1. *the organization authorizes access to management of audit functionality to only a limited subset of privileged users; and* 2. *the organization protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; 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 auditing and accountability responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, AC-6, AU-11, CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-9(4).1.1.1** | **Examine** audit and accountability policy, procedures addressing protection of audit information, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the subset of privileged users (by name, position, or role) to be authorized access to manage audit functions for the information system. |
| **AU-9(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 authorize access for managing audit functions to only the privileged users identified in AU-9(4).1.1.1. |
| **AU-9(4).1.1.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-9(4).1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-9(4).1.1.2. |
| **AU-9(4).1.1.4** | **Examine** access authorizations for an agreed-upon [*basic*] sample of user accounts configured to manage audit functions for the information system; [*reviewing*] for evidence that access to audit management functions is authorized and limited to the privileged users identified in AU-9(4).1.1.1. |
| **AU-9(4).1.1.5** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for authorizing access to audit management functions for the information system; conducting [*basic*] discussions for further evidence that the mechanisms and configurations identified in AU-9(4).1.1.2 are being applied. |
|  |  |
| **AU-9(4).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 protect the audit records of non-local accesses to privileged accounts and the execution of privileged functions. |
| **AU-9(4).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-9(4).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-9(4).1.2.1. |
| **AU-9(4).1.2.3** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-9(4).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |