| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AU-10** | NON-REPUDIATION | |
| **AU-10.1**  **AU-10.1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system protects against an individual falsely denying having performed a particular action.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing non-repudiation; 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 non-repudiation capability]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: CM-6, SC-8, SC-12, SC-13  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-10.1.1.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the user actions for that require non-repudiation and for the automated mechanisms and their configuration settings to be employed to protect against an individual falsely denying having performed a particular action. |
| **AU-10.1.1.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-10.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-10.1.1.1. |
| **AU-10.1.1.3** | | **Examine** information system audit records for an agreed-upon [*basic*] sample of the user actions identified in AU-10.1.1.1; [*reviewing*] for evidence that the mechanisms and configurations identified in AU-10.1.1.1 are being applied. |
| **AU-10.1.1.4** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-10.1.1.1; 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-10(1)** | NON-REPUDIATION |
| **AU-10(1).1**  **AU-10(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system associates the identity of the information producer with the information.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing non-repudiation; 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 non-repudiation capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: CM-6, SC-8, SC-12, SC-13  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-10(1).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to associate the identity of the information producer with the information. |
| **AU-10(1).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic* ] sample of the automated mechanisms identified in AU-10(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-10(1).1.1.1. |
| **AU-10(1).1.1.3** | **Examine** information system audit records for an agreed-upon [*basic*] sample of the user actions identified in AU-10.1.1.1; [*reviewing*] for evidence that the mechanisms and configurations identified in AU-10(1).1.1.1 are being applied. |
| **AU-10(1).1.1.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-10(1).1.1.1; 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-10(2)** | NON-REPUDIATION |
| **AU-10(2).1**  **AU-10(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system validates the binding of the information producer’s identity to the information.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing non-repudiation; 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 non-repudiation capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: CM-6, SC-8, SC-12, SC-13  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-10(2).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to validate the binding of the information producer’s identity to the information. |
| **AU-10(2).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-10(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-10(2).1.1.1. |
| **AU-10(2).1.1.3** | **Examine** information system audit records for an agreed-upon [*basic*] sample of the user actions identified in AU-10.1.1.1; [*reviewing*] for evidence that the mechanisms and configurations identified in AU-10(2).1.1.1 are being applied. |
| **AU-10(2).1.1.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-10(2).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-10(3)** | NON-REPUDIATION |
| **AU-10(3).1**  **AU-10(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing non-repudiation; 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 non-repudiation capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: CM-6, SC-8, SC-12, SC-13  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-10(3).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to maintain the identity and credentials of a reviewer/releaser within the established chain of custody for all information reviewed or released. |
| **AU-10(3).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic* ] sample of the automated mechanisms identified in AU-10(3).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-10(3).1.1.1. |
| **AU-10(3).1.1.3** | **Examine** information system audit records for an agreed-upon [*basic*] sample of the user actions identified in AU-10.1.1.1; [*reviewing*] for evidence that the mechanisms and configurations identified in AU-10(3).1.1.1 are being applied. |
| **AU-10(3).1.1.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-10(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-10(4)** | NON-REPUDIATION |
| **AU-10(4).1**  **AU-10(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system validates the binding of the reviewer’s identity to the information at the transfer/release point prior to release/transfer from one security domain to another security domain.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing non-repudiation; 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 non-repudiation capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: CM-6, SC-8, SC-12, SC-13  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-10(4).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to validate the binding of the reviewer’s identity to the information at the transfer/release point prior to releasing/transferring the information from one security domain to another security domain. |
| **AU-10(4).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] of the automated mechanisms identified in AU-10(4).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-10(4).1.1.1. |
| **AU-10(4).1.1.3** | **Examine** information system audit records for an agreed-upon [*basic*] sample of the user actions identified in AU-10.1.1.1; [*reviewing*] for evidence that the mechanisms and configurations identified in AU-10(4).1.1.1 are being applied. |
| **AU-10(4).1.1.4** | **Test** an agreed-upon [*basic*] of the automated mechanisms and their configuration settings identified in AU-10(4).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-10(5)** | NON-REPUDIATION |
| **AU-10(5).1**  **AU-10(5).1.1**  **AU-10(5).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines whether FIPS-validated or NSA-approved cryptography is employed to implement digital signatures; and* 2. *the organization employs the organization-defined cryptography to implement digital signatures.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing non-repudiation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Cryptographic mechanisms implementing digital signature capability within the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: CM-6, SC-8, SC-12, SC-13  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-10(5).1.1.1** | **Examine** audit and accountability policy, procedures addressing non-repudiation, security plan, or other relevant documents; [*reviewing*] for the cryptography (FIPS-validated or NSA-approved) to be employed to implement digital signatures. |
|  |  |
| **AU-10(5).1.2.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for cryptographic mechanisms and their configuration settings to be employed to implement digital signatures using the cryptography identified in AU-10(5).1.1.1. |
| **AU-10(5).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the cryptographic mechanisms identified in AU-10(5).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-10(5).1.2.1. |
| **AU-10(5).1.2.3** | **Examine** an agreed-upon [*basic*] sample of email records, information system audit records, or other relevant information system records for an agreed-upon [*basic*] sample of the user actions identified in AU-10.1.1 that require digital signatures; [*reviewing*] for evidence that the mechanisms and configurations identified in AU-10(5).1.2.1 are being applied. |
| **AU-10(5).1.2.4** | **Test** an agreed-upon [*basic*] sample of the cryptographic mechanisms and their configuration settings identified in AU-10(5).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |