| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SC-23** | SESSION AUTHENTICITY | |
| **SC-23.1**  **SC-23.1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system provides mechanisms to protect the authenticity of communications sessions.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing session authenticity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing session authenticity]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-8, SC-11  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. |
| **SC-23.1.1.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to protect the authenticity of communications sessions. |
| **SC-23.1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-23.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-23.1.1.1. |
| **SC-23.1.1.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-23.1.1.1; 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)** | |
| **SC-23(1)** | SESSION AUTHENTICITY |
| **SC-23(1).1**  **SC-23(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system invalidates session identifiers upon user logout or other session termination.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing session authenticity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing session identifier invalidation upon session termination]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-8, SC-11  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-23(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 invalidate session identifiers upon user logout or other session termination. |
| **SC-23(1).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-23(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-23(1).1.1.1. |
| **SC-23(1).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-23(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)** | |
| **SC-23(2)** | SESSION AUTHENTICITY |
| **SC-23(2).1**  **SC-23(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system provides a readily observable logout capability whenever authentication is used to gain access to Web pages.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing session authenticity; information system design documentation; information system configuration settings and associated documentation; information system site designs; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing logout capability for Web pages requiring user authentication]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-8, SC-11  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-23(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 provide a readily observable logout capability whenever authentication is used to gain access to Web pages. |
| **SC-23(2).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-23(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-23(2).1.1.1. |
| **SC-23(2).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-23(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)** | |
| **SC-23(3)** | SESSION AUTHENTICITY |
| **SC-23(3).1**  **SC-23(3).1.1**  **SC-23(3).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the information system generates a unique session identifier for each session; and* 2. *the information system recognizes only session identifiers that are system-generated.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing session authenticity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms generating and monitoring unique session identifiers]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-8, SC-11  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-23(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 generate a unique session identifier for each session. |
| **SC-23(3).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-23(3).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-23(3).1.1.1. |
| **SC-23(3).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-23(3).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **SC-23(3).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 recognize only session identifiers that are system-generated. |
| **SC-23(3).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-23(3).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-23(3).1.2.1. |
| **SC-23(3).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-23(3).1.2.1; 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)** | |
| **SC-23(4)** | SESSION AUTHENTICITY |
| **SC-23(4).1**  **SC-23(4).1.1**  **SC-23(4).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines requirements for randomly generating unique session identifiers; and* 2. *the information system generates unique session identifiers in accordance with organization-defined randomness requirements.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing session authenticity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms generating unique session identifiers]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-8, SC-11  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-23(4).1.1.1** | **Examine** system and communications protection policy, access control policy, procedures addressing session authenticity, security plan, or other relevant documents; [*reviewing*] for the requirements for randomly generating unique session identifiers. |
|  |  |
| **SC-23(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 generate unique session identifiers in accordance with the requirements identified in SC-23(4).1.1.1. |
| **SC-23(4).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-23(4).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-23(4).1.2.1. |
| **SC-23(4).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-23(4).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |