| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AC-11** | SESSION LOCK | |
| **AC-11.1**  **AC-11.1.1**  **AC-11.1.2**  **AC-11.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the time period of user inactivity after which the information system initiates a session lock;* 2. *the information system initiates a session lock after the organization-defined time period of inactivity or upon receiving a request from a user;* 3. *the information system retains the session lock until the user reestablishes access using established identification and authentication procedures.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; security plan; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing the access control policy for session lock]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-2, CM-6, IA-2, IA-8  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. |
| **AC-11.1.1.1** | | **Examine** access control policy, procedures addressing session lock, security plan, or other relevant documents; [*reviewing*] for the time period of user inactivity after which the information system initiates a session lock. |
|  | |  |
| **AC-11.1.2.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to initiate a session lock after the time period of inactivity identified in AC-11.1.1.1, or upon receiving a request from a user. |
| **AC-11.1.2.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-11.1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-11.1.2.1. |
| **AC-11.1.2.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-11.1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |  |
| **AC-11.1.3.1** | | **Examine** identification and authentication procedures; [*reviewing*] for the procedures established for users to reestablish access to the information system when the information system initiates a session lock after the time period of inactivity identified in AC-11.1.1.1, or upon receiving a request from a user. |
| **AC-11.1.3.2** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to retain the session lock until the user reestablishes access using the established identification and authentication procedures identified in AC-11.1.3.1. |
| **AC-11.1.3.3** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-11.1.3.2; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-11.1.3.2. |
| **AC-11.1.3.4** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-11.1.3.2; 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)** | | |
| **AC-11(1)** | | SESSION LOCK |
| **AC-11(1).1**  **AC-11(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing session lock; display screen with session lock activated; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Information system session lock mechanisms]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **AC-11(1).1.1.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the information system session lock mechanisms and their configuration settings to be employed that, when activated on a device with a display screen, places a publicly viewable pattern onto the display screen, hiding what was previously visible on the screen. |
| **AC-11(1).1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-11(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-11(1).1.1.1. |
| **AC-11(1).1.1.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-11(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |