| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AC-7** | UNSUCCESSFUL LOGIN ATTEMPTS | |
| **AC-7.1**  **AC-7.1.1**  **AC-7.1.2**  **AC-7.1.3**  **AC-7.1.3a**  **AC-7.1.3b**  **AC-7.1.3c**  **AC-7.1.4**  **AC-7.1.5** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the maximum number of consecutive invalid login attempts to the information system by a user and the time period in which the consecutive invalid attempts occur;* 2. *the information system enforces the organization-defined limit of consecutive invalid login attempts by a user during the organization-defined time period;* 3. *the organization defines action to be taken by the system when the maximum number of unsuccessful login attempts is exceeded as:*  * *lock out the account/node for a specified time period;* * *lock out the account/note until released by an administrator; or* * *delay the next login prompt according to organization-defined delay algorithm;*  1. *the information system either automatically locks the account/node for the organization-defined time period, locks the account/node until released by an administrator, or delays next login prompt for the organization-defined delay period when the maximum number of unsuccessful login attempts is exceeded; and* 2. *the information system performs the organization-defined actions when the maximum number of unsuccessful login attempts is exceeded regardless of whether the login occurs via a local or network connection.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing unsuccessful login attempts; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing the access control policy for unsuccessful login attempts]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IA-2, IA-3, IA-5, IA-8  concurrent controls: IA-6, 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. |
| **AC-7.1.1.1** | | **Examine** access control policy, procedures addressing unsuccessful login attempts, security plan, or other relevant documents; [*reviewing*] for the maximum number of consecutive invalid login attempts to the information system by a user and the time period in which the consecutive invalid attempts occur. |
|  | |  |
| **AC-7.1.2.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to enforce the limit of consecutive invalid login attempts identified in AC-7.1.1.1 during the time period identified in AC-7.1.1.1. |
| **AC-7.1.2.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-7.1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-7.1.2.1. |
| **AC-7.1.2.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-7.1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |  |
| **AC-7.1.3.1**  **AC-7.1.3.1.a**  **AC-7.1.3.1.b**  **AC-7.1.3.1.c** | | **Examine** access control policy, procedures addressing unsuccessful login attempts, security plan, or other relevant documents; [*reviewing*] for one of the following selected actions to be taken by the system when the maximum number of unsuccessful login attempts is exceeded:   * lock out the account/node for a specified time period; * lock out the account/note until released by an administrator; or * delay the next login prompt according to organization-defined delay algorithm; |
|  | |  |
| **AC-7.1.4.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to enforce the action defined in AC-7.1.3.1 when the maximum number of unsuccessful login attempts is exceeded. |
| **AC-7.1.4.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-7.1.4.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-7.1.4.1. |
| **AC-7.1.4.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-7.1.4.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |  |
| **AC-7.1.5.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to enforce the action defined in AC-7.1.3.1 when the maximum number of unsuccessful login attempts is exceeded for local and network logins. |
| **AC-7.1.5.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-7.1.5.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-7.1.5.1. |
| **AC-7.1.5.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-7.1.5.1; 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)** | | |
| **AC-7(1)** | | UNSUCCESSFUL LOGIN ATTEMPTS |
| **AC-7(1).1**  **AC-7(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful login attempts is exceeded.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing unsuccessful login attempts; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing the access control policy for unsuccessful login attempts]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IA-2, IA-3, IA-5, IA-8  concurrent controls: IA-6, CM-6  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **AC-7(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 lock the account/node until released by an administrator when the maximum number of unsuccessful login attempts identified in AC-7.1.1.1 is exceeded. |
| **AC-7(1).1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-7(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-7(1).1.1.1. |
| **AC-7(1).1.1.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-7(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)** | |
| **AC-7(2)** | UNSUCCESSFUL LOGIN ATTEMPTS |
| **AC-7(2).1**  **AC-7(2).1.1**  **AC-7(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the number of consecutive, unsuccessful login attempts allowed for accessing a mobile device before the information system purges information from the device; and* 2. *the information system provides protection for mobile devices accessed via login by purging information from such devices after the organization-defined number of consecutive, unsuccessful login attempts to the device is exceeded.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing unsuccessful login attempts on mobile devices; 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 the access control policy for unsuccessful login attempts]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IA-2, IA-3, IA-5  concurrent controls: IA-6, AC-19, CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-7(2).1.1.1** | **Examine** access control policy, procedures addressing unsuccessful login attempts, security plan, or other relevant documents; [*reviewing*] for the number of consecutive, unsuccessful login attempts allowed for accessing a mobile device before the system purges information from the device. |
|  |  |
| **AC-7(2).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 purge information from mobile devices after the number of consecutive, unsuccessful login attempts identified in AC-7(2).1.1.1 is exceeded. |
| **AC-7(2).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-7(2).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-7(2).1.2.1. |
| **AC-7(2).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-7(2).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |