| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AC-9** | PREVIOUS LOGON (ACCESS) NOTIFICATION | |
| **AC-9.1**  **AC-9.1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system, upon successful user logon (access), displays to the user the date and time of the last logon (access).*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing previous logon notification; information system configuration settings and associated documentation; information system notification messages; information system design documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing the access control policy for previous logon notification]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: 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-9.1.1.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to display the data and time of the last logon upon successful user logon. |
| **AC-9.1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-9.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-9.1.1.1. |
| **AC-9.1.1.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-9.1.1.1; 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)** | |
| **AC-9(1)** | PREVIOUS LOGON (ACCESS) NOTIFICATION |
| **AC-9(1).1**  **AC-9(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system, upon successful user logon/access, displays to the user the number of unsuccessful logon/access attempts since the last successful logon/access.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing previous logon notification; 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 previous logon notification]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-7  concurrent controls: CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-9(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, upon successful user logon, display the number of unsuccessful logon/access attempts since the last successful logon/access. |
| **AC-9(1).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-9(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-9(1).1.1.1. |
| **AC-9(1).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-9(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-9(2)** | PREVIOUS LOGON (ACCESS) NOTIFICATION |
| **AC-9(2).1**  **AC-9(2).1.1**  **AC-9(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the time period during which the number of successful logins/accesses and/or unsuccessful user login/access attempts occurs; and* 2. *the information system notifies the user of the number of successful logins/accesses and/or unsuccessful login/access attempts that occur during the organization-defined time period.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing previous logon notification; 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 previous logon notification]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-7  concurrent controls: CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-9(2).1.1.1** | **Examine** access control policy, procedures addressing previous logon notification, security plan, or other relevant documents; [*reviewing*] for the time period during which the number of successful logins/accesses and/or unsuccessful user login/access attempts occurs. |
|  |  |
| **AC-9(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 notify the user of the number of successful logins/accesses and/or unsuccessful login/access attempts that occur during the time period identified in AC-9(2).1.1.1. |
| **AC-9(2).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-9(2).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-9(2).1.2.1. |
| **AC-9(2).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-9(2).1.2.1; 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)** | |
| **AC-9(3)** | PREVIOUS LOGON (ACCESS) NOTIFICATION |
| **AC-9(3).1**  **AC-9(3).1.1**  **AC-9(3).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the time period for which security-related changes to the user’s account occur; and* 2. *the information system notifies the user of the organization-defined security-related changes to the user’s account that occur during the organization-defined time period.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing previous logon notification; 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 previous logon notification]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3  concurrent controls: CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-9(3).1.1.1** | **Examine** access control policy, procedures addressing previous logon notification, security plan, or other relevant documents; [*reviewing*] for the time period for which security-related changes to the user’s account occur. |
|  |  |
| **AC-9(3).1.2.1** | **Examine** access control policy, procedures addressing previous logon notification, security plan, or other relevant documents; [*reviewing*] for the types of security-related changes to the user’s account that are to be monitored by the organization. |
| **AC-9(3).1.2.2** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to notify the user of the types of security-related changes identified in AC-9(3).1.2.1 to the user’s account that occur during the time period identified in AC-9(3).1.1.1. |
| **AC-9(3).1.2.3** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-9(3).1.2.2; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-9(3).1.2.2. |
| **AC-9(3).1.2.4** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-9(3).1.2.2; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |