| **assessment case** | | |
| --- | --- | --- |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| ASSESSMENT – Base Control, Part 1of 1 | | |
| **AC-2** | ACCOUNT MANAGEMENT | |
| **AC-2.1**  **AC-2.1.1**  AC-2.1.1a  AC-2.1.1b  AC-2.1.1c  AC-2.1.1d  AC-2.1.1e  AC-2.1.1f  AC-2.1.1g  AC-2.1.1h  AC-2.1.1i  **AC-2.1.2**  **AC-2.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization manages information system accounts, including;*    * *identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);*    * *establishing conditions for group membership;*    * *identifying authorized users of the information system and specifying access privileges;*    * *requiring appropriate approvals for requests to establish accounts;*    * *establishing, activating, modifying, disabling, and removing accounts;*    * *specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;*    * *notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;*    * *deactivating: i) temporary accounts that are no longer required; and ii) accounts of terminated or transferred users; and*    * *granting access to the system based on:*  * *a valid access authorization;* * *intended system usage; and* * *other attributes as required by the organization or associated missions/business functions; and*  1. *the organization defines the frequency of information system account reviews; and* 2. *the organization reviews information system accounts in accordance with organization-defined frequency.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing account management; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest/anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with account management responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PL-2  concurrent controls: IA-2, IA-4, IA-5, CM-6  successor controls: AC-3, AC-4, AC-5, AC-6, AC-7, AC-9, AC10, AC-13 |
| **Action Steps** | | **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-2.1.1.1**  **AC-2.1.1.1.a**  **AC-2.1.1.1.b**  **AC-2.1.1.1.c**  **AC-2.1.1.1.d**  **AC-2.1.1.1.e**  **AC-2.1.1.1.f**  **AC-2.1.1.1.g**  **AC-2.1.1.1.h**  **AC-2.1.1.1.i** | | **Examine** access control policy, account management procedures, security plan, or other relevant documents; [*reviewing*] for the measures to be employed in managing information system accounts, including:   * + identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);   + establishing conditions for group membership;   + identifying authorized users of the information system and specifying access privileges;   + requiring appropriate approvals for requests to establish accounts;   + establishing, activating, modifying, disabling, and removing accounts;   + specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;   + notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;   + deactivating: i) temporary accounts that are no longer required; and ii) accounts of terminated or transferred users; and   + granting access to the system based on: * a valid access authorization; * intended system usage; and * other attributes as required by the organization or associated missions/business functions. |
| **AC-2.1.1.2** | | **Examine** an agreed-upon [*basic*] sample of records of account management actions for an agreed-upon [*basic*] sample of active information system accounts; [*reviewing*] for evidence that the measures identified in AC-2.1.1.1.a are being applied to identify system account types. |
| **AC-2.1.1.3** | | **Examine** an agreed-upon [*basic*] sample of records of active group accounts, along with the name of the individual associated with each account; [*reviewing*] for evidence that the measures identified in AC-2.1.1.1.b are being applied to establish conditions for group membership. |
| **AC-2.1.1.4** | | **Examine** records of user access authorizations and associated privileges for an agreed-upon [*basic*] sample of employees with active information system accounts; [*reviewing*] for evidence that the measures identified in AC-2.1.1.1.c are being applied to identify authorized users of the information system and specify access privileges. |
| **AC-2.1.1.5** | | **Examine** records of user access approvals and authorizations for an agreed-upon [*basic*] sample of system accounts, along with the name of the individual associated with each account; [*reviewing*] for evidence that the measures identified in AC-2.1.1.1.d are being applied to require appropriate approvals for requests to establish information system accounts. |
| **AC-2.1.1.6** | | **Examine** an agreed-upon [*basic*] sample of records of account maintenance actions for an agreed-upon [*basic*] sample of active information system accounts, along with the name of the individual associated with each account; [*reviewing*] for evidence that the measures identified in AC-2.1.1.1.e are being applied to establish, activate, or modify information system accounts. |
| **AC-2.1.1.7** | | **Examine** records of account disabling or removal actions for information system accounts associated with an agreed-upon [*basic*] sample of recently transferred, separated, or terminated employees; [*reviewing*] for evidence that the measures identified in AC-2.1.1.1.e are being applied to disable and remove information system accounts as appropriate. |
| **AC-2.1.1.8** | | **Examine** an agreed-upon [*basic*] sample of records of authorizing or monitoring actions associated with the use of an agreed-upon [*basic*] sample of guest/anonymous or temporary accounts; [*reviewing*] for evidence that the measures identified in AC-2.1.1.1.f are being applied to specifically authorize and monitor the use of guest/anonymous and temporary accounts. |
| **AC-2.1.1.9** | | **Examine** an agreed-upon [*basic*] sample of records associated with the process for notifying account managers when temporary accounts are no longer required; [*reviewing*] for evidence that the measures identified in AC-2.1.1.1.g are being applied to notify account managers when temporary accounts are no longer required.. |
| **AC-2.1.1.10** | | **Examine** an agreed-upon [*basic*] sample of records associated with the process for notifying account managers when information system users are terminated or transferred; [*reviewing*] for evidence that the measures identified in AC-2.1.1.1.g are being applied to notify account managers when information system users are terminated or transferred. |
| **AC-2.1.1.11** | | **Examine** an agreed-upon [*basic*] sample of records associated with the process for notifying account managers when information system usage, need-to-know, or need-to-share changes; [*reviewing*] for evidence that the measures identified in AC-2.1.1.1.g are being applied to notify account managers when information system usage or need-to-know/need-to-share changes. |
| **AC-2.1.1.12** | | **Examine** an agreed-upon [*basic*] sample of records associated with the process for deactivating temporary accounts; [*reviewing*] for evidence that the measures identified in AC-2.1.1.1.h are being applied to deactivate temporary accounts that are no longer required. |
| **AC-2.1.1.13** | | **Examine** an agreed-upon [*basic*] sample of records associated with the process for deactivating accounts of terminated or transferred employees; [reviewing] for evidence that the measures identified in AC-2.1.1.1.h are being applied to deactivate accounts of terminated or transferred users. |
| **AC-2.1.1.14** | | **Examine** an agreed-upon [*basic*] sample of records associated with the process for granting access to the information system based on valid access authorization, intended system usage, other organizational attributes or associated missions/business functions; [*reviewing*] for evidence that the measures identified in AC-2.1.1.1.i are being applied. |
| **AC-2.1.1.15** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with account management responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in AC-2.1.1.1.a are being applied to identify account types. |
| **AC-2.1.1.16** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with account management responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in AC-2.1.1.1.a are being applied to identify account types. |
| **AC-2.1.1.17** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with account management responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in AC-2.1.1.1.b are being applied to establish conditions for group membership. |
| **AC-2.1.1.18** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with account management responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in AC-2.1.1.1.c are being applied to identify authorized users of the information system and specify access privileges. |
| **AC-2.1.1.19** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with account management responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in AC-2.1.1.1.d are being applied to require appropriate approvals for requests to establish accounts. |
| **AC-2.1.1.20** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with account management responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in AC-2.1.1.1.a are being applied to identify account types. |
| **AC-2.1.1.21** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with account management responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in AC-2.1.1.1.e are being applied to establish, activate, modify, disable, and remove accounts. |
| **AC-2.1.1.22** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with account management responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in AC-2.1.1.1.f are being applied to specifically authorize and monitor the use of guest/anonymous and temporary accounts. |
| **AC-2.1.1.23** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with account management responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in AC-2.1.1.1.g are being applied to notify account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes. |
| **AC-2.1.1.24** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with account management responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in AC-2.1.1.1.h are being applied to deactivate: i) temporary accounts that are no longer needed, and ii) accounts of terminated or transferred users. |
| **AC-2.1.1.25** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with account management responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in AC-2.1.1.1.i are being applied to grant access to the system based on a valid access authorization, intended system usage, and other attributes as required by the organization or associated mission/business functions. |
|  | |  |
| **AC-2.1.2.1** | | **Examine** security plan; [reviewing] for the frequency of information system account reviews. |
|  | |  |
| **AC-2.1.3.1** | | **Examine** documentation for an agreed-upon [*basic*] sample of information system account reviews; [*reviewing*] for evidence that information system accounts are reviewed in accordance with the frequency identified in AC-2.1.2.1. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **AC-2(1)** | ACCOUNT MANAGEMENT |
| **AC-2(1).1**  **AC-2(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated mechanisms to support information system account management functions.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing account management functions]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PL-2  concurrent controls: CM-6, IA-2, IA-4, IA-5  successor controls: AC-3, AC-4, AC-5, AC-6, AC-7, AC-9, AC-10, AC-13 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-2(1).1.1.1** | **Examine** security plan, information system design documentation, or other relevantdocuments; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to support information system account management functions. |
| **AC-2(1).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-2(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-2(1).1.1.1. |
| **AC-2(1).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-2(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **AC-2(2)** | ACCOUNT MANAGEMENT |
| **AC-2(2).1**  **AC-2(2).1.1**  **AC-2(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines a time period for each type of account after which the information system terminates temporary and emergency accounts; and* 2. *the information system automatically terminates temporary and emergency accounts after organization-defined time period for each type of account.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of active accounts; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing account management functions]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PL-2  concurrent controls: CM-6, IA-2, IA-4, IA-5  successor controls: AC-3, AC-4, AC-5, AC-6, AC-7, AC-9, AC-10, AC-13 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-2(2).1.1.1** | **Examine** security plan; [*reviewing*] for the time period after which the information system terminates temporary and emergency accounts for each type of account. |
|  |  |
| **AC-2(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 automatically terminate temporary and emergency accounts after the time period identified in AC-2(2).1.1.1 for each type of account. |
| **AC-2(2).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AC-2(2).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-2(2).1.2.1. |
| **AC-2(2).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-2(2)1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **AC-2(3)** | ACCOUNT MANAGEMENT |
| **AC-2(3).1**  **AC-2(3).1.1**  **AC-2(3).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines a time period after which the information system disables inactive accounts; and* 2. *the information system automatically disables inactive accounts after organization-defined time period.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of last login dates; information system-generated list of active accounts; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing account management functions]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PL-2  concurrent controls: CM-6, IA-2, IA-4, IA-5  successor controls: AC-3, AC-4, AC-5, AC-6, AC-7, AC-9, AC-10, AC-13 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-2(3).1.1.1** | **Examine** security plan; [*reviewing*] for the time period after which the information system disables inactive accounts. |
|  |  |
| **AC-2(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 automatically disable inactive accounts after the time period identified in AC-2(3).1.1.1. |
| **AC-2(3).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AC-2(3).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-2(3).1.2.1. |
| **AC-2(3).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-2(3)1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **AC-2(4)** | ACCOUNT MANAGEMENT |
| **AC-2(4).1**  **AC-2(4).1.1**  **AC-2(4).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the information system automatically audits account:*    * *creation;*    * *modification;*    * *disabling; and*    * *termination actions; and* 2. *the information system notifies, as required, appropriate individuals.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Procedures addressing account management; 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 account management functions]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PL-2  concurrent controls: AU-2, AU-3, AU-6, AU-7, CM-6  successor controls: AC-3, AC-4, AC-5, AC-6, AC-7, AC-9, AC-10, AC-13 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-2(4).1.1.1**  **AC-2(4).1.1.1.a**  **AC-2(4).1.1.1.b**  **AC-2(4).1.1.1.c**  **AC-2(4).1.1.1.d** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to automatically audit account:   * + creation;   + modification;   + disabling; and   + termination actions |
| **AC-2(4).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AC-2(4).1.1.1.a; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-2(4).1.1.1.a to audit account creation actions. |
| **AC-2(4).1.1.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AC-2(4).1.1.1.b; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-2(4).1.1.1.b to audit account modification actions. |
| **AC-2(4).1.1.4** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AC-2(4).1.1.1.c; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-2(4).1.1.1.c to audit account disabling actions. |
| **AC-2(4).1.1.5** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AC-2(4).1.1.1.d; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-2(4).1.1.1.d to audit account termination actions. |
| **AC-2(4).1.1.6** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AC-2(4).1.1.1.a; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in AC-2(4).1.1.1.a to audit account creation actions. |
| **AC-2(4).1.1.7** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AC-2(4).1.1.1.b; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in AC-2(4).1.1.1.b to audit account modification actions. |
| **AC-2(4).1.1.8** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AC-2(4).1.1.1.c; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in AC-2(4).1.1.1.c to audit account disabling actions. |
| **AC-2(4).1.1.9** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AC-2(4).1.1.1.d; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in AC-2(4).1.1.1.d to audit account termination actions. |
|  |  |
| **AC-2(4).1.2.1** | **Examine** account management policy, procedures addressing account management, security plan, or other relevant documents; [*reviewing*] for the notifications deemed required by the organization with regard to account management actions and for the individuals deemed appropriate by the organization to receive these notifications.  Note to assessor: The identification of when notification is required and to whom the notification should be provided need only be specific enough to enable determination of whether the organizational intent is being achieved; for example, the individuals need not be called out by name but may be defined by the positions or roles that need to receive the notification. |
| **AC-2(4).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 accomplish the notifications identified in AC-2(4).1.2.1. |
| **AC-2(4).1.2.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AC-2(4).1.2.2; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-2(4).1.2.2. |
| **AC-2(4).1.2.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel identified in AC-2(4).1.2.1 with account management responsibilities; conducting [*basic*] discussions for further evidence that the mechanisms and configurations identified in AC-2(4).1.2.2 are being applied. |
| **AC-2(4).1.2.5** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AC-2(4).1.2.2; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 5** | |
| **AC-2(5)** | ACCOUNT MANAGEMENT |
| **AC-2(5).1**  **AC-2(5).1.1**  **AC-2(5).1.2**  **AC-2(5).1.3**  **AC-2(5).1.4**  **AC-2(5).1.5** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the time period of expected inactivity and/or description of when users log out;* 2. *the organization requires that users log out in accordance with the organization-defined time-period of inactivity and/or description of when to log out;* 3. *the organization determines normal time-of-day and duration usage for information system accounts;* 4. *the organization monitors for atypical usage of information system accounts; and* 5. *the organization reports atypical usage to designated organizational officials.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; security violation reports; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with account management responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PL-2  concurrent controls: CM-6, IA-2, IA-4, IA-5  successor controls: : AC-3, AC-4, AC-5, AC-6, AC-7, AC-9, AC-10, AC-13 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-2(5).1.1.1** | **Examine** security plan; [*reviewing*] for the time period of expected inactivity and/or description of when users log out. |
|  |  |
| **AC-2(5).1.2.1** | **Examine** access control policy, procedures addressing account management,security plan, or other relevant documents; [*reviewing*] for the requirement that users log out in accordance with the time period of inactivity and/or description identified in AC-2(5).1.1.1. |
| **AC-2(5).1.2.2** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with account management responsibilities; conducting [*basic*] discussions for further evidence of the requirement that users log out in accordance with the time period of inactivity and/or description identified in AC-2(5).1.1.1 . |
|  |  |
| **AC-2(5).1.3.1** | **Examine** security plan; [*reviewing*] for the normal time-of-day and duration usage parameter for information system accounts. |
|  |  |
| **AC-2(5).1.4.1** | **Examine** access control policy, procedures addressing account management, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to monitor for atypical usage of information system accounts. |
| **AC-2(5).1.4.2** | **Examine** an agreed-upon [*basic*] sample of security violation reports, information system audit records, or other relevant records associated with monitoring for atypical usage of information system accounts; [*reviewing*] for evidence that the measures identified in AC-2(5).1.4.1 are being applied. |
|  |  |
| **AC-2(5).1.5.1** | **Examine** access control policy, procedures addressing account management, security plan, or other relevant documents; [*reviewing*] for the process to be employed by the organization to report atypical usage of information system accounts, and for the officials designated by the organization to receive these reports. |
| **AC-2(5).1.5.2** | **Examine** an agreed-upon [*basic*] sample of security violation reports, information system audit records, or other relevant documents associated with reporting atypical usage of information system accounts to the organizational officials identified in AC-2(5).1.5.1; [*reviewing*] for evidence that the process identified in AC-2(5).1.5.1 is implemented as intended. |
| **AC-2(5).1.5.3** | **Interview** an agreed-upon [*basic*] sample of organizational officials designated in AC-2(5).1.5.1 to receive reports of atypical usage for information system accounts; conducting [*basic*] discussions for further evidence that the process identified in AC-2(5).1.5.1 is being applied. |
|  | |
| **ASSESSMENT – Control Enhancement 6** | |
| **AC-2(6)** | ACCOUNT MANAGEMENT |
| **AC-2(6).1**  **AC-2(6).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system dynamically manages user privileges and associated access authorizations.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with account management responsibilities].  **Test**: [*select from:* Automated mechanisms implementing account management functions]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PL-2  concurrent controls: CM-6, IA-2, IA-4, IA-5  successor controls: AC-3, AC-4, AC-5, AC-6, AC-7, AC-9, AC-10, AC-13 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-2(6).1.1.1** | **Examine** security plan, information system design documentation, or other relevantdocuments; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to dynamically manage user privileges and associated access authorizations. |
| **AC-2(6).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-2(6).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-2(6).1.1.1. |
| **AC-2(6).1.1.3** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AC-2(6).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 7** | |
| **AC-2(7)** | ACCOUNT MANAGEMENT |
| **AC-2(7).1**  **AC-2(7).1.1**  **AC-2(7).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and* 2. *the organization tracks and monitors privileged role assignments.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system-generated list of privileged user accounts and associated role; information system audit records; audit tracking and monitoring reports; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with account management responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PL-2  concurrent controls: CM-6, IA-2, IA-4, IA-5  successor controls: AC-3, AC-4, AC-5, AC-6, AC-7, AC-9, AC-10, AC-13 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-2(7).1.1.1** | **Examine** access control policy, procedures addressing account management, security plan, or other relevantdocuments; [*reviewing*] forthe role-based access scheme to be employed to organize information system and network privileges into roles. |
| **AC-2(7).1.1.2** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to establish and administer privileged user accounts in accordance with the role-based access scheme identified in AC-2(7).1.1.1. |
| **AC-2(7).1.1.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AC-2(7).1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-2(7).1.1.2. |
| **AC-2(7).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with account management responsibilities; conducting [*basic*] discussions for further evidence that the role-based access scheme identified in AC-2(7).1.1.1 is being applied to organize information system and network privileges into roles using the mechanisms identified in AC-2(7).1.1.2. |
| **AC-2(7).1.1.5** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AC-2(7).1.1.2; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **AC-2(7).1.2.1** | **Examine** access control policy, procedures addressing account management, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to track and monitor privileged role assignments. |
| **AC-2(7).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed upon [*basic*] sample of the automated mechanisms identified in AC-2(7).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-2(7).1.2.1. |
| **AC-2(7).1.2.3** | **Examine** an agreed-upon [*basic*] sample of information system audit records, audit tracking and monitoring reports, or other relevant documents associated with an information system-generated list of current privileged user accounts and related roles; [*reviewing*] for evidence that the measures identified in AC-2(7).1.2.1 are being applied. |
| **AC-2(7).1.2.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for tracking and monitoring privileged role assignments; conducting [*basic*] discussions for further evidence that the measures identified in AC-2(7).1.2.1 are being applied. |
| **AC-2(7).1.2.5** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AC-2(7).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |