| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **IA-4** | IDENTIFIER MANAGEMENT | |
| **IA-4.1**  **IA-4.1.1**  **IA-4.1.2**  **IA-4.1.3**  **IA-4.1.3a**  **IA-4.1.3b**  **IA-4.1.3c**  **IA-4.1.3d**  **IA-4.1.3e** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the time period for preventing reuse of user or device identifiers;* 2. *the organization defines the time period of inactivity after which a user identifier is to be disabled; and* 3. *the organization manages information system identifiers for users and devices by:*    * *receiving authorization from a designated organizational official to assign a user or device identifier;*    * *selecting* *an identifier that uniquely identifies an individual or device;*    * *assigning the user identifier to the intended party or the device identifier to the intended device;*    * *preventing reuse of user or device identifiers for the organization-defined time period; and*    * *disabling the user identifier after the organization-defined time period of inactivity.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; list of identifiers generated from physical access control devices; other relevant documents or records].  **Interview:** [*select from:* Organizational personnel with identifier management responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-14  concurrent controls: CM-6, IA-2, IA-3, IA-6, IA-7, IA-8, MA-4  successor controls: IA-5 |
| **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. |
| **IA-4.1.1.1** | | **Examine** identification and authentication policy, procedures addressing identifier management, procedures addressing account management, security plan, or other relevant documents; [*reviewing*] for the time period for preventing reuse of user or device identifiers. |
|  | |  |
| **IA-4.1.2.1** | | **Examine** identification and authentication policy, procedures addressing identifier management, procedures addressing account management, security plan, or other relevant documents; [*reviewing*] for the time period of inactivity after which a user identifier is to be disabled. |
|  | |  |
| **IA-4.1.3.1**  **IA-4.1.3.1.a**  **IA-4.1.3.1.b**  **IA-4.1.3.1.c**  **IA-4.1.3.1.d**  **IA-4.1.3.1.e** | | **Examine** identification and authentication policy, procedures addressing identifier management, 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 employed to manage information system identifiers for users and devices by:   * + receiving authorization from a designated organizational official to assign a user or device identifier;   + selecting an identifier that uniquely identifies an individual or device;   + assigning the user identifier to the intended party or the device identifier to the intended device;   + preventing reuse of user or device identifiers for the time period identified in IA-4.1.1.1; and   + disabling the user identifier after the time period of inactivity identified in IA-4.1.2.1. |
| **IA-4.1.3.2** | | **Examine** authorization approvals to assign a user or device identifier for an agreed-upon [*basic*] sample of information system accounts; [*reviewing*] for evidence that the measures identified in IA-4.1.3.1.a are being applied to receive authorization from a designated official to assign a user or device identifier. |
| **IA-4.1.3.3** | | **Examine** information system identifiers for an agreed-upon [*basic*] sample of users or devices; [*reviewing*] for evidence that the measures identified in IA-4.1.3.1.b are being applied to select an identifier that uniquely identifies an individual or device. |
| **IA-4.1.3.4** | | **Examine** information system identifiers for an agreed-upon [*basic*] sample of users or devices; [*reviewing*] for evidence that the measures identified in IA-4.1.3.1.c are being applied to assign a user identifier to the intended party or a device identifier to the intended device. |
| **IA-4.1.3.5** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in IA-4.1.3.1.d; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-4.1.3.1.d to prevent the reuse of user or device identifiers for the time period identified in IA-4.1.1.1. |
| **IA-4.1.3.6** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in IA-4.1.3.1.e; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-4.1.3.1.e to disable the user identifier after the time period identified in IA-4.1.2.1. |
| **IA-4.1.3.7** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for assigning user or device identifiers; conducting [*basic*] discussions for evidence that the measures identified in IA-4.1.3.1.a are being applied to receive authorization from a designated official to assign a user or device identifier. |
| **IA-4.1.3.8** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in IA-4.1.3.1.d; conducting [*basic*] testing for further evidence that these mechanisms are operating as intended in IA-4.1.3.1.d to prevent the reuse of user or device identifiers for the time period identified in IA-4.1.1.1. |
| **IA-4.1.3.9** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in IA-4.1.3.1.e; conducting [*basic*] testing for further evidence that these mechanisms are operating as intended in IA-4.1.3.1.e to disable the user identifier after the time period identified in IA-4.1.2.1. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **IA-4(1)** | | IDENTIFIER MANAGEMENT |
| **IA-4(1).1**  **IA-4(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if organization prohibits the use of information system account identifiers as public identifiers for user electronic mail accounts (i.e., user identifier portion of the electronic mail address).*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-14  concurrent controls: CM-6, IA-2, IA-3, IA-6, IA-7, IA-8  successor controls: IA-5 |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **IA-4(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 prohibit the use of information system account identifiers as public identifiers for user electronic mail accounts. |
| **IA-4(1).1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-4(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-4(1).1.1.1. |
| **IA-4(1).1.1.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-4(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)** | |
| **IA-4(2)** | IDENTIFIER MANAGEMENT |
| **IA-4(2).1**  **IA-4(2).1.1**  **IA-4(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization requires that registration to receive a user ID and password include authorization by a supervisor; and* 2. *the organization requires that registration to receive a user ID and password be done in person before a designated registration authority.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; user ID and password registration documentation; ID and password authorization records; registration authority records; other relevant documents or records].  **Interview:** [*select from:* Organizational personnel with identifier management responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3,  concurrent controls: IA-2, IA-3, IA-8  successor controls: IA-5 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-4(2).1.1.1** | **Examine** identification and authentication policy, procedures addressing identifier management, procedures addressing account management, security plan, or other relevant documents; [*reviewing*] for the requirement that registration to receive a user ID and password include authorization by a supervisor. |
|  |  |
| **IA-4(2).1.2.1** | **Examine** identification and authentication policy, procedures addressing identifier management, procedures addressing account management, security plan, or other relevant documents; [*reviewing*] for the requirement that registration to receive a user ID and password be done in person before a designated registration authority. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-4(3)** | IDENTIFIER MANAGEMENT |
| **IA-4(3).1**  **IA-4(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization requires multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; identifier certification documentation; organizational personnel biometrics records; other relevant documents or records].  **Interview:** [*select from:* Organizational personnel with identifier management responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3  concurrent controls: IA-2, IA-3, IA-8  successor controls: IA-5 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-4(3).1.1.1** | **Examine** identification and authentication policy, procedures addressing identifier management, procedures addressing account management, security plan, or other relevant documents; [*reviewing*] for the requirement that multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-4(4)** | IDENTIFIER MANAGEMENT |
| **IA-4(4).1**  **IA-4(4).1.1**  **IA-4(4).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the characteristic to be used to identify user status; and* 2. *the organization manages user identifiers by uniquely identifying the user with the organization-defined characteristic identifying user status.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; list of characteristics identifying user status; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3  concurrent controls: IA-2, IA-3, IA-8  successor controls: IA-5 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-4(4).1.1.1** | **Examine** identification and authentication policy, procedures addressing identifier management, procedures addressing account management, security plan, or other relevant documents; [*reviewing*] for the characteristics to be used to identify user status. |
|  |  |
| **IA-4(4).1.2.1** | **Examine** identification and authentication policy, procedures addressing identifier management, procedures addressing account management, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to uniquely identify the user with the characteristics identified in IA-4(4).1.1.1. |
| **IA-4(4).1.2.2** | **Examine** identifier management records, account management records, or other relevant records for an agreed-upon [*basic*] sample of information system users; [*reviewing*] for evidence that the measures identified in IA-4(4).1.2.1 are being applied. |
| **IA-4(4).1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for managing user identifiers; conducting [*basic*] discussions for evidence that the measures identified in IA-4(4).1.2.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-4(5)** | IDENTIFIER MANAGEMENT |
| **IA-4(5).1**  **IA-4(5).1.1**  **IA-4(5).1.1a**  **IA-4(5).1.1b**  **IA-4(5).1.1c** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system dynamically manages:*   * *identifiers;* * *attributes; and* * *associated access authorizations.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing identifier management; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing identifier management functions]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-14  concurrent controls: CM-6, IA-2, IA-3, IA-6, IA-7, IA-8  successor controls: IA-5 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-4(5).1.1.1**  **IA-4(5).1.1.1.a**  **IA-4(5).1.1.1.b**  **IA-4(5).1.1.1.c** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to dynamically manage:   * identifiers; * attributes; and * associated access authorizations. |
| **IA-4(5).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-4(5).1.1.1.a; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-4(5).1.1.1.a to dynamically manage identifiers. |
| **IA-4(5).1.1.3** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-4(5).1.1.1.b; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-4(5).1.1.1.b to dynamically manage attributes. |
| **IA-4(5).1.1.4** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-4(5).1.1.1.c; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-4(5).1.1.1.c to dynamically manage associated access authorizations. |
| **IA-4(5).1.1.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-4(5).1.1.1.a; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in IA-4(5).1.1.1.a to dynamically manage identifiers. |
| **IA-4(5).1.1.6** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-4(5).1.1.1.b; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in IA-4(5).1.1.1.b to dynamically manage attributes. |
| **IA-4(5).1.1.7** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-4(5).1.1.1.c; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in IA-4(5).1.1.1.c to dynamically manage associated access authorizations. |