| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **IA-5** | AUTHENTICATOR MANAGEMENT | |
| **IA-5.1**  **IA-5.1.1**  **IA-5.1.2**  **IA-5.1.2a**  **IA-5.1.2b**  **IA-5.1.2c**  **IA-5.1.2d**  **IA-5.1.2e**  **IA-5.1.2f**  **IA-5.1.2g**  **IA-5.1.2h**  **IA-5.1.2i**  **IA-5.1.2j**  **IA-5.1.2k** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the time period (by authenticator type) for changing/refreshing authenticators; and* 2. *the organization manages information system authenticators for users and devices by:*    * *verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;*    * *establishing initial authenticator content for authenticators defined by the organization;*    * *ensuring that authenticators have sufficient strength of mechanism for their intended use;*    * *establishing and implementing administrative procedures for initial authenticator distribution;*    * *establishing and implementing administrative procedures for lost/compromised or damaged authenticators;*    * *establishing and implementing administrative procedures for revoking authenticators;*    * *changing default content of authenticators upon information system installation;*    * *establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if deemed to be appropriate by the organization);*    * *changing/refreshing authenticators in accordance with the organization-defined time period by authenticator type;*    * *protecting authenticator content from unauthorized disclosure and modification; and*    * *requiring users to take, and having devices implement, specific measures to safeguard authenticators.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for determining initial authenticator content].  **Test**: [*select from:* Automated mechanisms implementing authenticator management functions]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-14, IA-4  concurrent controls: CM-6, IA-2, IA-3, IA-6, IA-7, IA-8, MA-4, SC-28  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
|  | | *\*\*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-5.1.1.1** | | **Examine** identification and authentication policy, procedures addressing authenticator management, security plan, or other relevant documents; [*reviewing*] for the time period (by authenticator type) for changing/refreshing authenticators. |
|  | |  |
| **IA-5.1.2.1**  **IA-5.1.2.1.a**  **IA-5.1.2.1.b**  **IA-5.1.2.1.c**  **IA-5.1.2.1.d**  **IA-5.1.2.1.e**  **IA-5.1.2.1.f**  **IA-5.1.2.1.g**  **IA-5.1.2.1.h**  **IA-5.1.2.1.i**  **IA-5.1.2.1.j**  **IA-5.1.2.1.k** | | **Examine** identification and authentication policy, procedures addressing authenticator 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 manage information system authenticators for users and devices by:   * + verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;   + establishing initial authenticator content for authenticators defined by the organization;   + ensuring that authenticators have sufficient strength of mechanism for their intended use;   + establishing and implementing administrative procedures for initial authenticator distribution;   + establishing and implementing administrative procedures for lost/compromised or damaged authenticators;   + establishing and implementing administrative procedures for revoking authenticators;   + changing default content of authenticators upon information system installation;   + establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if deemed to be appropriate by the organization);   + changing/refreshing authenticators in accordance with the time period (by authenticator type) identified in IA-5.1.1.1;   + protecting authenticator content from unauthorized disclosure and modification; and   + requiring users to take, and having devices implement, specific measures to safeguard authenticators. |
| **IA-5.1.2.2** | | **Examine** identity verification forms for an agreed-upon [*basic*] sample of information system users and devices; [*reviewing*] for evidence that the measures identified in IA-5.1.2.1.a are being applied to verify the identity of individuals and/or devices as part of the initial authenticator distribution. |
| **IA-5.1.2.3** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-5.1.2.1.b; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-5.1.2.1.b to establish initial authenticator content for authenticators defined by the organization.  Note to assessor: Authenticators generated manually will be covered by assessor action IA-5.1.2.12. |
| **IA-5.1.2.4** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-5.1.2.1.c; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-5.1.2.1.c to ensure authenticators have sufficient strength of mechanism for their intended use. |
| **IA-5.1.2.5** | | **Examine** identification and authentication policy, procedures addressing authenticator management, security plan, or other relevant documents; [*reviewing*] for the administrative procedures to be employed in IA-5.1.2.1.d for initial authenticator distribution. |
| **IA-5.1.2.6** | | **Examine** identification and authentication policy, procedures addressing authenticator management, security plan, or other relevant documents; [*reviewing*] for the administrative procedures to be employed in IA-5.1.2.1.e for lost/compromised or damaged authenticators. |
| **IA-5.1.2.7** | | **Examine** identification and authentication policy, procedures addressing authenticator management, security plan, or other relevant documents; [*reviewing*] for the administrative procedures to be employed in IA-5.1.2.1.f for revoking authenticators. |
| **IA-5.1.2.8** | | **Examine** an agreed-upon [*basic*] sample of information system accounts known to be delivered with default authenticators; [*reviewing*] for evidence that the measures identified in IA-5.1.2.1.g are being applied to change default content of authenticators upon information system installation. |
| **IA-5.1.2.9** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in IA-5.1.2.1.h ; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-5.1.2.1.h to establish minimum and maximum lifetime restrictions and reuse conditions for authenticators. |
| **IA-5.1.2.10** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-5.1.2.1.i.; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-5.1.2.1.i to change/refresh authenticators in accordance with the time period identified in IA-5.1.1.1. |
| **IA-5.1.2.11** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-5.1.2.1.j; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-5.1.2.1.j to protect authenticator content from unauthorized disclosure and modification. |
| **IA-5.1.2.12** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for assigning initial user or device authenticators; conducting [*basic*] discussions for evidence that the measures identified in IA-5.1.2.1.a are being applied to verify the identity of the individual and/or device receiving the authenticator. |
| **IA-5.1.2.13** | | **Interview** an agreed-upon [*basic*] sample of organization personnel responsible for determining initial authenticator content; conducting [*basic*] discussions for evidence of the measures identified in IA-5.1.2.1.b are being applied to establish initial authenticator content for authenticators defined by the organization. |
| **IA-5.1.2.14** | | **Interview** an agreed-upon [*basic*] sample of organization personnel responsible for initial authenticator distribution; conducting [*basic*] discussions for evidence that the administrative procedures identified in IA-5.1.2.1.d are being applied for initial authenticator distribution. |
| **IA-5.1.2.15** | | **Interview** an agreed-upon [*basic*] sample of organization personnel responsible for handling lost/compromised or damaged authenticators; conducting [*basic*] discussions for evidence that the administrative procedures identified in IA-5.1.2.1.e are being applied for lost/compromised or damaged authenticators. |
| **IA-5.1.2.16** | | **Interview** an agreed-upon [*basic*] sample of organization personnel responsible for revoking authenticators; conducting [*basic*] discussions for evidence that the administrative procedures identified in IA-5.1.2.1.f are being applied for revoking authenticators. |
| **IA-5.1.2.17** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with authenticator management responsibilities; [*reviewing*] for evidence of the requirement identified in IA-5.1.2.1.k for users to take, and devices to implement, specific measures to safeguard authenticators. |
| **IA-5.1.2.18** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-5.1.2.1.b; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in IA-5.1.2.1.b to establish initial authenticator content for authenticators identified by the organization. |
| **IA-5.1.2.19** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-5.1.2.1.c; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in IA-5.1.2.1.c to ensure authenticators have sufficient strength of mechanism for their intended use. |
| **IA-5.1.2.20** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-5.1.2.1.h; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in IA-5.1.2.1.h to establish minimum and maximum lifetime restrictions and reuse conditions for authenticators. |
| **IA-5.1.2.21** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-5.1.2.1.i; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in IA-5.1.2.1.i to change/refresh authenticators in accordance with the time period identified in IA-5.1.1.1. |
| **IA-5.1.2.22** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-5.1.2.1.j; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in IA-5.1.2.1.j to protect authenticator content from unauthorized disclosure and modification. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-5(1)** | AUTHENTICATOR MANAGEMENT |
| **IA-5(1).1**  **IA-5(1).1.1**  **IA-5(1).1.2**  **IA-5(1).1.3**  **IA-5(1).1.4**  **IA-5(1).1.5**  **IA-5(1).1.5a**  **IA-5(1).1.5b**  **IA-5(1).1.5c**  **IA-5(1).1.5d**  **IA-5(1).1.5e** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the minimum password complexity requirements to be enforced for case sensitivity, the number of characters, and the mix of upper-case letters, lower-case letters, numbers, and special characters including minimum requirements for each type;* 2. *the organization defines the minimum number of characters that must be changed when new passwords are created;* 3. *the organization defines the restrictions to be enforced for password minimum lifetime and password maximum lifetime parameters;* 4. *the organization defines the number of generations for which password reuse is prohibited; and* 5. *the information system, for password-based authentication:*    * *enforces the minimum password complexity standards that meet the organization-defined requirements;*    * *enforces the organization-defined minimum number of characters that must be changed when new passwords are created;*    * *encrypts passwords in storage and in transmission;*    * *enforces the organization-defined restrictions for password minimum lifetime and password maximum lifetime parameters; and*    * *prohibits password reuse for the organization-defined number of generations.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; password policy; procedures  addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing authenticator management functions]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-14, IA-4  concurrent controls: CM-6, IA-2, IA-3, IA-7, IA-8, MA-4, SC-28  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-5(1).1.1.1** | **Examine** identification and authentication policy, password policy, procedures addressing authenticator management, security plan, or other relevant documents; [*reviewing*] for the minimum password complexity requirements to be enforced for case sensitivity, the number of characters, and the mix of upper-case letters, lower-case letters, numbers, and special characters including minimum requirements for each type. |
|  |  |
| **IA-5(1).1.2.1** | **Examine** identification and authentication policy, password policy, procedures addressing authenticator management, security plan, or other relevant documents; [*reviewing*] for the minimum number of characters that must be changed when new passwords are created. |
|  |  |
| **IA-5(1).1.3.1** | **Examine** identification and authentication policy, password policy, procedures addressing authenticator management, security plan, or other relevant documents; [*reviewing*] for the restrictions to be enforced for password minimum lifetime and password maximum lifetime parameters. |
|  |  |
| **IA-5(1).1.4.1** | **Examine** identification and authentication policy, password policy, procedures addressing authenticator management, security plan, or other relevant documents; [*reviewing*] for the number of generations for which password reuse is to be prohibited. |
|  |  |
| **IA-5(1).1.5.1**  **IA-5(1).1.5.1.a**  **IA-5(1).1.5.1.b**  **IA-5(1).1.5.1.c**  **IA-5(1).1.5.1.d**  **IA-5(1).1.5.1.e** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed, for password-based authentication, to:   * + enforce the minimum password complexity standards that meet the requirements identified in IA-5(1).1.1.1;   + enforce the minimum number of characters identified in IA-5(1).1.2.1 that must be changed when new passwords are created;   + encrypt passwords in storage and in transmission;   + enforce the restrictions identified in IA-5(1).1.3.1 for password minimum lifetime and password maximum lifetime parameters; and   + prohibit password reuse for the number of generations identified in IA-5(1).1.4.1. |
| **IA-5(1).1.5.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-5(1).1.5.1.a; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-5(1).1.5.1.a to enforce the minimum password complexity requirements identified in IA-5(1).1.1.1. |
| **IA-5(1).1.5.3** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-5(1).1.5.1.b; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-5(1).1.5.1.b to enforce the minimum number of characters identified in IA-5(1).1.2.1 that must be changed when new passwords are created. |
| **IA-5(1).1.5.4** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-5(1).1.5.1.c; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-5(1).1.5.1.c to encrypt passwords in storage and in transmission. |
| **IA-5(1).1.5.5** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-5(1).1.5.1.d; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-5(1).1.5.1.d to enforce the restrictions identified in IA-5(1).1.3.1 for password minimum lifetime and password maximum lifetime parameters. |
| **IA-5(1).1.5.6** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-5(1).1.5.1.e; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-5(1).1.5.1.e to prohibit password reuse for the number of generations identified in IA-5(1).1.4.1. |
| **IA-5(1).1.5.7** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-5(1).1.5.1.a; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in IA-5(1).1.5.1.a to enforce the minimum password complexity requirements identified in IA-5(1).1.1.1. |
| **IA-5(1).1.5.8** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-5(1).1.5.1.b; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in IA-5(1).1.5.1.b to enforce the minimum number of characters identified in IA-5(1).1.2.1 that must be changed when new passwords are created. |
| **IA-5(1).1.5.9** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-5(1).1.5.1.c; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in IA-5(1).1.5.1.c to encrypt passwords in storage and in transmission. |
| **IA-5(1).1.5.10** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-5(1).1.5.1.d; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in IA-5(1).1.5.1.d to enforce the restrictions identified in IA-5(1).1.3.1 for password minimum lifetime and password maximum lifetime parameters. |
| **IA-5(1).1.5.11** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-5(1).1.5.1.e; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in IA-5(1).1.5.1.e to prohibit password reuse for the number of generations identified in IA-5(1).1.4.1. |
|  | |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-5(2)** | AUTHENTICATOR MANAGEMENT |
| **IA-5(2).1**  **IA-5(2).1.1**  **IA-5(2).1.1a**  **IA-5(2).1.1b**  **IA-5(2).1.1c** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system, for PKI-based authentication:*   * *validates certificates by constructing a certification path with status information to an accepted trust anchor;* * *enforces authorized access to the corresponding private key; and* * *maps the authenticated identity to the user account.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; PKI certification revocation lists; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for PKI-based authentication management].  **Test**: [*select from:* Automated mechanisms implementing PKI-based authenticator management functions]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-14, IA-4  concurrent controls: CM-6, IA-2, IA-3, IA-7, IA-8, MA-4, SC-12, SC-13, SC-28  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-5(2).1.1.1**  **IA-5(2).1.1.1.a**  **IA-5(2).1.1.1.b**  **IA-5(2).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, for PKI-based authentication, to:   * validate certificates by constructing a certification path with status information to an accepted trust anchor; * enforce authorized access to the corresponding private key; and * map the authenticated identity to the user account. |
| **IA-5(2).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-5(2).1.1.1.a; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-5(2).1.1.1.a to validate certificates by constructing a certification path with status information to an accepted trust anchor. |
| **IA-5(2).1.1.3** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-5(2).1.1.1.b; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-5(2).1.1.1.b to enforce authorized access to the corresponding private key. |
| **IA-5(2).1.1.4** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-5(2).1.1.1.c; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-5(2).1.1.1.c to map the authenticated identity to the user account. |
| **IA-5(2).1.1.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-5(2).1.1.1.a; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in IA-5(2).1.1.1.a to validate certificates by constructing a certification path with status information to an accepted trust anchor. |
| **IA-5(2).1.1.6** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-5(2).1.1.1.b; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in IA-5(2).1.1.1.b to enforce authorized access to the corresponding private key. |
| **IA-5(2).1.1.7** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-5(2).1.1.1.c; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in IA-5(2).1.1.1.c to map the authenticated identity to the user account. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-5(3)** | AUTHENTICATOR MANAGEMENT |
| **IA-5(3).1**  **IA-5(3).1.1**  **IA-5(3).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the types of and/or specific authenticators for which the registration process must be carried out in person before* *a designated registration authority with authorization by a designated organizational official; and* 2. *the organization requires that the registration process to receive organization-defined types of and/or specific authenticators be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing authenticator management; list of authenticators that require in-person registration; authenticator registration documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with authenticator management responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, IA-4  concurrent controls: IA-2, IA-3, IA-7, IA-8  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-5(3).1.1.1** | **Examine** identification and authentication policy, procedures addressing authenticator management, security plan, or other relevant documents; [*reviewing*] for the types of and/or specific authenticators for which the registration process must be carried out in person, before a designated registration authority, with authorization by a designated organizational official. |
|  |  |
| **IA-5(3).1.2.1** | **Examine** identification and authentication policy, procedures addressing authenticator management, security plan, or other relevant documents; [*reviewing*] for the requirement that the registration process to receive the types of and/or specific authenticators identified in IA-5(3).1.1.1 be carried out in person, before a designated registration authority, with authorization by a designated organizational official. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-5(4)** | AUTHENTICATOR MANAGEMENT |
| **IA-5(4).1**  **IA-5(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; automated tools for testing authenticators; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with authenticator management responsibilities].  **Test**: [*select from:* Automated mechanisms for authenticator strength]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, IA-4  concurrent controls: CM-6, IA-2,IA-3, IA-6, IA-7, IA-8  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-5(4).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 determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators. |
| **IA-5(4).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-5(4).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-5(4).1.1.1. |
| **IA-5(4).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-5(4).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-5(5)** | AUTHENTICATOR MANAGEMENT |
| **IA-5(5).1**  **IA-5(5).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization requires vendors and/or manufacturers of information system components to provide unique authenticators or change default authenticators prior to delivery.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; system and services acquisition policy; procedures addressing authenticator management; procedures addressing the integration of security requirements into the acquisition process; acquisition documentation; acquisition contracts for information system procurements or services; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with authenticator management responsibilities; organizational personnel with information system security, acquisition, and contracting responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IA-4  concurrent controls: IA-2, IA-3, IA-8, SA-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-5(5).1.1.1** | **Examine** identification and authentication policy, system and services acquisition policy, procedures addressing authenticator management, acquisition contracts for information system procurements or services, security plan, or other relevant documents; [*reviewing*] for the requirement that vendors and/or manufacturers of information system components provide unique authenticators or change default authenticators prior to delivery. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 6** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-5(6)** | **AUTHENTICATOR MANGEMENT** |
| **IA-5(6).1**  **IA-5(6).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization protects authenticators commensurate with the classification or sensitivity of the information accessed.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing authenticator management; information classification or sensitivity documentation; security categorization documentation for the information system; security assessments of authenticator protections; risk assessment results; security plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with authenticator management responsibilities; organizational personnel implementing and/or maintaining authenticator protections]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IA-4  concurrent controls: IA-2, IA-3, IA-8, RA-2, RA-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-5(6).1.1.1** | **Examine** identification and authentication policy, procedures addressing authenticator management, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to protect authenticators commensurate with the classification or sensitivity of the information accessed. |
| **IA-5(6).1.1.2** | **Examine** risk assessments, security categorization results, and authenticator protections for an agreed-upon [*basic*] sample of information being accessed; [*reviewing*] for evidence that the measures identified in IA-5(6).1.1.1 are being applied. |
| **IA-5(6).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with authenticator management responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in IA-5(6).1.1.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 7** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-5(7)** | AUTHENTICATOR MANAGEMENT |
| **IA-5(7).1**  **IA-5(7).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; logical access scripts; application code reviews for detecting unencrypted static authenticators; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: IA-4  concurrent controls: CM-6, IA-2, IA-3, IA-8, SC-28  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-5(7).1.1.1** | **Examine** identification and authentication policy, procedures addressing authenticator 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 ensure that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys. |
| **IA-5(7).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-5(7).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-5(7).1.1.1. |
| **IA-5(7).1.1.3** | **Examine** information system code reviews for an agreed-upon [*basic*] sample of applications, access scripts, or function keys; [*reviewing*] for evidence that the measures identified in IA-5(7).1.1.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 8** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-5(8)** | AUTHENTICATOR MANAGEMENT |
| **IA-5(8).1**  **IA-5(8).1.1**  **IA-5(8).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines measures taken to manage the risk of compromise due to individuals having accounts on multiple information systems; and* 2. *the organization takes organization-defined measures to manage the risk of compromise due to individuals having accounts on multiple information systems.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing authenticator management; security plan; list of individuals having accounts on multiple information systems; list of measures intended to manage risk of compromise due to individuals having accounts on multiple information systems ; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, IA-4  concurrent controls: IA-2, IA-3, IA-8, PM-9, RA-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-5(8).1.1.1** | **Examine** identification and authentication policy, procedures addressing authenticator management, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to manage the risk of compromise due to individuals having accounts on multiple information systems. |
| **IA-5(8).1.2.1** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with authenticator management responsibilities; conducting [*basic*] discussions for evidence that the measures identified in IA-5(8).1.1.1 are being applied. |