| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **IA-2** | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | |
| **IA-2.1**  **IA-2.1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing identification and authentication capability for the information system]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-14  concurrent controls: AC-17, AC-18, AC-19, CM-6, IA-3, IA-4, IA-5, IA-6, IA-7, MA-4  successor controls: IA-8 |
| **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-2.1.1.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users). |
| **IA-2.1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-2.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-2.1.1.1. |
| **IA-2.1.1.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-2.1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-2(1)** | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) |
| **IA-2(1).1**  **IA-2(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system uses multifactor authentication for network access to privileged accounts.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing identification and authentication capability for the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-14  concurrent controls: AC-17, AC-18, AC-19, CM-6, IA-3, IA-4, IA-5, IA-6, IA-7, MA-4  successor controls: IA-8 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-2(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 enforce multifactor authentication for network access to privileged accounts. |
| **IA-2(1).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-2(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-2(1).1.1.1. |
| **IA-2(1).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-2(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-2(2)** | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) |
| **IA-2(2).1**  **IA-2(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system uses multifactor authentication for network access to non-privileged accounts.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of non-privileged information system accounts; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing identification and authentication capability for the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-14  concurrent controls: AC-17, AC-18, AC-19, CM-6, IA-3, IA-4, IA-5, IA-6, IA-7,  successor controls: IA-8 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-2(2).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 enforce multifactor authentication for network access to non-privileged accounts. |
| **IA-2(2).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-2(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-2(2).1.1.1. |
| **IA-2(2).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-2(2).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-2(3)** | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) |
| **IA-2(3).1**  **IA-2(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system uses multifactor authentication for local access to privileged accounts.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing identification and authentication capability for the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-14  concurrent controls: CM-6, IA-4, IA-5, IA-6, IA-7  successor controls: IA-8 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-2(3).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 enforce multifactor authentication for local access to privileged accounts. |
| **IA-2(3).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-2(3).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-2(3).1.1.1. |
| **IA-2(3).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-2(3).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-2(4)** | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) |
| **IA-2(4).1**  **IA-2(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system uses multifactor authentication for local access to non-privileged accounts.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of non-privileged information system accounts; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing identification and authentication capability for the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-14  concurrent controls: CM-6, IA-4, IA-5, IA-6, IA-7  successor controls: IA-8 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-2(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 enforce multifactor authentication for local access to non-privileged accounts. |
| **IA-2(4).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-2(4).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-2(4).1.1.1. |
| **IA-2(4).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-2(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-2(5)** | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) |
| **IA-2(5).1**  **IA-2(5).1.1**  **IA-2(5).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and* 2. *the organization requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing identification and authentication capability for the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-14  concurrent controls: AC-17, AC-18, AC-19, CM-6, IA-3, IA-4, IA-5, IA-6, IA-7, MA-4  successor controls: IA-8 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-2(5).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 allow the use of group authenticators only when used in conjunction with an individual/unique authenticator. |
| **IA-2(5).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-2(5).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-2(5).1.1.1. |
| **IA-2(5).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-2(5).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **IA-2(5).1.2.1** | **Examine** identification and authentication policy, procedures addressing user identification and authentication, security plan, or other relevant documents; [*reviewing*] for the requirement that individuals are to be authenticated with an individual authenticator prior to using a group authenticator. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 6** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-2(6)** | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) |
| **IA-2(6).1**  **IA-2(6).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if* *the information system uses multifactor authentication for network access to privileged accounts where one of the factors is provided by a device separate from the information system being accessed.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing identification and authentication capability for the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-14  concurrent controls: AC-17, AC-18, AC-19, CM-6, IA-3, IA-4, IA-5, IA-6, IA-7, MA-4  successor controls: IA-8 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-2(6).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 enforce multifactor authentication for network access to privileged accounts where one of the factors is provided by a device separate from the information system being accessed. |
| **IA-2(6).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-2(6).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-2(6).1.1.1. |
| **IA-2(6).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-2(6).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 7** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-2(7)** | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) |
| **IA-2(7).1**  **IA-2(7).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system uses multifactor authentication for network access to non-privileged accounts where one of the factors is provided by a device separate from the information system being accessed.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of non-privileged information system accounts; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing identification and authentication capability for the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-14  concurrent controls: AC-17, AC-18, AC-19, CM-6, IA-3, IA-4, IA-5, IA-6, IA-7  successor controls: IA-8 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-2(7).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 enforce multifactor authentication for network access to non-privileged accounts where one of the factors is provided by a device separate from the information system being accessed. |
| **IA-2(7).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in IA-2(7).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-2(7).1.1.1. |
| **IA-2(7).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in IA-2(7).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 8** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-2(8)** | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) |
| **IA-2(8).1**  **IA-2(8).1.1**  **IA-2(8).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the replay-resistant authentication mechanisms to be used for network access to privileged accounts; and* 2. *the information system uses the organization-defined replay-resistant authentication mechanisms for network access to privileged accounts.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing identification and authentication capability for the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-14  concurrent controls: AC-17, AC-18, AC-19, CM-6, IA-3, IA-4, IA-5, IA-6, IA-7, MA-4  successor controls: IA-8 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-2(8).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the replay-resistant authentication mechanisms to be used for network access to privileged accounts. |
|  |  |
| **IA-2(8).1.2.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the configuration settings to be employed for the replay-resistant authentication mechanisms identified in IA-2(8).1.1.1. |
| **IA-2(8).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the replay-resistant authentication mechanisms identified in IA-2(8).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-2(8).1.2.1. |
| **IA-2(8).1.2.3** | **Test** an agreed-upon [*basic*]sample of the replay-resistant authentication mechanisms identified in IA-2(8).1.1.1 and their configuration settings identified in IA-2(8).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 9** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **IA-2(9)** | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) |
| **IA-2(9).1**  **IA-2(9).1.1**  **IA-2(9).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the replay-resistant authentication mechanisms to be used for network access to non-privileged accounts; and* 2. *the information system uses the organization-defined replay-resistant authentication mechanisms for network access to non-privileged accounts.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing identification and authentication capability for the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, AC-14  concurrent controls: AC-17, AC-18, AC-19, CM-6, IA-3, IA-4, IA-5, IA-6, IA-7,  successor controls: IA-8 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **IA-2(9).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the replay-resistant authentication mechanisms to be used for network access to non-privileged accounts. |
|  |  |
| **IA-2(9).1.2.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the configuration settings to be employed for the replay-resistant authentication mechanisms identified in IA-2(9).1.1.1. |
| **IA-2(9).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the replay-resistant authentication mechanisms identified in IA-2(9).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in IA-2(9).1.2.1. |
| **IA-2(9).1.2.3** | **Test** an agreed-upon [*basic*]sample of the replay-resistant authentication mechanisms identified in IA-2(9).1.1.1 and their configuration settings identified in IA-2(9).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |