| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AC-18** | WIRELESS ACCESS | |
| **AC-18.1**  **AC-18.1.1**  **AC-18.1.2**  **AC-18.1.3**  **AC-18.1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization establishes usage restrictions and implementation guidance for wireless access;* 2. *the organization monitors for unauthorized wireless access to the information system;* 3. *the organization authorizes wireless access to the information system prior to connection; and* 4. *the organization enforces requirements for wireless connections to the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); activities related to wireless monitoring, authorization, and enforcement; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel responsible for authorizing, monitoring or controlling the use of wireless technologies in the information system].  **Test**: [*select from:* Wireless access usage and restrictions]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2  concurrent controls: AC-3, AC-17, AC-19, CM-6, CM-7, IA-2, IA-3, IA-8, SC-7  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. |
| **AC-18.1.1.1** | | **Examine** access control policy, procedures addressing wireless implementation and usage (including restrictions), security plan, or other relevant documents; [*reviewing*] for the usage restrictions and implementation guidance for wireless access. |
|  | |  |
| **AC-18.1.2.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to monitor for unauthorized wireless access to the information system. |
| **AC-18.1.2.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-18.1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-18.1.2.1. |
| **AC-18.1.2.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-18.1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |  |
| **AC-18.1.3.1** | | **Examine** access control policy, procedures addressing wireless implementation and usage (including restrictions), security plan, or other relevant documents; [*reviewing*] for the measures to be employed to authorize wireless access to the information system prior to connection. |
| **AC-18.1.3.2** | | **Examine** authorization approvals for an agreed-upon [*basic*] sample of wireless access connections to the information system; [*reviewing*] for evidence that the measures identified in AC-18.1.3.1 are being applied to authorize wireless access prior to connection. |
| **AC-18.1.3.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for authorizing wireless access connections to the information system; [*reviewing*] for further evidence that the measures identified in AC-18.1.3.1 are being applied. |
|  | |  |
| **AC-18.1.4.1** | | **Examine** access control policy, procedures addressing wireless implementation wireless implementation and usage (including restrictions), security plan, or other relevant documents; [*reviewing*] for the measures to be employed to enforce requirements for wireless connections to the information system. |
| **AC-18.1.4.2** | | **Examine** configuration settings and associated documentation for an agreed-upon [*basic*] sample of wireless access connections to the information system; [*reviewing*] for evidence that the measures identified in AC-18.1.4.1 are being applied to enforce requirements for wireless connections to the information system. |
| **AC-18.1.4.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for controlling wireless connections to the information system; [*reviewing*] for further evidence that the measures identified in AC-18.1.4.1 are being applied. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-18(1)** | WIRELESS ACCESS |
| **AC-18(1).1**  **AC-18(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system protects wireless access to the system using authentication and encryption.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing the access control policy for wireless access to the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-2, AC-3, AC-4, AC-17, AC-19, CM-6, IA-2, IA-3, IA-8, SC-7, SC-8,  SC-9, SC-13  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-18(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 protect wireless access to the system using authentication and encryption. |
| **AC-18(1).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-18(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-18(1).1.1.1. |
| **AC-18(1).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-18(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-18(2)** | WIRELESS ACCESS |
| **AC-18(2).1**  **AC-18(2).1.1**  **AC-18(2).1.2**  **AC-18(2).1.3**  **AC-18(2).1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the frequency of monitoring for unauthorized wireless connections to the information system, including scans for unauthorized wireless access points;* 2. *the organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points, in accordance with organization-defined frequency;* 3. *the organization defines the appropriate action(s) to be taken if an unauthorized connection is discovered; and* 4. *the organization takes appropriate action(s) if an unauthorized connection discovered.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); wireless scanning reports; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel responsible for monitoring wireless connections to the information system].  **Test**: [*select from:* Scanning procedures for detecting unauthorized wireless connections and access points]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-2, AU-2, AU-3, AU-6, AU-7, AU-12, AU-14, CM-6, CM-8, IA-3, IR-4,  IR-5, IR-6, IR-8, SI-4, SC-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-18(2).1.1.1** | **Examine** access control policy, procedures addressing wireless implementation and usage (including restrictions), security plan, or other relevant documents; [*reviewing*] for the frequency of monitoring for unauthorized wireless connections to the information system, including scans for unauthorized wireless access points. |
|  |  |
| **AC-18(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 monitor for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points, in accordance with the frequency identified in AC-18(2).1.1.1. |
| **AC-18(2).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-18(2).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-18(2).1.2.1. |
| **AC-18(2).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-18(2).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **AC-18(2).1.3.1** | **Examine** access control policy, procedures addressing wireless implementation and usage (including restrictions), security plan, or other relevant documents; [*reviewing*] for the appropriate action(s) to be taken if an unauthorized connection is discovered. |
|  |  |
| **AC-18(2).1.4.1** | **Examine** access control policy, procedures addressing wireless implementation and usage (including restrictions), security plan, or other relevant documents; [*reviewing*] for the measures to be employed to take the appropriate actions identified in AC-18(2).1.3.1 if an unauthorized connection is discovered. |
| **AC-18(2).1.4.2** | **Examine** after-action reports for an agreed-upon [*basic*] sample of unauthorized connections discovered; [*reviewing*] for evidence that the measures identified in AC-18(2).1.4.1 are being applied. |
| **AC-18(2).1.4.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for monitoring wireless connections to the information system; [*reviewing*] for further evidence that the measures identified in AC-18(2).1.4.1 are being applied. |
|  | |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-18(3)** | WIRELESS ACCESS |
| **AC-18(3).1**  **AC-18(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization disables, when not intended for use, wireless networking capabilities internally embedded within the information system components prior to issuance and deployment.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); 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 controlling the disabling of wireless networking capabilities internally embedded within the information system components]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, CM-7, IA-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-18(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 disable wireless networking capabilities (when not intended for use) internally embedded within the information system components prior to issuance and deployment. |
| **AC-18(3).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-18(3).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-18(3).1.1.1. |
| **AC-18(3).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-18(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)** | |
| **AC-18(4)** | WIRELESS ACCESS |
| **AC-18(4).1**  **AC-18(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization does not allow users to independently configure wireless networking capabilities.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); 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 preventing independent configuration of wireless networking capabilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, CM-7, IA-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-18(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 prevent independent configuration of wireless networking capabilities. |
| **AC-18(4).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-18(4).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-18(4).1.1.1. |
| **AC-18(4).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-18(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)** | |
| **AC-18(5)** | WIRELESS ACCESS |
| **AC-18(5).1**  **AC-18(5).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization confines wireless communications to organization-controlled boundaries.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing the access control policy for wireless access to the information system; Wireless connections and access points outside of organizational boundaries using scanning devices.]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, CM-7, IA-3, SC-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-18(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 confine wireless communications to organization-controlled boundaries. |
| **AC-18(5).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-18(5).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-18(5).1.1.1. |
| **AC-18(5).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-18(5).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |