| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AC-19** | ACCESS CONTROL FOR MOBILE DEVICES | |
| **AC-19.1**  **AC-19.1.1**  **AC-19.1.2**  **AC-19.1.3**  **AC-19.1.4**  **AC-19.1.5**  **AC-19.1.6**  **AC-19.1.7**  **AC-19.1.8** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices;* 2. *the organization authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems;* 3. *the organization monitors for unauthorized connections of mobile devices to organizational information systems;* 4. *the organization enforces requirements for the connection of mobile devices to organizational information systems;* 5. *the organization disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;* 6. *the organization issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures;* 7. *the organization defines the inspection and preventative measures to be applied to mobile devices returning from locations that the organization deems to be of significant risk; and* 8. *the organization applies organization-defined inspection and preventative measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel who use portable and mobile devices to access the information system].  **Test**: [*select from:* Automated mechanisms implementing access control policy for portable and mobile devices]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, AC-17, AC-18, CM-6, CM-7, MP-4, MP-5, SI-3, SI-4  successor controls: None |

|  |  |
| --- | --- |
| **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. |
| **AC-19.1.1.1** | **Examine** access control policy, procedures addressing access control for portable and mobile devices, security plan, or other relevant documents; [*reviewing*] for the usage restrictions and implementation guidance for organization-controlled portable and mobile devices. |
|  |  |
| **AC-19.1.2.1** | **Examine** access control policy, procedures addressing access control for portable and mobile devices, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to authorize connection of mobile devices that meet the organizational usage restrictions and implementation guidance identified in AC-19.1.1.1 to the information system. |
| **AC-19.1.2.2** | **Examine** authorization approvals for an agreed-upon [*basic*] sample of mobile devices with connection to the information system; [*reviewing*] for evidence that the measures identified in AC-19.1.2.1 are being applied to authorize mobile device connections. |
| **AC-19.1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for authorizing mobile device connections to the information system; [*reviewing*] for further evidence that the measures identified in AC-19.1.2.1 are being applied. |
|  |  |
| **AC-19.1.3.1** | **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 connections of mobile devices to the information system. |
| **AC-19.1.3.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-19.1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-19.1.3.1. |
| **AC-19.1.3.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-19.1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **AC-19.1.4.1** | **Examine** access control policy, procedures addressing access control for portable and mobile devices, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to enforce requirements for the connection of mobile devices to the information system. |
| **AC-19.1.4.2** | **Examine** configuration settings and associated documentation for an agreed-upon [*basic*] sample of mobile device connections to the information system; [*reviewing*] for evidence that the measures identified in AC-19.1.4.1 are being applied to enforce requirements for the connection of mobile devices to the information system. |
| **AC-19.1.4.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for controlling mobile device connections to the information system; [*reviewing*] for further evidence that the measures identified in AC-19.1.4.1 are being applied. |
|  |  |
| **AC-19.1.5.1** | **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 information system functionality that provides the capability for automatic execution of code on mobile devices without user direction. |
| **AC-19.1.5.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-19.1.5.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-19.1.5.1. |
| **AC-19.1.5.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-19.1.5.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **AC-19.1.6.1** | **Examine** access control policy, procedures addressing access control for portable and mobile devices, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to issue specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk. |
| **AC-19.1.6.2** | **Examine** mobile devices issued to an agreed-upon [*basic*] sample of individuals traveling to locations that the organization deems to be of significant risk; [*reviewing*] for evidence that the measures identified in AC-19.1.6.1 are being applied. |
|  |  |
| **AC-19.1.7.1** | **Examine** access control policy, procedures addressing access control for portable and mobile devices, security plan, or other relevant documents; [*reviewing*] for locations that are deemed to be of significant risk. |
| **AC-19.1.7.2** | **Examine** access control policy, procedures addressing access control for portable and mobile devices, security plan, or other relevant documents; [*reviewing*] for the inspection and preventative measures to be applied to mobile devices returning from locations identified in AC-19.1.7.1. |
|  |  |
| **AC-19.1.8.1** | **Examine** access control policy, procedures addressing access control for portable and mobile devices, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to apply the inspection and preventative measures identified in AC-19.1.7.2 to mobile devices returning from locations that the organization deems to be of significant risk. |
| **AC-19.1.8.2** | **Examine** an agreed-upon [*basic*] sample of mobile devices returning from locations identified in AC-19.1.7.1; [*reviewing*] for evidence that the measures identified in AC-19.1.8.1 are being applied. |
| **AC-19.1.8.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for inspecting mobile devices; [*reviewing*] for further evidence that the measures identified in AC-19.1.8.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-19(1)** | ACCESS CONTROL FOR MOBILE DEVICES |
| **AC-19(1).1**  **AC-19(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization restricts the use of writable, removable media in organizational information systems.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel who use portable and mobile devices to access the information system].  **Test**: [*select from:* Automated mechanisms implementing access control policy for portable and mobile devices]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, CM-7, MP-4, SC-34, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-19(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 restrict the use of writable, removable media in the information system. |
| **AC-19(1).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-19(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-19(1).1.1.1. |
| **AC-19(1).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-19(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-19(2)** | ACCESS CONTROL FOR MOBILE DEVICES |
| **AC-19(2).1**  **AC-19(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization prohibits the use of personally owned, removable media in organizational information systems.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing access control for portable and mobile devices; 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 access control policy for portable and mobile devices]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-20, CM-6,CM-7, MP-4, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-19(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 prohibit the use of personally-owned, removable media in the information system. |
| **AC-19(2).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-19(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-19(2).1.1.1. |
| **AC-19(2).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-19(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)** | |
| **AC-19(3)** | ACCESS CONTROL FOR MOBILE DEVICES |
| **AC-19(3).1**  **AC-19(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing access control for portable and mobile devices; 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 access control policy for portable and mobile devices]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, CM-7, MP-4, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-19(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 prohibit the use of removable media in the information system when the media has no identifiable owner. |
| **AC-19(3).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-19(3).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-19(3).1.1.1. |
| **AC-19(3).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-19(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-19(4)** | ACCESS CONTROL FOR MOBILE DEVICES |
| **AC-19(4).1**  **AC-19(4).1.1**  **AC-19(4).1.2**  **AC-19(4).1.3**  **AC-19(4).1.3a**  **AC-19(4).1.3b**  **AC-19(4).1.3c**  **AC-19(4).1.3d** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization prohibits the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information unless specifically permitted by the appropriate authorizing official(s);* 2. *the organization defines the security officials authorized to randomly review/inspect mobile devices and the information stored on those devices for classified information; and* 3. *the organization enforces the following restrictions on individuals permitted to use mobile devices in facilities containing information systems processing, storing, or transmitting classified information:*    * *connection of unclassified mobile devices to classified information systems is prohibited;*    * *connection of unclassified mobile devices to unclassified information systems requires approval from the appropriate authorizing official(s);*    * *use of internal or external modems or wireless interfaces within the mobile devices is prohibited; and*    * *mobile devices and the information stored on those devices are subject to random reviews/inspections by organization-defined security officials, and if classified information is found, the incident handling policy is enforced.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing access control for portable and mobile devices; evidentiary documentation for random inspections of mobile devices; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel responsible for randomly reviewing/inspecting mobile devices; Organizational personnel using mobile devices in facilities containing information systems processing, storing, or transmitting classified information].  **Test**: [*select from:* Test automated mechanisms prohibiting the use of internal or external modems or wireless interfaces with mobile devices]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-18, AC-20, AU-13, CM-6, CM-7, MP-4, MP-5, IR-4, IR-5, IR-6, IR-8,  SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-19(4).1.1.1** | **Examine** access control policy, procedures addressing access control for portable and mobile devices, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to prohibit the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information unless specifically permitted by the appropriate authorizing officials. |
| **AC-19(4).1.1.2** | **Examine** facilities containing classified information; [*observing*] for evidence that the measures identified in AC-19(4).1.1.1 are being applied to prohibit the use of unclassified mobile devices in facilities containing classified information. |
| **AC-19(4).1.1.3** | **Examine** authorization approvals for an agreed-upon [*basic*] sample of mobile devices used in facilities containing classified information, if applicable; [*reviewing*] for further evidence that the measures identified in AC-19(4).1.1.1 are being applied. |
| **AC-19(4).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for monitoring facilities containing classified information; [*reviewing*] for further evidence that the measures identified in AC-19(4).1.1.1 are being applied to prohibit the use of unclassified mobile devices in facilities containing classified information. |
|  |  |
| **AC-19(4).1.2.1** | **Examine** access control policy, procedures addressing access control for portable and mobile devices, security plan, or other relevant documents; [*reviewing*] for the security officials authorized to randomly review/inspect mobile devices and the information stored on those devices for classified information. |
|  |  |
| **AC-19(4).1.3.1** | **Examine** access control policy, procedures addressing access control for portable and mobile devices, security plan, or other relevant documents; [*reviewing*] for the official(s) authorized to approve connection of unclassified mobile devices to unclassified information systems. |
| **AC-19(4).1.3.2**  **AC-19(4).1.3.2.a**  **AC-19(4).1.3.2.b**  **AC-19(4).1.3.2.c**  **AC-19(4).1.3.2.d** | **Examine** access control policy, procedures addressing access control for portable and mobile devices, security plan, information system design documentation, other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to enforce the following restrictions on individuals permitted to use mobile devices in facilities containing information systems processing, storing, or transmitting classified information:   * + connection of unclassified mobile devices to classified information systems is prohibited;   + connection of unclassified mobile devices to unclassified information systems requires approval from the appropriate authorizing official(s) as identified in AC-19(4).1.3.1;   + use of internal or external modems or wireless interfaces within the mobile devices is prohibited; and   + mobile devices and the information stored on those devices are subject to random reviews/inspections by organization-defined security officials, and if classified information is found, the incident handling policy is enforced. |
| **AC-19(4).1.3.3** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-19(4).1.3.2.a; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-19(4).1.3.2.a to prohibit the connection of unclassified mobile devices to unclassified information systems. |
| **AC-19(4).1.3.4** | **Examine** authorization approvals for an agreed-upon [*basic*] sample of unclassified mobile devices connected to unclassified information systems; [*reviewing*] for evidence that the measures identified in AC-19(4).1.3.2.b are being applied to require approval from the appropriate authorizing official(s) as identified in AC-19(4).1.3.1 regarding the connection of unclassified mobile devices to unclassified information systems. |
| **AC-19(4).1.3.5** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-19(4).1.3.2.c; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-19(4).1.3.2.c to prohibit the use of internal or external modems or wireless interfaces within the mobile devices. |
| **AC-19(4).1.3.6** | **Examine** documentation for an agreed-upon [*basic*] sample of random reviews/inspections of mobile devices; [*reviewing*] for evidence that the measures identified in AC-19(4).1.3.2.d are being applied to ensure mobile devices and the information stored on those devices are subject to random reviews/inspections by the security officials identified in AC-19(4).1.2.1. |
| **AC-19(4).1.3.7** | **Examine** incident handling documentation for an agreed-upon [*basic*] sample of any incidents identified during random reviews/inspections, if applicable; [*reviewing*] for evidence that the measures identified in AC-19(4).1.3.2.d are being applied to enforce the incident handling policy if classified information is found on mobile devices during random reviews/inspections by the security officials identified in AC-19(4).1.2.1. |
| **AC-19(4).1.3.8** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-19(4).1.3.2.a; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
| **AC-19(4).1.3.9** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-19(4).1.3.2.c; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |