| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SC-18** | MOBILE CODE | |
| **SC-18.1**  **SC-18.1.1**  **SC-18.1.2**  **SC-18.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines acceptable and unacceptable mobile code and mobile code technologies;* 2. *the organization establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and* 3. *the organization authorizes, monitors, and controls the use of mobile code within the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; list of acceptable mobile code and mobile code technologies; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with mobile code authorization, monitoring, and control responsibilities].  **Test**: [*select from:* Mobile code authorization and monitoring capability for the organization]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, CM-6, CM-7, PL-4, SA-6, SA-7, 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. |
| **SC-18.1.1.1** | | **Examine** system and communications protection policy, mobile code implementation policy, procedures addressing mobile code, security plan, or other relevant documents; [*reviewing*] for acceptable and unacceptable mobile code and mobile code technologies. |
|  | |  |
| **SC-18.1.2.1** | | **Examine** system and communications protection policy, mobile code implementation policy, procedures addressing mobile code, security plan, or other relevant documents; [*reviewing*] for the usage restrictions and implementation guidance established for the acceptable mobile code and mobile code technologies identified in SC-18.1.1.1. |
|  | |  |
| **SC-18.1.3.1** | | **Examine** system and communications protection policy, mobile code implementation policy, procedures addressing mobile code, security plan, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to authorize, monitor, and control the use of mobile code within the information system. |
| **SC-18.1.3.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-18.1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-18.1.3.1. |
| **SC-18.1.3.3** | | **Examine** authorization records for an agreed-upon [*basic*] sample of mobile code within the information system; [*reviewing*] for evidence that the measures identified in SC-18.1.3.1 are being applied. |
| **SC-18.1.3.4** | | **Examine** an agreed-upon [*basic*] sample of mobile code monitoring records; [*reviewing*] for evidence that the measures identified in SC-18.1.3.1 are being applied. |
| **SC-18.1.3.5** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with mobile code authorization, monitoring, and control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in SC-18.1.3.1 are being applied. |
| **SC-18.1.3.6** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-18.1.3.1; 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)** | |
| **SC-18(1)** | MOBILE CODE |
| **SC-18(1).1**  **SC-18(1).1.1**  **SC-18(1).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the information system implements detection and inspection mechanisms to identify unauthorized mobile code; and* 2. *the information system takes corrective action when unauthorized mobile code is identified.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; 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 mobile code detection and inspection capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SI-3, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-18(1).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the detection and inspection mechanisms and their configuration settings to be employed to identify unauthorized mobile code. |
| **SC-18(1).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-18(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-18(1).1.1.1. |
| **SC-18(1).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-18(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **SC-18(1).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 take corrective action when unauthorized mobile code is identified. |
| **SC-18(1).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-18(1).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-18(1).1.2.1. |
| **SC-18(1).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-18(1).1.2.1; 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)** | |
| **SC-18(2)** | MOBILE CODE |
| **SC-18(2).1**  **SC-18(2).1.1**  **SC-18(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines requirements for the acquisition, development and/or use of mobile code; and* 2. *the organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets the organization-defined mobile code requirements.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with mobile code management responsibilities; organizational personnel with information system security, acquisition, and contracting responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: PS-7, SA-2, SA-4, SA-6, SA-9  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-18(2).1.1.1** | **Examine** system and communications protection policy, mobile code implementation policy, procedures addressing mobile code, security plan, or other relevant documents; [*reviewing*] for the requirements for the acquisition, development and/or use of mobile code. |
|  |  |
| **SC-18(2).1.2.1** | **Examine** system and communications protection policy, mobile code implementation policy, procedures addressing mobile, security plan, or other relevant documents; [*reviewing*] for the measures to ensure the acquisition, development, and/or use of mobile to be deployed in information systems meets the mobile code requirements identified in SC-18(2).1.1.1. |
| **SC-18(2).1.2.2** | **Examine** an agreed-upon [*basic*] sample of information system acquisition contracts, system development documentation, mobile code usage documentation, or other relevant documents associated with the deployment of mobile code in information systems, [*reviewing*] for evidence that the measures identified in SC-18(2).1.2.1 are being applied to meet the requirements identified in SC-18(2).1.1.1. |
| **SC-18(2).1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system security, acquisition, and contracting responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in SC-18(2).1.2.1 are being applied to meet the requirements identified in SC-18(2).1.1.1. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-18(3)** | MOBILE CODE |
| **SC-18(3).1**  **SC-18(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system* *prevents the download and execution of prohibited mobile code.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; 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 download and execution of prohibited mobile code]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, CM-7, PL-4, SA-6, SI-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-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 prevent the download and execution of prohibited mobile code. |
| **SC-18(3).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-18(3).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-18(3).1.1.1. |
| **SC-18(3).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-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)** | |
| **SC-18(4)** | MOBILE CODE |
| **SC-18(4).1**  **SC-18(4).1.1**  **SC-18(4).1.2**  **SC-18(4).1.3**  **SC-18(4).1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines software applications for which automatic mobile code execution is to be prohibited;* 2. *the organization defines actions required by the information system before executing mobile code;* 3. *the information system prevents the automatic execution of mobile code in the organization-defined software applications; and* 4. *the information system requires organization-defined actions before executing mobile code.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions; information system design documentation; information system configuration settings and associated documentation; list of applications for which automatic execution of mobile code must be prohibited; list of actions required before execution of mobile code; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms preventing mobile code execution within the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, CM-7, PL-4, SA-6, SI-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-18(4).1.1.1** | **Examine** system and communications protection policy, mode code implementation policy, procedures addressing mobile code, security plan, or other relevant documents; [*reviewing*] for the software applications for which automatic mobile code execution is to be prohibited. |
|  |  |
| **SC-18(4).1.2.1** | **Examine** system and communications protection policy, mobile code implementation policy, procedures addressing mobile code, security plan, or other relevant documents; [*reviewing*] for the actions required by the information system before executing mobile code. |
|  |  |
| **SC-18(4).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 prevent the automatic execution of mobile code in the software applications identified in SC-18(4).1.1.1. |
| **SC-18(4).1.3.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-18(4).1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-18(4).1.3.1. |
| **SC-18(4).1.3.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-18(4).1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **SC-18(4).1.4.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to require the actions identified in SC-18(4).1.2.1 before executing mobile code. |
| **SC-18(4).1.4.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-18(4).1.4.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-18(4).1.4.1. |
| **SC-18(4).1.4.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-18(4).1.4.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |