| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **MA-3** | MAINTENANCE TOOLS | |
| **MA-3.1**  **MA-3.1.1**  **MA-3.1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization approves, controls, and monitors the use of information system maintenance tools; and* 2. *the organization maintains information system maintenance tools on an ongoing basis.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: MA-2  concurrent controls: AC-2, AC-3, AU-3, CM-5, CM-6, PE-2, PE-3, PE-6, PE-7, PE-8,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. |
| **MA-3.1.1.1** | | **Examine** information system maintenance policy, procedures addressing information system maintenance tools, 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 approve, control, and monitor the use of, information system maintenance tools. |
| **MA-3.1.1.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in MA-3.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in MA-3.1.1.1. |
| **MA-3.1.1.3** | | **Examine** authorization approvals, maintenance records, information system monitoring records, information system audit records, access control records, or other relevant documents for an agreed-upon [*basic*] sample of information system maintenance tools; [*reviewing*] for evidence that the measures identified in MA-3.1.1.1 are being applied. |
|  | |  |
| **MA-3.1.2.1** | | **Examine** information system maintenance policy, procedures addressing information system maintenance tools, security plan, or other relevant documents; [*reviewing*] for the frequency to maintain information system maintenance tools on an ongoing basis. |
| **MA-3.1.2.2** | | **Examine** information system maintenance policy, procedures addressing information system maintenance tools, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to maintain information system maintenance tools in accordance with the frequency identified in MA-3.1.2.1. |
| **MA-3.1.2.3** | | **Examine** maintenance records, change control records, or other relevant documents for an agreed-upon [*basic*] sample of information system maintenance tools; [*reviewing*] for evidence that the measures identified in MA-3.1.2.2 are being applied. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **MA-3(1)** | | MAINTENANCE TOOLS |
| **MA-3(1).1**  **MA-3(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system maintenance responsibilities]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: MA-2  concurrent controls: PE-16  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **MA-3(1).1.1.1** | | **Examine** information system maintenance policy, procedures addressing information system maintenance tools, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to inspect all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications. |
| **MA-3(1).1.1.2** | | **Examine** an agreed-upon [*basic*] sample of inspection verifications, inspection checklists, inspection logs, or other relevant documents for information system maintenance tools carried into a facility by maintenance personnel; [*reviewing*] for evidence that the measures identified in MA-3(1).1.1.1 are being applied. |
| **MA-3(1).1.1.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in MA-3(1).1.1.1 are being applied. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **MA-3(2)** | MAINTENANCE TOOLS |
| **MA-3(2).1**  **MA-3(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization checks all media containing diagnostic and test programs (e.g., software or firmware used for information system maintenance or diagnostics) for malicious code before the media are used in the information system.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; information system media containing maintenance programs (including diagnostic and test programs); maintenance records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system maintenance responsibilities].  **Test**: [*select from:* Media checking process for malicious code detection]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: MA-2  concurrent controls: RA-5, SI-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **MA-3(2).1.1.1** | **Examine** information system maintenance policy, procedures addressing information system maintenance tools, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to check media, containing diagnostic and test programs, for malicious code before the media are used in the information system. |
| **MA-3(2).1.1.2** | **Examine** results of malicious code checks for an agreed-upon [*basic*] sample of information system media containing maintenance diagnostic and test programs; [*reviewing*] for evidence that the measures identified in MA-3(2).1.1.1 are being applied. |
| **MA-3(2).1.1.3** | **Examine** media checking process; [*observing*] for evidence that the measures identified in MA-3(2).1.1.1 are being applied. |
| **MA-3(2).1.1.4** | **Interview** organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in MA-3(2).1.1.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **MA-3(3)** | MAINTENANCE TOOLS |
| **MA-3(3).1**  **MA-3(3).1.1**  **MA-3(3).1.1a**  **MA-3(3).1.1b**  **MA-3(3).1.1c**  **MA-3(3).1.1d** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization prevents the unauthorized removal of maintenance equipment by one of the following:*   * *verifying that there is no organizational information contained on the equipment;* * *sanitizing or destroying the equipment;* * *retaining the equipment within the facility; or* * *obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; information system media containing maintenance programs (including diagnostic and test programs); maintenance records; equipment sanitization records; media sanitization records; exemptions for equipment removal; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system maintenance responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: MA-2  concurrent controls: MP-5, MP-6, PE-16  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **MA-3(3).1.1.1**  **MA-3(3).1.1.1.a**  **MA-3(3).1.1.1.b**  **MA-3(3).1.1.1.c**  **MA-3(3).1.1.1.d** | **Examine** information system maintenance policy, procedures addressing information system maintenance tools, security plan, or other relevant documents; [*reviewing*] for one or more of the following measures to be employed to prevent the unauthorized removal of maintenance equipment:   * verifying that there is no organizational information contained on the equipment; * sanitizing or destroying the equipment; * retaining the equipment within the facility; or * obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.   Note to assessor: The measures identified as being employed by the organization to prevent unauthorized removal of maintenance equipment should guide the selection of assessor actions MA-3(3).1.1.2 thru MA-3(3).1.1.9 as appropriate. |
| **MA-3(3).1.1.2** | **Examine** an agreed-upon [*basic*] sample of equipment maintenance records, equipment sanitization records, media sanitization records, or other relevant documents; [*reviewing*] for evidence that the measures identified in MA-3(3).1.1.1.a are being applied to verify that there is no organizational information contained on maintenance equipment. |
| **MA-3(3).1.1.3** | **Examine** an agreed-upon [*basic*] sample of equipment maintenance records, equipment sanitization records, media sanitization records, or other relevant documents; [*reviewing*] for evidence that the measures identified in MA-3(3).1.1.1.b are being applied to sanitize or destroy maintenance equipment. |
| **MA-3(3).1.1.4** | **Examine** an agreed-upon [*basic*] sample of equipment maintenance records or other relevant documents; [*reviewing*] for evidence that the measures identified in MA-3(3).1.1.1.c are being applied to retain maintenance equipment within the facility. |
| **MA-3(3).1.1.5** | **Examine** an agreed-upon [*basic*] sample of exemptions for equipment removal or other relevant documents; [*reviewing*] for evidence that the measures identified in MA-3(3).1.1.1.d are being applied to obtain an exemption from a designated organization official explicitly authorizing removal of maintenance equipment from the facility. |
| **MA-3(3).1.1.6** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in MA-3(3).1.1.1.a are being applied to verify that there is no organizational information contained on maintenance equipment. |
| **MA-3(3).1.1.7** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in MA-3(3).1.1.1.b are being applied to sanitize or destroy maintenance equipment. |
| **MA-3(3).1.1.8** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in MA-3(3).1.1.1.c are being applied to retain maintenance equipment within the facility. |
| **MA-3(3).1.1.9** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system maintenance responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in MA-3(3).1.1.1.d are being applied to obtain an exemption from a designated organization official explicitly authorizing removal of maintenance equipment from the facility. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **MA-3(4)** | MAINTENANCE TOOLS |
| **MA-3(4).1**  **MA-3(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; automated mechanisms supporting information system maintenance activities; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms supporting information system maintenance activities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: MA-2  concurrent controls: CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **MA-3(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 restrict the use of maintenance tools to authorized personnel only. |
| **MA-3(4).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in MA-3(4).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in MA-3(4).1.1.1. |
| **MA-3(4).1.1.3** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in MA-3(4).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |