| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **MA-2** | CONTROLLED MAINTENANCE | |
| **MA-2.1**  **MA-2.1.1**  **MA-2.1.2**  **MA-2.1.3**  **MA-2.1.4**  **MA-2.1.5** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization schedules, performs, documents, and reviews records*   *of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;*   1. *the organization controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;* 2. *the organization requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;* 3. *the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and* 4. *the organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization 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: AU-2, AU-3, AU-14, CM-2, CM-5, SA-5  concurrent controls: AC-2, AC-3, AC-17, CM-3, CM-4, CM-6, MP-6, PE-2, PE-3, PE-6,  PE-7, PE-8, PE-16, PL-4, PS-2, PS-3, PS-6, PS-7, SI-2, SI-4, SI-6  successor controls: MA-3, MA-4, MA-5, MA-6 |
| **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-2.1.1.1** | | **Examine** information system documentation; [*reviewing*] for manufacturer or vendor specifications and/or organizational requirements for maintenance and repairs on information system components. |
| **MA-2.1.1.2** | | **Examine** information system maintenance policy, procedures addressing controlled maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with the specifications and requirements identified in MA-2.1.1.1. |
| **MA-2.1.1.3** | | **Examine** maintenance schedules, maintenance activity reviews, and an agreed-upon [*basic*] sample of maintenance records for the information system; [*reviewing*] for evidence that the measures identified in MA-2.1.1.2 are being applied. |
| **MA-2.1.1.4** | | **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-2.1.1.2 are being applied. |
|  | |  |
| **MA-2.1.2.1** | | **Examine** information system maintenance policy, procedures addressing controlled maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to control maintenance activities performed on site. |
| **MA-2.1.2.2** | | **Examine** information system maintenance policy, procedures addressing controlled maintenance for the information system, 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 control maintenance activities performed remotely. |
| **MA-2.1.2.3** | | **Examine** information system maintenance policy, procedures addressing controlled maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to control maintenance activities for equipment serviced on site. |
| **MA-2.1.2.4** | | **Examine** information system maintenance policy, procedures addressing controlled maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to control maintenance activities for equipment removed to another location. |
| **MA-2.1.2.5** | | **Examine** access authorizations, service level agreements, maintenance records, change control records, information system monitoring records, information system audit records, or other relevant documents for an agreed-upon [*basic*] sample of maintenance activities performed on site; [*reviewing*] for evidence that the measures identified in MA-2.1.2.1 are being applied to control maintenance activities performed on site. |
| **MA-2.1.2.6** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in MA-2.1.2.2; [*reviewing*] for evidence that these mechanisms are configured as identified in MA-2.1.2.2 to control maintenance activities performed remotely. |
| **MA-2.1.2.7** | | **Examine** access authorizations, service level agreements, maintenance records, remote access control records, change control records, information system monitoring records, information system audit records, or other relevant documents for an agreed-upon [*basic*] sample of maintenance activities performed remotely; [*reviewing*] for evidence that the measures identified in MA-2.1.2.2 are being applied to control maintenance activities performed remotely. |
| **MA-2.1.2.8** | | **Examine** access authorizations, service level agreements, maintenance records, change control records, information system monitoring records, information system audit records, or other relevant documents for an agreed-upon [*basic*] sample of maintenance activities performed for equipment serviced on site; [*reviewing*] for evidence that the measures identified in MA-2.1.2.3 are being applied to control maintenance activities for equipment serviced on site. |
| **MA-2.1.2.9** | | **Examine** access authorizations, service level agreements, maintenance records, equipment removal records, equipment sanitization records, media sanitization records, change control records, or other relevant documents for an agreed-upon [*basic*] sample of maintenance activities performed for equipment removed to another location; [*reviewing*] for evidence that the measures identified in MA-2.1.2.4 are being applied to control maintenance activities for equipment removed to another location. |
| **MA-2.1.2.10** | | **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-2.1.2.1 are being applied to control maintenance activities performed on site. |
| **MA-2.1.2.11** | | **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-2.1.2.2 are being applied to control maintenance activities performed remotely. |
| **MA-2.1.2.12** | | **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-2.1.2.3 are being applied to control maintenance activities for equipment serviced on site. |
| **MA-2.1.2.13** | | **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-2.1.2.4 are being applied to control maintenance activities for equipment removed to another location. |
|  | |  |
| **MA-2.1.3.1** | | **Examine** information system maintenance policy, procedures addressing controlled maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the requirement that a designated official must explicitly approve the removal of information system or system components from organizational facilities for off-site maintenance or repairs. |
|  | |  |
| **MA-2.1.4.1** | | **Examine** information system maintenance policy, procedures addressing controlled maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs. |
| **MA-2.1.4.2** | | **Examine** equipment sanitization records, media sanitization records, or other relevant documents for an agreed-upon [*basic*] sample of equipment removed from organizational facilities for off-site maintenance or repairs; [*reviewing*] for evidence that the measures identified in MA-2.1.4.1 are being applied. |
| **MA-2.1.4.3** | | **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-2.1.4.1 are being applied. |
|  | |  |
| **MA-2.1.5.1** | | **Examine** information system maintenance policy, procedures addressing controlled maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to check for potential impacts to security controls before and after maintenance or repair actions to verify that the controls continue to function properly. |
| **MA-2.1.5.2** | | **Examine** security impact analyses, security control impact assessments, security function assessments, security function verifications, or other relevant documents for an agreed-upon [*basic*] sample of maintenance or repair actions; [*reviewing*] for evidence that the measures identified in MA-2.1.5.1 are being applied. |
| **MA-2.1.5.3** | | **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-2.1.5.1 are being applied. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **MA-2(1)** | | CONTROLLED MAINTENANCE |
| **MA-2(1).1**  **MA-2(1).1.1**  **MA-2(1).1.1a**  **MA-2(1).1.1b**  **MA-2(1).1.1c**  **MA-2(1).1.1d**  **MA-2(1).1.1e** | | **ASSESSMENT OBJECTIVE:**  *Determine if the organization maintains maintenance records for the information system that include:*   * *date and time of maintenance;* * *name of the individual performing the maintenance;* * *name of escort, if necessary;* * *a description of the maintenance performed; and* * *a list of equipment removed or replaced (including identification numbers, if applicable).*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; other relevant documents or records]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3  concurrent controls: CM-8, MP-6, PE-2, PE-3, PE-6, PE-7, PE-8, PE-16, PS-7  successor controls: MA-4, MA-5 |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **MA-2(1).1.1.1**  **MA-2(1).1.1.1.a**  **MA-2(1).1.1.1.b**  **MA-2(1).1.1.1.c**  **MA-2(1).1.1.1.d**  **MA-2(1).1.1.1.e** | | **Examine** information system maintenance policy, procedures addressing controlled maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to maintain maintenance records for the information system that include:   * Date and time of maintenance; * Name of the individual performing the maintenance; * Name of escort, if necessary; * A description of maintenance performed; and * A list of equipment removed or replaced (including identification numbers, if applicable). |
| **MA-2(1).1.2** | | **Examine** an agreed-upon [*basic*] sample of maintenance records stored or retained in maintenance logs for the information system; [*reviewing*] for evidence that the measures identified in MA-2(1).1.1.1 are being applied. |
| **MA-2(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-2(1).1.1.1 are being applied. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **MA-2(2)** | CONTROLLED MAINTENANCE |
| **MA-2(2).1**  **MA-2(2).1.1**  **MA-2(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs as required; and* 2. *the organization employs automated mechanisms to produce up-to-date, accurate, complete, and available records of all maintenance and repair actions needed, in process and complete.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system maintenance policy; procedures addressing controlled maintenance for the information system; automated mechanisms supporting information system maintenance activities; information system configuration settings and associated documentation; maintenance records; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, PE-8  successor controls: MA-4 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **MA-2(2).1.1.1** | **Examine** information system maintenance policy, procedures addressing controlled maintenance for the information system, security plan, or other relevant documents; [*reviewing*] for types of maintenance and repairs requiring the use of automated mechanisms to schedule, conduct, and document such maintenance and repairs. |
| **MA-2(2).1.1.2** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to schedule, conduct, and document the types of maintenance and repairs identified in MA-2(2).1.1.1. |
| **MA-2(2).1.1.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in MA-2(2).1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in MA-2(2).1.1.2. |
| **MA-2(2).1.1.4** | **Examine** maintenance schedules and maintenance records for an agreed-upon [*basic*] sample of the types of maintenance and repairs identified in MA-2(2).1.1.1; [*reviewing*] for evidence that the mechanisms and configurations identified in MA-2(2).1.1.2 are being applied. |
| **MA-2(2).1.1.5** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in MA-2(2).1.1.2; conducting [*basic*] testing using simulated events or conditions for evidence that these mechanisms are operating as intended. |
|  |  |
| **MA-2(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 produce up-to-date, accurate, complete, and available records of all maintenance and repair actions needed, in process, and completed. |
| **MA-2(2).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in MA-2(2).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in MA-2(2).1.2.1. |
| **MA-2(2).1.2.3** | **Examine** maintenance records for an agreed-upon [*basic*] sample of maintenance and repair actions needed, in process, and completed; [*reviewing*] for evidence that the mechanisms and configurations identified in MA-2(2).1.2.1 are being applied. |
| **MA-2(2).1.2.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in MA-2(2).1.2.1; conducting [*basic*] testing using simulated events or conditions for evidence that these mechanisms are operating as intended. |