| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SI-2** | FLAW REMEDIATION | |
| **SI-2.1**  **SI-2.1.1**  **SI-2.1.2**  **SI-2.1.3**  **SI-2.1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization* *identifies, reports, and corrects information system flaws;* 2. *the organization tests software updates related to flaw remediation for effectiveness before installation;* 3. *the organization tests software updates related to flaw remediation for potential side effects on organizational information systems before installation; and* 4. *the organization incorporates flaw remediation into the organizational configuration management process.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing flaw remediation; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with flaw remediation responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: RA-5  concurrent controls: CA-2, CA-7, CM-3, CM-4, IR-4, MA-2, SA-4, SA-11, SI-4, SI-11  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. |
| **SI-2.1.1.1** | | **Examine** system and information integrity policy, procedures addressing flaw remediation, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to identify, report, and correct information system flaws. |
| **SI-2.1.1.2** | | **Examine** an agreed-upon [*basic*] sample of flaw remediation reports, records of installed patches, services, hot fixes, and other software updates, or other relevant documents; [*reviewing*] for evidence that the measures identified in SI-2.1.1.1 are being applied. |
| **SI-2.1.1.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with flaw remediation responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in SI-2.1.1.1 are being applied. |
|  | |  |
| **SI-2.1.2.1** | | **Examine** system and information integrity policy, procedures addressing flaw remediation, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to test software updates related to flaw remediation for effectiveness before installation. |
| **SI-2.1.2.2** | | **Examine** software update test records, configuration management records, or other relevant records for an agreed-upon [*basic*] sample of software updates related to flaw remediation; [*reviewing*] for evidence that the measures identified in SI-2.1.2.1 are being applied. |
| **SI-2.1.2.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with flaw remediation responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in SI-2.1.2.1 are being applied. |
|  | |  |
| **SI-2.1.3.1** | | **Examine** system and information integrity policy, procedures addressing flaw remediation, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to test software updates related to flaw remediation for potential side effects on organizational information systems before installation. |
| **SI-2.1.3.2** | | **Examine** software update test records, configuration management records, or other relevant records for an agreed-upon [*basic*] sample of software updates related to flaw remediation; [*reviewing*] for evidence that the measures identified in SI-2.1.3.1 are being applied. |
| **SI-2.1.3.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with flaw remediation responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in SI-2.1.3.1 are being applied. |
|  | |  |
| **SI-2.1.4.1** | | **Examine** configuration management policy, procedures addressing configuration management, security plan, or other relevant documents; [*reviewing*] for the configuration management process. |
| **SI-2.1.4.2** | | **Examine** configuration management process; [*reviewing*] for the incorporation of flaw remediation into this process. |
| **SI-2.1.4.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with flaw remediation responsibilities; conducting [*basic*] discussions for further evidence that the configuration management process identified in SI-2.1.4.1 incorporates flaw remediation. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-2(1)** | FLAW REMEDIATION |
| **SI-2(1).1**  **SI-2(1).1.1**  **SI-2(1).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization centrally manages the flaw remediation process; and* 2. *the organization installs software updates automatically.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms supporting centralized management of flaw remediation and automatic software updates]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: RA-5  concurrent controls: CA-2, CA-7, CM-3, CM-4, CM-6, IR-4, MA-2, SA-11, SI-11  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-2(1).1.1.1** | **Examine** system and information integrity policy, procedures addressing flaw remediation, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including the process and/or the automated mechanisms and their configuration settings) to be employed to centrally manage the flaw remediation process. |
| **SI-2(1).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SI-2(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-2(1).1.1.1. |
| **SI-2(1).1.1.3** | **Examine** the process employed to centrally manage the flaw remediation process; [*reviewing*] for evidence that the process identified in SI-2(1).1.1.1 is being applied. |
| **SI-2(1).1.1.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in SI-2(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **SI-2(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 install software updates automatically. |
| **SI-2(1).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-2(1).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-2(1).1.2.1. |
| **SI-2(1).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-2(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)** | |
| **SI-2(2)** | FLAW REMEDIATION |
| **SI-2(2).1**  **SI-2(2).1.1**  **SI-2(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the frequency of employing automated mechanisms to determine the state of information system components with regard to flaw remediation; and* 2. *the organization employs automated mechanisms in accordance with the organization-defined frequency to determine the state of information system components with regard to flaw remediation.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing information system flaw remediation update status]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: RA-5  concurrent controls: CA-2, CA-7, CM-3, CM-4, CM-6, IR-4, MA-2, SA-11, SI-11  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-2(2).1.1.1** | **Examine** system and information integrity policy, procedures addressing flaw remediation, security plan, or other relevant documents; [*reviewing*] for the frequency of employing automated mechanisms to determine the state of information system components with regard to flaw remediation. |
|  |  |
| **SI-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 determine the state of information system components with regard to flaw remediation in accordance with the frequency identified in SI-2(2).1.1.1. |
| **SI-2(2).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-2(2).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-2(2).1.2.1. |
| **SI-2(2).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-2(2).1.2.1; 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)** | |
| **SI-2(3)** | FLAW REMEDIATION |
| **SI-2(3).1**  **SI-2(3).1.1**  **SI-2(3).1.2**  **SI-2(3).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the benchmarks to which the organization’s measurement of time elapsed between flaw identification and flaw remediation should be compared;* 2. *the organization measures the time between flaw identification and flaw remediation; and* 3. *the organization compares the time measured between flaw identification and flaw remediation with organization-defined benchmarks.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: RA-5  concurrent controls: CA-2, CA-7, CM-3, CM-4, CM-6, IR-4, SA-11, SI-11  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-2(3).1.1.1** | **Examine** system and information integrity policy, procedures addressing flaw remediation, security plan, or other relevant documents; [*reviewing*] for the benchmarks to which the organization’s measurement of time elapsed between flaw identification and flaw remediation should be compared. |
|  |  |
| **SI-2(3).1.2.1** | **Examine** system and information integrity policy, procedures addressing flaw remediation, security plan, or other relevant documents; [*reviewing*] for the process to be employed to measure the time elapsed between flaw identification and flaw remediation. |
| **SI-2(3).1.2.2** | **Examine** the process employed to measure the time elapsed between an agreed-upon [*basic*] sample of flaw identification records and corresponding flaw remediation records; [*reviewing*] for evidence that the process identified in SI-2(3).1.2.1 is being applied. |
|  |  |  |
| **SI-2(3).1.3.1** | **Examine** system and information integrity policy, procedures addressing flaw remediation, security plan, or other relevant documents; [*reviewing*] for the process to be employed to compare the time measured/elapsed, between flaw identification and flaw remediation, with the benchmarks identified in SI-2(3).1.1.1. |
| **SI-2(3).1.3.2** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with flaw remediation responsibilities; conducting [*basic*] discussions for evidence that the process identified in SI-2(3).1.3.1 is being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-2(4)** | FLAW REMEDIATION |
| **SI-2(4).1**  **SI-2(4).1.1**  **SI-2(4).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines information system components for which automated patch management tools are to be employed to facilitate flaw remediation; and* 2. *the organization employs automated patch management tools to facilitate flaw remediation to organization-defined information system components.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms facilitating flaw remediation to information system components]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: RA-5  concurrent controls: CA-2, CA-7, CM-3, CM-4, CM-6, IR-4, MA-2, SA-11, SI-11  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-2(4).1.1.1** | **Examine** system and information integrity policy, procedures addressing flaw remediation, security plan, or other relevant documents; [*reviewing*] for the information system components for which automated patch management tools are to be employed to facilitate flaw remediation. |
|  |  |
| **SI-2(4).1.2.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated patch management tools and their configuration settings to be employed to facilitate flaw remediation to the information system components identified in SI-2(4).1.1.1. |
| **SI-2(4).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-2(4).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-2(4).1.2.1. |
| **SI-2(4).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-2(4).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |