| **assessment case** | |
| --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | |
| **SI-3** | MALICIOUS CODE PROTECTION |
| **SI-3.1**  **SI-3.1.1**  **SI-3.1.1a**  **SI-3.1.1b**  **SI-3.1.2**  **SI-3.1.2a**  **SI-3.1.2b**  **SI-3.1.3**  **SI-3.1.4**  **SI-3.1.5**  **SI-3.1.5a**  **SI-3.1.5b**  **SI-3.1.5c**  **SI-3.1.6**  **SI-3.1.6a**  **SI-3.1.6b**  **SI-3.1.6c**  **SI-3.1.7** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code:*    * *transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means; or*    * *inserted through the exploitation of information system vulnerabilities;* 2. *the organization employs malicious code protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:*    * *transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means; or*    * *inserted through the exploitation of information system vulnerabilities;* 3. *the organization updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with configuration management policy and procedures defined in CM-1;* 4. *the organization defines the frequency of periodic scans of the information system by malicious code protection mechanisms;* 5. *the organization defines one or more of the following actions to be taken in response to malicious code detection:*    * *block malicious code;*    * *quarantine malicious code; and/or*    * *send alert to administrator;* 6. *the organization configures malicious code protection mechanisms to:*    * *perform periodic scans of the information system in accordance with organization-defined frequency;*    * *perform real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and*    * *take organization-defined action(s) in response to malicious code detection; and* 7. *the organization addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with malicious code protection responsibilities].  **Test**: [*select from:* Automated mechanisms implementing malicious code protection capability]. |

|  |  |
| --- | --- |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-1, RA-5  concurrent controls: CM-6, SA-4, SA-8, SA-12, SA-13, SI-4, SI-7, SI-8  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-3.1.1.1**  **SI-3.1.1.1.a**  **SI-3.1.1.1.b** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the malicious code protection mechanisms and their configuration settings to be employed at information system entry and exit points to detect and eradicate malicious code:   * + transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means; or   + inserted through the exploitation of information system vulnerabilities; |
| **SI-3.1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-3.1.1.1.a; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-3.1.1.1.a to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means. |
| **SI-3.1.1.3** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-3.1.1.1.b; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-3.1.1.1.b to detect and eradicate malicious code inserted through the exploitation of information system vulnerabilities. |
| **SI-3.1.1.4** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-3.1.1.1.a; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in SI-3.1.1.1.a to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means. |
| **SI-3.1.1.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-3.1.1.1.b; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in SI-3.1.1.1.b to detect and eradicate malicious code inserted through the exploitation of information system vulnerabilities. |
|  |  |
| **SI-3.1.2.1**  **SI-3.1.2.1.a**  **SI-3.1.2.1.b** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the malicious code protection mechanisms and their configuration settings to be employed at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:   * + transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means; or   + inserted through the exploitation of information system vulnerabilities; |
| **SI-3.1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-3.1.2.1.a; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-3.1.2.1.a to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means. |
| **SI-3.1.2.3** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-3.1.2.1.b; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-3.1.2.1.b to detect and eradicate malicious code inserted through the exploitation of information system vulnerabilities. |
| **SI-3.1.2.4** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-3.1.2.1.a; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in SI-3.1.2.1.a to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means. |
| **SI-3.1.2.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-3.1.2.1.b; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in SI-3.1.2.1.b to detect and eradicate malicious code inserted through the exploitation of information system vulnerabilities. |
|  |  |
| **SI-3.1.3.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to update malicious code protection mechanisms (including signature definitions), whenever new releases are available in accordance with configuration management policy and procedures defined in CM-1. |
| **SI-3.1.3.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-3.1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-3.1.3.1. |
| **SI-3.1.3.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-3.1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **SI-3.1.4.1** | **Examine** system and information integrity policy, procedures addressing malicious code protection, security plan, or other relevant documents; [*reviewing*] for the frequency of periodic scans of the information system by malicious code protection mechanisms. |
|  |  |
| **SI-3.1.5.1**  **SI-3.1.5.1.a**  **SI-3.1.5.1.b**  **SI-3.1.5.1.c** | **Examine** system and information integrity policy, procedures addressing malicious code protection, security plan, or other relevant documents; [*reviewing*] for one or more of the following actions to be taken in response to malicious code detection:   * + block malicious code;   + quarantine malicious code; and/or   + send alert to administrator; |
|  |  |
| **SI-3.1.6.1**  **SI-3.1.6.1.a**  **SI-3.1.6.1.b**  **SI-3.1.6.1.c** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the information system configurations to be employed to:   * + perform periodic scans of the information system in accordance with frequency identified in SI-3.1.4.1;   + perform real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and   + take the actions identified in SI-3.1.5.1 in response to malicious code detection. |
| **SI-3.1.6.2** | **Examine** an agreed-upon [*basic*] sample of the information system configuration settings identified in SI-3.1.6.1.a; [*reviewing*] for evidence that the information system is configured as identified in SI-3.1.6.1.a to perform periodic scans of the information system in accordance with the frequency identified in SI-3.1.4.1. |
| **SI-3.1.6.3** | **Examine** an agreed-upon [*basic*] sample of the information system configuration settings identified in SI-3.1.6.1.b; [*reviewing*] for evidence that the information system is configured as identified in SI-3.1.6.1.b to perform real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy. |
| **SI-3.1.6.4** | **Examine** an agreed-upon [*basic*] sample of the information system configuration settings identified in SI-3.1.6.1.c; [*reviewing*] for evidence that the information system is configured as identified in SI-3.1.6.1.c to take the actions identified in SI-3.1.5.1 in response to malicious code detection. |
|  |  |
| **SI-3.1.7.1** | **Examine** system and information integrity policy, procedures addressing malicious code protection, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. |
| **SI-3.1.7.2** | **Examine** an agreed-upon [*basic*] sample of reports addressing false positives during malicious code detection and eradication, or other relevant records; [*reviewing*] for evidence that the measures identified in SI-3.1.7.1 are being applied. |
| **SI-3.1.7.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with malicious code protection responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in SI-3.1.7.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-3(1)** | MALICIOUS CODE PROTECTION |
| **SI-3(1).1**  **SI-3(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization centrally manages malicious code protection mechanisms.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SA-4, RA-5, SA-8, SA-12, SA-13, SI-4, SI-7, SI-8  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-3(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 malicious code protection mechanisms. |
| **SI-3(1).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SI-3(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-3(1).1.1.1. |
| **SI-3(1).1.1.3** | **Examine** the process employed to centrally manage malicious code protection mechanisms; [*reviewing*] for evidence that the process identified in SI-3(1).1.1.1 is being applied. |
| **SI-3(1).1.1.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in SI-3(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)** | |
| **SI-3(2)** | MALICIOUS CODE PROTECTION |
| **SI-3(2).1**  **SI-3(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system automatically updates malicious code protection mechanisms, including signature definitions.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-3, CM-6, SI-8  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-3(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 automatically update malicious code protection mechanisms, including signature definitions. |
| **SI-3(2).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-3(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-3(2).1.1.1 |
| **SI-3(2).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-3(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)** | |
| **SI-3(3)** | MALICIOUS CODE PROTECTION |
| **SI-3(3).1**  **SI-3(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system prevents non-privileged users from circumventing malicious code protection capabilities.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing malicious code protection capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, AC-5, AC-6, CM-6, SI-8  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-3(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 non-privileged users from circumventing malicious code protection capabilities. |
| **SI-3(3).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-3(3).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-3(3).1.1.1 |
| **SI-3(3).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-3(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)** | |
| **SI-3(4)** | MALICIOUS CODE PROTECTION |
| **SI-3(4).1**  **SI-3(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system updates malicious code protection mechanisms only when directed by a privileged user.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing malicious code protection capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, AC-6, CM-3, CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-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 update malicious code protection mechanisms only when directed by a privileged user. |
| **SI-3(4).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-3(4).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-3(4).1.1.1. |
| **SI-3(4).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-3(4).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-3(5)** | MALICIOUS CODE PROTECTION |
| **SI-3(5).1**  **SI-3(5).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization does not allow users to introduce removable media into the information system.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with malicious code protection responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-6, AC-19  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-3(5).1.1.1** | **Examine** system and information integrity policy, procedures addressing malicious code protection, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to not allow users to introduce removable media into the information system. |
| **SI-3(5).1.1.2** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with malicious code protection responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in SI-3(5).1.1.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 6** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-3(6)** | MALICIOUS CODE PROTECTION |
| **SI-3(6).1**  **SI-3(6).1.1**  **SI-3(6).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the frequency of testing malicious code protection mechanisms; and* 2. *the organization tests malicious code protection mechanisms, in accordance with organization-defined frequency, by introducing a known benign, non-spreading test case into the information system and subsequently verifying that both detection of the test case and associated incident reporting occur, as required.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing malicious code protection capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: None  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-3(6).1.1.1** | **Examine** system and information integrity policy, procedures malicious code protection, security plan, or other relevant documents; [*reviewing*] for the frequency of testing malicious code protection mechanisms. |
|  |  |
| **SI-3(6).1.2.1** | **Examine** system and information integrity policy, procedures malicious code protection, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to test malicious code protections, in accordance with the frequency identified in SI-3(6).1.1.1, by introducing a known benign, non-spreading test case into the information system and subsequently verifying that both detection of the test case and associated incident reporting occur, as required. |
| **SI-3(6).1.2.2** | **Examine** an agreed-upon [*basic*] sample of records testing malicious code protection mechanisms; [*reviewing*] for evidence that the measures identified in SI-3(6).1.2.1 are being applied. |
| **SI-3(6).1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with malicious code protection responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in SI-3(6).1.2.1 are being applied. |