| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SI-8** | SPAM PROTECTION | |
| **SI-8.1**  **SI-8.1.1**  **SI-8.1.2**  **SI-8.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means;* 2. *the organization employs spam protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means; and* 3. *the organization updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures defined in CM-1.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with spam protection responsibilities].  **Test**: [*select from:* Automated mechanisms implementing spam detection and handling capability]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-1  concurrent controls: CM-3, CM-6, SI-3, SI-4, SC-5  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-8.1.1.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the spam protection mechanisms and their configuration settings to be employed at information system entry and exit points to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means. |
| **SI-8.1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-8.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-8.1.1.1. |
| **SI-8.1.1.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-8.1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |  |
| **SI-8.1.2.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the spam protection mechanisms and their configuration settings to be employed at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means. |
| **SI-8.1.2.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-8.1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-8.1.2.1. |
| **SI-8.1.2.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-8.1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |  |
| **SI-8.1.3.1** | | **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 spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures defined in CM-1. |
| **SI-8.1.3.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-8.1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-8.1.3.1. |
| **SI-8.1.3.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-8.1.3.1; 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)** | |
| **SI-8(1)** | SPAM PROTECTION |
| **SI-8(1).1**  **SI-8(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization centrally manages spam protection mechanisms.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; 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-3, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-8(1).1.1.1** | **Examine** system and information integrity policy, procedures addressing spam protection, 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 spam protection mechanisms. |
| **SI-8(1).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SI-8(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-8(1).1.1.1. |
| **SI-8(1).1.1.3** | **Examine** the process employed to centrally manage spam protection mechanisms; [*reviewing*] for evidence that the process identified in SI-8(1).1.1.1 is being applied. |
| **SI-8(1).1.1.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in SI-8(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-8(2)** | SPAM PROTECTION |
| **SI-8(2).1**  **SI-8(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system automatically updates spam protection mechanisms (including signature definitions).*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; 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-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-8(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 spam protection mechanisms (including signature definitions). |
| **SI-8(2).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-8(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-8(2).1.1.1. |
| **SI-8(2).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-8(2).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |