| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SI-4** | INFORMATION SYSTEM MONITORING | |
| **SI-4.1**  **SI-4.1.1**  **SI-4.1.2**  **SI-4.1.3**  **SI-4.1.4**  **SI-4.1.4a**  **SI-4.1.4b**  **SI-4.1.5**  **SI-4.1.6** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines objectives for monitoring events on the information system;* 2. *the organization monitors events on the information system in accordance with organization-defined objectives and detects information system attacks;* 3. *the organization identifies unauthorized use of the information system;* 4. *the organization deploys monitoring devices:*    * *strategically within the information system to collect organization-determined essential information; and*    * *at ad hoc locations within the system to track specific types of transactions of interest to the organization;* 5. *the organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and* 6. *the organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system monitoring responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, AC-8, AC-17, AU-2, AU-6, CA-2, CA-7, CM-4, RA-3, SI-3, 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-4.1.1.1** | **Examine** system and information integrity policy, procedures addressing information system monitoring tools and techniques, security plan, or other relevant documents; [*reviewing*] for the objectives for monitoring events on the information system. |
|  |  |
| **SI-4.1.2.1** | **Examine** system and information integrity policy, procedures addressing information system monitoring tools and techniques, information system design documentation, security plan, or other relevant documents; [*reviewing*] for the measures (including the process and/or the automated mechanisms and their configuration settings) to be employed to monitor events on the information system in accordance with the objectives identified in SI-4.1.1.1 and detect information system attacks. |
| **SI-4.1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SI-4.1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4.1.2.1. |
| **SI-4.1.2.3** | **Examine** the process employed to monitor events on the information system; [*reviewing*] for evidence that the process identified in SI-4.1.2.1 is being applied. |
| **SI-4.1.2.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in SI-4.1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **SI-4.1.3.1** | **Examine** system and information integrity policy, procedures addressing information system monitoring tools and techniques, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to identify unauthorized use of the information system. |
| **SI-4.1.3.2** | **Examine** information system audit records, information system monitoring records, or other relevant records associated with an agreed-upon [*basic*] sample of events identified as unauthorized use of the information system; [*reviewing*] for evidence that the measures identified in SI-4.1.3.1 are being applied. |
|  |  |
| **SI-4.1.4.1**  **SI-4.1.4.1.a**  **SI-4.1.4.1.b** | **Examine** system and information integrity policy, procedures addressing information system monitoring tools and techniques, security plan, or other relevant documents; [*reviewing*] for monitoring devices to be deployed:   * + strategically within the information system to collect organization-determined essential information; and   + at ad hoc locations within the system to track specific types of transactions of interest to the organization. |
|  |  |
| **SI-4.1.5.1** | **Examine** system and information integrity policy, procedures information system monitoring tools and techniques, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to heighten the level of information system monitoring activity whenever there is an indication of increased risks to the operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. |
| **SI-4.1.5.2** | **Examine** risk assessments, security impact analyses, security assessments, change control records, continuous monitoring records, or other relevant documents associated with, or resulting from, heightening the level of information system monitoring activities; [*reviewing*] for evidence that the measures identified in SI-4.1.5.1 are being applied. |
| **SI-4.1.5.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system monitoring responsibilities; conducting [*basic*] discussions for evidence that the measures identified in SI-4.1.5.1 are being applied. |
|  |  |
| **SI-4.1.6.1** | **Examine** system and information integrity policy, procedures information system monitoring, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations. |
| **SI-4.1.6.2** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system monitoring responsibilities; conducting [*basic*] discussions for evidence that the measures identified in SI-4.1.6.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-4(1)** | INFORMATION SYSTEM MONITORING |
| **SI-4(1).1**  **SI-4(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records].  **Test**: [*select from:* Information system-wide intrusion detection capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CA-3, CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(1).1.1.1** | **Examine** system and information integrity policy, procedures addressing information system monitoring tools and techniques, security plan, or other relevant documents; [*reviewing*] for the common protocols to be used to interconnect and configure individual intrusion detection tools into a system-wide intrusion detection system. |
| **SI-4(1).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 interconnect and configure individual intrusion detection tools into a system-wide intrusion detection system using the common protocols identified in SI-4(1).1.1.1. |
| **SI-4(1).1.1.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(1).1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(1).1.1.2. |
| **SI-4(1).1.1.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in SI-4(1).1.1.2; 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-4(2)** | INFORMATION SYSTEM MONITORING |
| **SI-4(2).1**  **SI-4(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated tools to support near real-time analysis of events.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols documentation; other relevant documents or records].  **Test**: [*select from:* Automated tools supporting near real-time event analysis]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AU-6, CM-6, IR-5, PE-6, SI-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(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 support near real-time analysis of events. |
| **SI-4(2).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(2).1.1.1. |
| **SI-4(2).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-4(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-4(3)** | INFORMATION SYSTEM MONITORING |
| **SI-4(3).1**  **SI-4(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records].  **Test**: [*select from:* Automated tools supporting the integration of intrusion detection tools and access/flow control mechanisms]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, AC-4, CM-6, IR-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(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 integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination. |
| **SI-4(3).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(3).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(3).1.1.1. |
| **SI-4(3).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-4(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-4(4)** | INFORMATION SYSTEM MONITORING |
| **SI-4(4).1**  **SI-4(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records].  **Test**: [*select from:* Automated tools supporting the integration of intrusion detection tools and access/flow control mechanisms]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AU-6, CM-6, IR-5, SI-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(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 monitor inbound and outbound communications for unusual or unauthorized activities or conditions. |
| **SI-4(4).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(4).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(4).1.1.1. |
| **SI-4(4).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-4(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-4(5)** | INFORMATION SYSTEM MONITORING |
| **SI-4(5).1**  **SI-4(5).1.1**  **SI-4(5).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization* *defines indicators of compromise or potential compromise to the security of the information system; and* 2. *the information system provides near real-time alerts when any of the organization-defined list of compromise or potential compromise indicators occurs.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; security plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Information system monitoring real-time alert capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AU-6, CM-6, IR-4, IR-5 IR-6, PE-6, SI-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(5).1.1.1** | **Examine** system and communications protection policy, procedures addressing information system monitoring tools and techniques, security plan, or other relevant documents; [*reviewing*] for the indicators of compromise or potential compromise to the security of the information system. |
|  |  |
| **SI-4(5).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 provide near real-time alerts when any of the compromise or potential compromise indicators identified in SI-4(5).1.1.1 occurs. |
| **SI-4(5).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(5).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(5).1.2.1. |
| **SI-4(5).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-4(5).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 6** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-4(6)** | INFORMATION SYSTEM MONITORING |
| **SI-4(6).1**  **SI-4(6).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records].  **Test**: [*select from:* Information system-wide intrusion detection and prevention capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-5, AC-6, CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(6).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 intrusion detection and prevention capabilities. |
| **SI-4(6).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(6).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(6).1.1.1. |
| **SI-4(6).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-4(6).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 7** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-4(7)** | INFORMATION SYSTEM MONITORING |
| **SI-4(7).1**  **SI-4(7).1.1**  **SI-4(7).1.2**  **SI-4(7).1.3**  **SI-4(7).1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines incident response personnel (identified by name and/or by role) to be notified of suspicious events;* 2. *the organization defines least-disruptive actions to be taken by the information system to terminate suspicious events;* 3. *the information system notifies organization-defined incident response personnel of suspicious events; and* 4. *the information system takes organization-defined least-disruptive actions to terminate suspicious events.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols documentation; other relevant documents or records].  **Test**: [*select from:* Information system notification capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, IR-4, IR-5 IR-6, SI-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(7).1.1.1** | **Examine** system and communications protection policy, procedures addressing information system monitoring tools and techniques, security plan, or other relevant documents; [*reviewing*] for the incident response personnel (identified by name and/or by role) to be notified of suspicious events. |
|  |  |
| **SI-4(7).1.2.1** | **Examine** system and communications protection policy, procedures addressing information system monitoring tools and techniques, security plan, or other relevant documents; [*reviewing*] for the least-disruptive actions to be taken by the information system to terminate suspicious events. |
|  |  |
| **SI-4(7).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 notify the incident response personnel identified in SI-4(7).1.1.1 of suspicious events. |
| **SI-4(7).1.3.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(7).1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(7).1.3.1. |
| **SI-4(7).1.3.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-4(7).1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
| **SI-4(7).1.4.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to take the actions identified in SI-4(7).1.2.1 to terminate suspicious events. |
| **SI-4(7).1.4.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(7).1.4.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(7).1.4.1. |
| **SI-4(7).1.4.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-4(7).1.4.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |
| **ASSESSMENT – Control Enhancement 8** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-4(8)** | INFORMATION SYSTEM MONITORING |
| **SI-4(8).1**  **SI-4(8).1.1**  **SI-4(8).1.1a**  **SI-4(8).1.1b**  **SI-4(8).1.1c** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization protects information obtained from intrusion-monitoring tools from:*   * *unauthorized access;* * *modification; and* * *deletion.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system monitoring responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, AC-6, CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(8).1.1.1**  **SI-4(8).1.1.1a**  **SI-4(8).1.1.1b**  **SI-4(8).1.1.1c** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to protect information obtained from intrusion-monitoring tools from:   * unauthorized access; * modification; and * deletion. |
| **SI-4(8).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(8).1.1.1.a; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(8).1.1.1.a to protect information obtained from intrusion-monitoring tools from unauthorized access. |
| **SI-4(8).1.1.3** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(8).1.1.1.b; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(8).1.1.1.b to protect information obtained from intrusion-monitoring tools from modification. |
| **SI-4(8).1.1.4** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(8).1.1.1.c; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(8).1.1.1.c to protect information obtained from intrusion-monitoring tools from deletion. |
| **SI-4(8).1.1.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-4(8).1.1.1.a; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in SI-4(8).1.1.1.a to protect information obtained from intrusion-monitoring tools from unauthorized access. |
| **SI-4(8).1.1.6** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-4(8).1.1.1.b; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in SI-4(8).1.1.1.b to protect information obtained from intrusion-monitoring tools from modification. |
| **SI-4(8).1.1.7** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-4(8).1.1.1.c; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in SI-4(8).1.1.1.c to protect information obtained from intrusion-monitoring tools from deletion. |
|  | |
| **ASSESSMENT – Control Enhancement 9** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-4(9)** | INFORMATION SYSTEM MONITORING |
| **SI-4(9).1**  **SI-4(9).1.1**  **SI-4(9).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the time period for testing/exercising intrusion-monitoring tools; and* 2. *the organization tests/exercises intrusion-monitoring tools in accordance with organization-defined time period.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; documentation providing evidence of testing intrusion monitoring tools; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: None  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(9).1.1.1** | **Examine** system and information integrity policy, procedures addressing information system monitoring tools and techniques, security plan, or other relevant documents; [*reviewing*] for the time period for testing/exercising intrusion-monitoring tools. |
| **SI-4(9).1.1.2** | **Examine** system and information integrity policy, procedures addressing information system monitoring tools and techniques, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to test/exercise intrusion –monitoring tools in accordance with the time period identified in SI-4(9).1.1.1. |
|  |  |
| **SI-4(9).1.2.2** | **Examine** an agreed-upon [*basic*] sample of tests/exercises conducted for intrusion-monitoring tools; [*reviewing*] for evidence that the measures identified in SI-4(9).1.2.2 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 10** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-4(10)** | INFORMATION SYSTEM MONITORING |
| **SI-4(10).1**  **SI-4(10).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization makes provisions so that encrypted traffic is visible to information system monitoring tools.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: SC-7, SC-9  concurrent controls: CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(10).1.1.1** | **Examine** system and information integrity policy, procedures addressing information system monitoring tools and techniques, security plan, information system design documentation, security plan, or other relevant documents; [*reviewing*] for the provisions (including the process and/or automated mechanisms and configuration settings) to be employed so that encrypted traffic is visible to information system monitoring tools. |
| **SI-4(10).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(10).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(10).1.1.1. |
| **SI-4(10).1.1.3** | **Examine** the process employed to make provisions so that encrypted traffic is visible to information system monitoring tools; [*reviewing*] for evidence that the process identified in SI-4(10).1.1.1 is being applied. |
| **SI-4(10).1.1.4** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-4(10).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 11** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-4(11)** | INFORMATION SYSTEM MONITORING |
| **SI-4(11).1**  **SI-4(11).1.1**  **SI-4(11).1.1a**  **SI-4(11).1.1b** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization to discover anomalies analyzes outbound communications traffic at:*   * *the external boundary of the system (i.e., system perimeter); and* * *as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems).*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system monitoring logs or records; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-7, SI-3, SI-8  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(11).1.1.1** | **Examine** security plan, information system design documentation, information system architecture documentation, or other relevant documents; [*reviewing*] for the selected interior points within the system (e.g., subnets, subsystem) deemed necessary for analysis to discover potential anomalies. |
| **SI-4(11).1.1.2**  **SI-4(11).1.1.2.a**  **SI-4(11).1.1.2.b** | **Examine** security plan, information system design documentation, or other relevant documents, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed analyze outbound communications traffic in order to discover anomalies at:   * the external boundary of the system (i.e., system perimeter); and * as deemed necessary, the selected interior points identified in SI-4(11).1.1.1. |
| **SI-4(11).1.1.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(11).1.1.2.a; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(11).1.1.2.a to analyze communications traffic at the external boundary of the system (i.e., system perimeter). |
| **SI-4(11).1.1.4** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(11).1.1.2.b; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(11).1.1.2.b to analyze communications at the selected interior points identified in SI-4(11).1.1.1. |
| **SI-4(11).1.1.5** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in SI-4(11).1.1.2.a; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in SI-4(11).1.1.2.a to analyze communications traffic at the external boundary of the system (i.e., system perimeter). |
| **SI-4(11).1.1.6** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in SI-4(11).1.1.1.b; conducting [*basic*] testing for evidence that these mechanisms are operating as intended SI-4(11).1.1.1.b to analyze communications at the selected interior points identified in SI-4(11).1.1.1. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 12** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-4(12)** | INFORMATION SYSTEM MONITORING |
| **SI-4(12).1**  **SI-4(12).1.1**  **SI-4(12).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines inappropriate or unusual activities with security implications that should trigger alerts to security personnel; and* 2. *the organization employs automated mechanisms to alert security personnel of the organization-defined inappropriate or unusual activities with security implications.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; list of inappropriate or unusual activities that trigger alerts; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing alerts to security personnel for inappropriate or unusual activities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, IR-4, IR-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(12).1.1.1** | **Examine** system and communications protection policy, procedures addressing information system monitoring tools and techniques, security plan, or other relevant documents; [*reviewing*] for the inappropriate or unusual activities with security implications that should trigger alerts to security personnel. |
|  |  |
| **SI-4(12).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 alert security personnel of the inappropriate or unusual activities identified in SI-4(12).1.1.1. |
| **SI-4(12).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(12).1.2.1.; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(12).1.2.1. |
| **SI-4(12).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SI-4(12).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 13** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-4(13)** | INFORMATION SYSTEM MONITORING |
| **SI-4(13).1**  **SI-4(13).1.1**  **SI-4(13).1.2**  **SI-4(13).1.3**  **SI-4(13).1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization analyzes communications traffic/event patterns for the information system;* 2. *the organization develops profiles representing common traffic patterns and/or events;* 3. *the organization defines the respective measurements to which the organization must tune system monitoring devices to reduce the number of false positives and false negatives; and* 4. *the organization uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and false negatives to their respective organization-defined measures.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; list of common traffic patterns and/or events; information system protocols documentation; list of acceptable thresholds for false positives and false negatives; other relevant documents or records].  **Interview:** [*select from:* Organizational personnel with information system monitoring responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, SC-7, SI-3, SI-8  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(13).1.1.1** | **Examine** system and information integrity policy, procedures addressing information system monitoring tools and techniques, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to analyze communications traffic/event patterns for the information system. |
| **SI-4(13).1.1.2** | **Examine** an agreed-upon [*basic*] sample of traffic/event patterns records and analyses; [*reviewing*] for evidence that the measures identified in SI-4(13).1.1.1 are being applied. |
| **SI-4(13).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system monitoring responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in SI-4(13).1.1.1 are being applied. |
|  |  |
| **SI-4(13).1.2.1** | **Examine** system and information integrity policy, procedures addressing information system monitoring tools and techniques, information system monitoring tools and techniques documentation, security plan, or other relevant documents; [*reviewing*] for a list of profiles representing common traffic patterns and/or events. |
|  |  |
| **SI-4(13).1.3.1** | **Examine** system and information integrity policy, procedures addressing information system monitoring tools and techniques, security plan, information system monitoring tools and techniques documentation, or other relevant documents; [*reviewing*] for the respective measurements to which the organization must tune system monitoring devices to reduce the number of false positives and false negatives. |
|  |  |
| **SI-4(13).1.4.1** | **Examine** security plan, information system design documentation, information system monitoring tools and techniques documentation, or other relevant documents; [*reviewing*] for the system-monitoring devices and their configuration settings to be employed using the traffic/event profiles identified in SI-4(13).1.2.1 to tune these devices to reduce the number of false positives and false negatives to their respective measures identified in SI-4(13).1.3.1. |
| **SI-4(13).1.4.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the system-monitoring devices identified in SI-4(13).1.4.1; [*reviewing*] for evidence that these devices are configured as identified in SI-4(13).1.4.1. |
| **SI-4(13).1.4.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system monitoring responsibilities; conducting [*basic*] discussions for further evidence that the traffic/event profiles identified in SI-4(13).1.2.1 are being used in tuning system-monitoring devices to reduce the number of false positives and false negatives to their respective measurements identified in SI-4(13).1.3.1. |
| **SI-4(13).1.4.4** | **Test** an agreed-upon [*basic*] sample of the system-monitoring devices and their configuration settings identified in SI-4(13).1.4.1; conducting [*basic*] testing for evidence that these devices are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 14** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-4(14)** | INFORMATION SYSTEM MONITORING |
| **SI-4(14).1**  **SI-4(14).1.1**  **SI-4(14).1.1a**  **SI-4(14).1.1b**  **SI-4(14).1.1c** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs a wireless intrusion detection system to:*   * *identify rogue wireless devices to the information system;* * *detect attack attempts to the information system; and* * *detect potential compromises/breaches to the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing wireless communications intrusion detection capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, AC-8, CM-6, SC-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(14).1.1.1**  **SI-4(14).1.1.1.a**  **SI-4(14).1.1.1.b**  **SI-4(14).1.1.1.c** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the wireless intrusion detection system mechanisms and their configuration settings to be employed to:   * identify rogue wireless devices to the information system; * detect attack attempts to the information system; and * detect potential compromises/breaches to the information system. |
| **SI-4(14).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the wireless intrusion detection system mechanisms identified in SI-4(14).1.1.1.a [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(14).1.1.1.a to identify rogue wireless devices to the information system. |
| **SI-4(14).1.1.3** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the wireless intrusion detection system mechanisms identified in SI-4(14).1.1.1.b [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(14).1.1.1.b to detect attack attempts to the information system. |
| **SI-4(14).1.1.4** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the wireless intrusion detection system mechanisms identified in SI-4(14).1.1.1.c [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(14).1.1.1.c to detect potential compromises/breaches to the information system. |
| **SI-4(14).1.1.5** | **Test** an agreed-upon [*basic*]sample of the wireless intrusion detection system mechanisms and their configuration settings identified in SI-4(14).1.1.1.a; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in SI-4(14).1.1.1.a to identify rogue wireless devices to the information system. |
| **SI-4(14).1.1.6** | **Test** an agreed-upon [*basic*]sample of the wireless intrusion detection system mechanisms and their configuration settings identified in SI-4(14).1.1.1.b; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in SI-4(14).1.1.1.b to detect attack attempts to the information system. |
| **SI-4(14).1.1.7** | **Test** an agreed-upon [*basic*]sample of the wireless intrusion detection system mechanisms and their configuration settings identified in SI-4(14).1.1.1.c; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in SI-4(14).1.1.1.c to detect potential compromises/breaches to the information system. |
|  | |
| **ASSESSMENT – Control Enhancement 15** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-4(15)** | INFORMATION SYSTEM MONITORING |
| **SI-4(15).1**  **SI-4(15).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing wireless communications intrusion detection capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, AC-8, CM-6, SC-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(15).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the intrusion detection system mechanisms and their configuration settings to be employed to monitor wireless communications traffic as the traffic passes from wireless to wireline networks. |
| **SI-4(15).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the intrusion detection system mechanisms identified in SI-4(15).1.1.1.; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(15).1.1.1. |
| **SI-4(15).1.1.3** | **Test** an agreed-upon [*basic*]sample of the intrusion detection system mechanisms and their configuration settings identified in SI-4(15).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 16** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-4(16)** | INFORMATION SYSTEM MONITORING |
| **SI-4(16).1**  **SI-4(16).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization correlates information from monitoring tools employed throughout the information system to achieve organization-wide situational awareness.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; event correlation logs or records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system monitoring responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AU-6, CM-6, PE-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(16).1.1.1** | **Examine** system and information integrity policy, procedures information system monitoring tools and techniques, 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 correlate information from monitoring tools employed throughout the information system to achieve organization-wide situational awareness. |
| **SI-4(16).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(16).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(16).1.1.1. |
| **SI-4(16).1.1.3** | **Examine** the process employed to correlate information from monitoring tools employed throughout the information system; [*observing*] for evidence that the process identified in SI-4(16).1.1.1 is being applied. |
| **SI-4(16).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system monitoring responsibilities; conducting [*basic*] discussions for further evidence that measures identified in SI-4(16).1.1.1 are being applied. |
| **SI-4(16).1.1.5** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in SI-4(16).1.1.1 using an agreed-upon [*basic*] sample of simulated information from monitoring tools; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 17** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SI-4(17)** | INFORMATION SYSTEM MONITORING |
| **SI-4(17).1**  **SI-4(17).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization correlates results from monitoring physical, cyber, and supply chain activities to achieve integrated situational awareness.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; event correlation logs or records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system monitoring responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AU-6, CM-6, PE-6, SA-12  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SI-4(17).1.1.1** | **Examine** system and information integrity policy, procedures information system monitoring tools and techniques, 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 correlate results from monitoring physical, cyber, and supply chain activities to achieve integrated situational awareness. |
| **SI-4(17).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in SI-4(17).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SI-4(17).1.1.1. |
| **SI-4(17).1.1.3** | **Examine** the process employed to correlate results from monitoring physical, cyber, and supply chain activities; [*observing*] for evidence that the process identified in SI-4(17).1.1.1 is being applied. |
| **SI-4(17).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system monitoring responsibilities; conducting [*basic*] discussions for further evidence that measures identified in SI-4(17).1.1.1 are being applied. |
| **SI-4(17).1.1.5** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in SI-4(17).1.1.1 using an agreed-upon [*basic*] sample of simulated monitoring activities; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |