| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SA-12** | SUPPLY CHAIN PROTECTION | |
| **SA-12.1**  **SA-12.1.1**  **SA-12.1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the measures to be employed to protect against supply chain threats; and* 2. *the organization protects against supply chain threats by employing organization-defined measures as part of a comprehensive, defense-in-breadth information security strategy.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; acquisition contracts and service level agreements; list of supply chain threats; list of measures to be taken against supply chain threats; information system development life cycle documentation; other relevant documents or records]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: RA-3, SA-8  concurrent controls: CA-2, CM-2, CM-6, SC-34, SI-3, PE-16  successor controls: SA-4, SA-9, SA-13, SA-14 |
| **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. |
| **SA-12.1.1.1** | | **Examine** system and services acquisition policy, procedures addressing supply chain protection, procedures addressing the integration of information security requirements and/or security specifications into the acquisition process, solicitation documentation, acquisition documentation, acquisition contracts for information system services, service level agreements, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to protect against supply chain threats. |
|  | |  |
| **SA-12.1.2.1** | | **Examine** list of supply chain threats and corresponding measures employed to protect an agreed-upon [*basic*] sample of information systems against supply chain threats; [*reviewing*] for evidence that the measures identified in SA-12.1.1.1 are being applied as part of a comprehensive, defense-in-breadth information security strategy to protect against supply chain threats. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **SA-12(1)** | | SUPPLY CHAIN PROTECTION |
| **SA-12(1).1**  **SA-12(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the organization purchases all anticipated information system components and spares in the initial acquisition.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: None  successor controls: MA-6, SA-4, SA-13, SA-14 |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **SA-12(1).1.1.1** | | **Examine** system and services acquisition policy, procedures addressing supply chain protection, procedures addressing the integration of information security requirements and/or security specifications into the acquisition process, solicitation documentation, acquisition documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to purchase all anticipated information system components and spares in the initial acquisition. |
| **SA-12(1).1.1.2** | | **Examine** inventory reports, purchase orders, invoices, or other relevant documents associated with the initial acquisition of information system components and spares for the information system; [*reviewing*] for evidence that the measures identified in SA-12(1).1.1.1 are being applied. |
| **SA-12(1).1.1.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system security, acquisition, and contracting responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in SA-12(1).1.1.1 are being applied. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-12(2)** | SUPPLY CHAIN PROTECTION |
| **SA-12(2).1**  **SA-12(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; due diligence reviews documentation; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with supply chain protection responsibilities; organizational personnel with information system security, acquisition, and contracting responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: RA-3  concurrent controls: CA-2  successor controls: SA-4, SA-9, SA-13, SA-14 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-12(2).1.1.1** | **Examine** system and services acquisition policy, procedures addressing supply chain protection, procedures addressing the integration of information security requirements and/or security specifications into the acquisition process, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to conduct a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services. |
| **SA-12(2).1.1.2** | **Examine** due diligence reviews for an agreed-upon [*basic*] sample of acquisition contracts deployed to acquire information system hardware, software, firmware, or services; [*reviewing*] for evidence that the measures identified in SA-12(2).1.1.1 are being applied. |
| **SA-12(2).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with supply chain protection responsibilities or organizational personnel with information system security, acquisition, and contracting responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in SA-12(2).1.1.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-12(3)** | SUPPLY CHAIN PROTECTION |
| **SA-12(3).1**  **SA-12(3).1.1**  **SA-12(3).1.1a**  **SA-12(3).1.1b**  **SA-12(3).1.1c** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization uses trusted shipping and warehousing for:*   * *information systems;* * *information system components; and* * *information technology products.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with supply chain protection responsibilities; organizational personnel with information system security, acquisition, and contracting responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: None  successor controls: SA-4, SA-9, SA-13, SA-14 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-12(3).1.1.1**  **SA-12(3).1.1.1.a**  **SA-12(3).1.1.1.b**  **SA-12(3).1.1.1.c** | **Examine** system and services acquisition policy, procedures addressing supply chain protection, procedures addressing the integration of information security requirements and/or security specifications into the acquisition process, solicitation documentation, acquisition documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the trusted shipping and warehousing services to be used for:   * information systems; * information system components; and * information technology products. |
| **SA-12(3).1.1.2** | **Examine** records of shipping and warehousing services used for information systems; [*reviewing*] for evidence that the trusted shipping and warehousing services identified in SA-12(3).1.1.1.a are being used for information systems. |
| **SA-12(3).1.1.3** | **Examine** records of shipping and warehousing services used for information system components; [*reviewing*] for evidence that the trusted shipping and warehousing services identified in SA-12(1).1.1.1.b are being used for information system components. |
| **SA-12(3).1.1.4** | **Examine** records of shipping and warehousing services used for information technology products; [*reviewing*] for evidence that the trusted shipping and warehousing services identified in SA-12(1).1.1.1.c are being used for information technology products. |
| **SA-12(3).1.1.5** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with supply chain protection responsibilities or organizational personnel with information system security, acquisition, and contracting responsibilities; conducting [*basic*] discussions for further evidence that the trusted shipping and warehousing services identified in SA-12(3).1.1.1.a are being used for information systems. |
| **SA-12(3).1.1.6** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with supply chain protection responsibilities or organizational personnel with information system security, acquisition, and contracting responsibilities; conducting [*basic*] discussions for further evidence that the trusted shipping and warehousing services identified in SA-12(3).1.1.1.b are being used for information system components. |
| **SA-12(3).1.1.7** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with supply chain protection responsibilities or organizational personnel with information system security, acquisition, and contracting responsibilities; conducting [*basic*] discussions for further evidence that the trusted shipping and warehousing services identified in SA-12(3).1.1.1.c are being used for information technology products. |
|  | |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-12(4)** | SUPPLY CHAIN PROTECTION |
| **SA-12(4).1**  **SA-12(4).1.1**  **SA-12(4).1.1a**  **SA-12(4).1.1b**  **SA-12(4).1.1c**  **SA-12(4).1.1d** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs a diverse set of suppliers for:*   * *information systems;* * *information system components;* * *information technology products; and* * *information system services.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: None  successor controls: SA-4, SA-9, SA-13, SA-14 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-12(4).1.1.1**  **SA-12(4).1.1.1.a**  **SA-12(4).1.1.1.b**  **SA-12(4).1.1.1.c**  **SA-12(4).1.1.1.d** | **Examine** system and services acquisition policy, procedures addressing supply chain protection, procedures addressing the integration of information security requirements and/or security specifications into the acquisition process, security plan, or other relevant documents; [*reviewing*] for the diverse set of suppliers to be employed for:   * information systems; * information system components * information technology products; and * information system services. |
| **SA-12(4).1.1.2** | **Examine** the list of suppliers employed for information systems; [*reviewing*] for evidence that the diverse set of suppliers identified in SA-12(4).1.1.1.a is being employed for information systems. |
| **SA-12(4).1.1.3** | **Examine** the list of suppliers employed for information system components; [*reviewing*] for evidence that the diverse set of suppliers identified in SA-12(4).1.1.1.b is being employed for information system components. |
| **SA-12(4).1.1.4** | **Examine** the list of suppliers employed for information technology products; [*reviewing*] for evidence that the diverse set of suppliers identified in SA-12(4).1.1.1.c is being employed for information technology products. |
| **SA-12(4).1.1.5** | **Examine** the list of suppliers employed for information system services; [*reviewing*] for evidence that the diverse set of suppliers identified in SA-12(4).1.1.1.d is being employed for information system services. |
|  | |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-12(5)** | SUPPLY CHAIN PROTECTION |
| **SA-12(5).1**  **SA-12(5).1.1**  **SA-12(5).1.1a**  **SA-12(5).1.1b**  **SA-12(5).1.1c** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs standard configurations for:*   * *information systems;* * *information system components; and* * *information technology products.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; configuration management policy; procedures addressing the baseline configuration of the information system; configuration management plan; information system design documentation; information system architecture and configuration documentation; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9, PM-7, SA-8  concurrent controls: CA-2, CM-2, CM-6, SC-34, SI-3  successor controls: SA-4, SA-9, SA-13, SA-14 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-12(5).1.1.1**  **SA-12(5).1.1.1.a**  **SA-12(5).1.1.1.b**  **SA-12(5).1.1.1.c** | **Examine**  configuration management plan, security plan, information system design documentation, information system architecture and configuration documentation, or other relevant documents; [*reviewing*] for the standard configurations to be employed for:   * information systems; * information system components; and * information technology products. |
| **SA-12(5).1.1.2** | **Examine** documentation describing the current configuration settings identified in SA-12(5).1.1.1.a for an agreed-upon [*basic*] sample of information systems; [*reviewing*] for evidence that these configuration settings are being applied for information systems. |
| **SA-12(5).1.1.3** | **Examine** documentation describing the current configuration settings identified in SA-12(5).1.1.1.b for an agreed-upon [*basic*] sample of information system components; [*reviewing*] for evidence that these configuration settings are being applied for information system components. |
| **SA-12(5).1.1.4** | **Examine** documentation describing the current configuration settings identified in SA-12(5).1.1.1.c for an agreed-upon [*basic*] sample of information technology products; [*reviewing*] for evidence that these configuration settings are being applied for information technology products. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 6** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-12(6)** | SUPPLY CHAIN PROTECTION |
| **SA-12(6).1**  **SA-12(6).1.1**  **SA-12(6).1.1a**  **SA-12(6).1.1b**  **SA-12(6).1.1c** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization minimizes the time between purchase decisions and delivery of:*   * *information systems;* * *information system components; and* * *information technology products.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; shipment records; 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** |
| **SA-12(6).1.1.1**  **SA-12(6).1.1.1.a**  **SA-12(6).1.1.1.b**  **SA-12(6).1.1.1.c** | **Examine** system and services acquisition policy, procedures addressing supply chain protection, procedures addressing the integration of information security requirements and/or security specifications into the acquisition process, solicitation documents, acquisition documentation, acquisition contracts for information systems or services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to minimize the time between purchase decisions and delivery of:   * information systems; * information system components; and * information technology products. |
| **SA-12(6).1.1.2** | **Examine** purchase requisitions, invoices, and corresponding shipping and delivery documentation for an agreed-upon [*basic*] sample of information systems; [*reviewing*] for evidence that the measures identified in SA-12(6).1.1.1.a are being applied to minimize the time between purchase decisions and delivery of information systems. |
| **SA-12(6).1.1.3** | **Examine** purchase requisitions, invoices, and corresponding shipping and delivery documentation for an agreed-upon [*basic*] sample of information system components; [*reviewing*] for evidence that the measures identified in SA-12(6).1.1.1.b are being applied to minimize the time between purchase decisions and delivery of information system components. |
| **SA-12(6).1.1.4** | **Examine** purchase requisitions, invoices, and corresponding shipping and delivery documentation for an agreed-upon [*basic*] sample of information technology products; [*reviewing*] for evidence that the measures identified in SA-12(6).1.1.1.c are being applied to minimize the time between purchase decisions and delivery of information technology products. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 7** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-12(7)** | SUPPLY CHAIN PROTECTION |
| **SA-12(7).1**  **SA-12(7).1.1**  **SA-12(7).1.1a**  **SA-12(7).1.1b**  **SA-12(7).1.1c** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs independent analysis and penetration testing against delivered:*   * *information systems;* * *information system components; and* * *information technology products.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; penetration testing records; security test and evaluation results reports; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CA-2, RA-5  successor controls: CA-7 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-12(7).1.1.1**  **SA-12(7).1.1.1.a**  **SA-12(7).1.1.1.b**  **SA-12(7).1.1.1.c** | **Examine** system and services acquisition policy, procedures addressing supply chain protection, procedures addressing the integration of information security requirements and/or security specifications into the acquisition process, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to conduct independent analysis and penetration testing against delivered:   * information systems; * information system components; and * information technology products. |
| **SA-12(7).1.1.2** | **Examine** penetration testing records and security test and evaluation results for an agreed-upon [*basic*] sample of information systems; [*reviewing*] for evidence that the measures identified in SA-12(7).1.1.1.a are being applied to employ independent analysis and penetration testing against delivered information systems. |
| **SA-12(7).1.1.3** | **Examine** penetration testing records and security test and evaluation results for an agreed-upon [*basic*] sample of information system components; [*reviewing*] for evidence that the measures identified in SA-12(7).1.1.1.b are being applied to employ independent analysis and penetration testing against delivered information system components. |
| **SA-12(7).1.1.4** | **Examine** penetration testing records and security test and evaluation results for an agreed-upon [*basic*] sample of information technology products; [*reviewing*] for evidence that the measures identified in SA-12(7).1.1.1.c are being applied to employ independent analysis and penetration testing against delivered information technology products. |