| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SA-4** | ACQUISITIONS | |
| **SA-4.1**  **SA-4.1.1**  **SA-4.1.1a**  **SA-4.1.1b**  **SA-4.1.1c** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:*   * *security functional requirements/specifications;* * *security-related documentation requirements; and* * *developmental and evaluation-related assurance requirements.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; acquisition contracts for information systems or services; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system security, acquisition, and contracting responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9, PM-3, PM-7, PM-11, SA-2, SA-3, SA-8, SA-12, SA-13, SC-3  concurrent controls: CA-2, CM-2, CM-6, CM-8, RA-3, SI-2, SI-3, SI-6, SI-7  successor controls: CA-6, SA-5, SA-6, SA-7, SA-9, SA-10, SA-11, SI-6 |
| **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-4.1.1.1**  **SA-4.1.1.1.a**  **SA-4.1.1.1.b**  **SA-4.1.1.1.c** | | **Examine** system and services acquisition policy, risk assessment policy, 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 risk assessment measures, applicable federal laws, Executive Orders, directives, policies, regulations, and standards to be employed to include the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts:   * security functional requirements/specifications; * security-related documentation requirements; and * developmental and evaluation-related assurance requirements. |
| **SA-4.1.1.2** | | **Examine** an agreed-upon [*basic*] sample of acquisition contracts and associated risk assessments for information system services; [*reviewing*] for evidence that the measures identified in SA-4.1.1.1.a are being applied to include security functional requirements/specifications, explicitly or by reference, in information system acquisition contracts. |
| **SA-4.1.1.3** | | **Examine** an agreed-upon [*basic*] sample of acquisition contracts and associated risk assessments for information system services; [*reviewing*] for evidence that the measures identified in SA-4.1.1.1.b are being applied to include security-related documentation requirements, explicitly or by reference, in information system acquisition contracts. |
| **SA-4.1.1.4** | | **Examine** an agreed-upon [*basic*] sample of acquisition contracts and associated risk assessments for information system services; [*reviewing*] for evidence that the measures identified in SA-4.1.1.1.c are being applied to include developmental and evaluation-related assurance requirements, explicitly or by reference, in information system acquisition contracts. |
| **SA-4.1.1.5** | | **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-4.1.1.1.a are being applied to include security functional requirements/specifications, explicitly or by reference, in information system acquisition contracts. |
| **SA-4.1.1.6** | | **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-4.1.1.1.b are being applied to include security-related documentation requirements, explicitly or by reference, in information system acquisition contracts. |
| **SA-4.1.1.7** | | **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-4.1.1.1.c are being applied to include developmental and evaluation-related assurance requirements, explicitly or by reference, in information system acquisition contracts. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-4(1)** | ACQUISITIONS |
| **SA-4(1).1**  **SA-4(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; 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: PM-3, PM-7, PM-11, SA-2, SA-3, SA-8, SA-12, SA-13, SC-2, SC-3  concurrent controls: CA-2, CM-2, CM-6, CM-8, SI-2, SI-3, SI-6, SI-7  successor controls: CA-6, SA-5, SA-6, SA-7, SA-9, SA-10, SA-11 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-4(1).1.1.1** | **Examine** system and services acquisition policy, 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 requirement that vendors/contractors provide information in acquisition documents that describes the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-4(2)** | ACQUISITIONS |
| **SA-4(2).1**  **SA-4(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; 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: PM-3, PM-7, PM-11, SA-2, SA-3, SA-8, SA-12, SA-13, SC-2, SC-3  concurrent controls: CA-2, CM-2, CM-6, CM-8, SI-2, SI-3, SI-6, SI-7  successor controls: CA-6, SA-5, SA-6, SA-7, SA-9, SA-10, SA-11 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-4(2).1.1.1** | **Examine** system and services acquisition policy, 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 requirement that vendors/contractors provide information in acquisition documents that describes the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-4(3)** | ACQUISITIONS |
| **SA-4(3).1**  **SA-4(3).1.1**  **SA-4(3).1.1a**  **SA-4(3).1.1b**  **SA-4(3).1.1c** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization requires software vendors/manufacturers to minimize flawed or malformed software by demonstrating that their software development processes employ:*   * *state-of-the-practice software and security engineering methods;* * *quality control processes; and* * *validation techniques.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; 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: PM-7, SA-2, SA-3, SA-8, SA-12, SA-13  concurrent controls: CA-2, RA-5,SI-2, SI-6, SI-7  successor controls: CA-6, SA-5, SA-6, SA-7, SA-9, SA-10, SA-11, |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-4(3).1.1.1**  **SA-4(3).1.1.1.a**  **SA-4(3).1.1.1.b**  **SA-4(3).1.1.1.c** | **Examine** system and services acquisition policy, 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 requirement of software vendors/manufacturers to minimize flawed or malformed software by demonstrating that their software development processes employ:   * state-of-the-practice software and security engineering methods; * quality control processes; and * validation techniques. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-4(4)** | ACQUISITIONS |
| **SA-4(4).1**  **SA-4(4).1.1**  **SA-4(4).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization explicitly assigns each acquired information system component to an information system; and* 2. *the owner of the system acknowledges each assignment of information system components to the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; 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 information system security, acquisition, and contracting responsibilities; information system owner]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PM-7, CM-9  concurrent controls: CM-2, CM-8, PL-2  successor controls: CA-6, PE-18 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-4(4).1.1.1** | **Examine** system and services acquisition policy, procedures addressing the assignment of information system components to an information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to assign each acquired information system component to the information system. |
| **SA-4(4).1.1.2** | **Examine** acquisition contracts or other relevant acquisition documentation, and inventory records associated with an agreed-upon [*basic*] sample of information system components acquired for the information system; [*reviewing*] for evidence that the measures identified in SA-4(4).1.1.1 are being applied. |
| **SA-4(4).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with inventory control responsibilities for assigning acquired information system components to the information system; [*reviewing*] for further evidence that the measures identified in SA-4(4).1.1.1 are being applied. |
|  |  |
| **SA-4(4).1.2.1** | **Examine** system and services acquisition policy, procedures addressing system owner acknowledgement of system component assignments to the information system, security plan, or other relevant documents; [*reviewing*] for the measures to be employed by the information system owner to acknowledge each assignment of information system components to the information system. |
| **SA-4(4).1.2.2** | **Examine** signed acknowledgement forms and inventory records associated with an agreed-upon [*basic*] sample of system component assignments to the information system; [*reviewing*] for evidence that the measures identified in SA-4(4).1.2.1 are being applied. |
| **SA-4(4).1.2.3** | **Interview** information system owner; [*reviewing*] for further evidence that the measures identified in SA-4(4)1.2.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-4(5)** | ACQUISITIONS |
| **SA-4(5).1**  **SA-4(5).1.1**  **SA-4(5).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization requires in acquisition documents that information system components are delivered in a secure, documented configuration; and* 2. *the organization requires in acquisition documents that the secure configuration is the default configuration for any software reinstalls or upgrades.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; 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: CM-9, PM-7, SA-3, SA-8  concurrent controls: CM-2, CM-6, CM-8  successor controls: SA-5, SA-6, SA-7, SA-10, SA-11 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-4(5).1.1.1** | **Examine** system and services acquisition policy, 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 requirement in acquisition documents that information system components be delivered in a secure, documented configuration. |
|  |  |
| **SA-4(5).1.2.1** | **Examine** system and services acquisition policy, 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 requirement in acquisition documents that the secure configuration delivered for information system components be the default configuration for any software reinstalls or upgrades. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 6** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-4(6)** | ACQUISITIONS |
| **SA-4(6).1**  **SA-4(6).1.1**  **SA-4(6).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization employs only government off-the-shelf (GOTS) or commercial off-the-shelf (COTS) information assurance (IA) and IA-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and* 2. *the organization ensures that these products have been evaluated and/or validated by the NSA or in accordance with NSA-approved procedures.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; 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 information system security, acquisition, and contracting responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PM-7, SA-8, SA-13  concurrent controls: CM-2, CM-6  successor controls: SA-5, SA-6, SA-7 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-4(6).1.1.1** | **Examine** information system documentation; [*reviewing*] for the networks used to transmit classified information. |
| **SA-4(6).1.1.2** | **Examine** security categorization documentation or other relevant documents for the networks identified in SA-4(6).1.1.1 and for the classified information transmitted using these networks; [*reviewing*] for those networks with a lower classification level than the classification level of the information being transmitted. |
| **SA-4(6).1.1.3** | **Examine** system and services acquisition policy, 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 GOTS or COTS IA and IA-enabled information technology products to be employed that compose an NSA-approved solution to protect classified information transmitted using the networks identified in SA-4(6).1.1.2 that are at a lower classification level than the information being transmitted. |
| **SA-4(6).1.1.4** | **Examine** an agreed-upon [*basic*] sample of the information technology products employed to protect classified information when the networks identified in SA-4(6).1.1.2 are used to transmit this information; [*reviewing*] for evidence that only the GOTS or COTS IA and IA-enabled information technology products identified in SA-4(6).1.1.3 are being applied. |
|  |  |
| **SA-4(6).1.2.1** | **Examine** system and services acquisition policy, 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 ensure that GOTS or COTS IA and IA-enabled technology products are evaluated and/or validated by NSA or in accordance with NSA-approved procedures. |
| **SA-4(6).1.2.2** | **Examine** the measures employed to ensure GOTS or COTS IA and IA-enabled technology products are evaluated and/or validated by NSA or in accordance with NSA-approved procedures; [*reviewing*] for evidence that the measures identified in SA-4(6).1.2.1 are being applied. |
| **SA-4(6).1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system security, acquisition, and contracting responsibilities; [*reviewing*] for further evidence that the measures identified in SA-4(6).1.2.1 are being applied. |
|  | |
| **ASSESSMENT – Control Enhancement 7** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-4(7)** | ACQUISITIONS |
| **SA-4(7).1**  **SA-4(7).1.1**  **SA-4(7).1.2**  **SA-4(7).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization limits the use of commercially-provided information technology products to those products that have been successfully evaluated against a validated U.S. Government Protection Profile for a specific technology type, if such a profile exists;* 2. *the organization requires a commercially-provided information technology product to rely on cryptographic functionality to enforce its security policy when no U.S. Government Protection Profile exists for such a specific technology type; and* 3. *the organization requires the use of a FIPS-validated, cryptographic module for a technology product that relies on cryptographic functionality to enforce its security policy when no U.S. Government Protection Profile exists for such a specific technology type.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; 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 information system security, acquisition, and contracting responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PM-7, SA-8, SA-13  concurrent controls: CM-2, CM-6, SC-13  successor controls: SA-5, SA-6, SA-7 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-4(7).1.1.1** | **Examine** the list of validated U.S. Government Protection Profiles; [*reviewing*] for the technology types associated with each profile. |
| **SA-4(7).1.1.2** | **Examine** system and services acquisition policy, 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 limit the use of commercially-provided information technology products to those products that have been successfully evaluated against a validated U.S. Government Protection Profile identified in SA-4(7).1.1.1. |
| **SA-4(7).1.1.3** | **Examine** vendor/manufacturer product evaluation documentation, vendor/manufacturer product validation documentation, or other relevant product documentation for an agreed-upon [*basic*] sample of commercially-provided information technology products acquired for information system services; [*reviewing*] for evidence that the measures identified in SA-4(7).1.1.2 are being applied. |
|  |  |
| **SA-4(7).1.2.1** | **Examine** system and services acquisition policy, 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 requirement that commercially-provided information technology products rely on cryptographic functionality to enforce its security policy when no U.S. Government Protection Profile exists for that technology type. |
|  |  |
| **SA-4(7).1.3.1** | **Examine** system and services acquisition policy, 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 requirement that a FIPS-validated cryptographic module be used for a technology product that relies on cryptographic functionality to enforce its security policy when no U.S. Government Protection Profile exists for that technology type. |