| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SA-11** | DEVELOPER SECURITY TESTING | |
| **SA-11.1**  **SA-11.1.1**  **SA-11.1.1a**  **SA-11.1.1b**  **SA-11.1.1c** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):*   * *create and implement a security test and evaluation plan;* * *implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and* * *document the results of the security testing/evaluation and flaw remediation processes.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with developer security testing responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: SA-4, SA-5, SA-8  concurrent controls: CA-2, CM-4, SA-3, SA-10, SI-2  successor controls: CA-5, CA-6, CA-7 |
| **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-11.1.1.1**  **SA-11.1.1.1.a**  **SA-11.1.1.1.b**  **SA-11.1.1.1.c** | | **Examine** system and services acquisition policy, procedures addressing information system developer/integrator security testing, solicitation documentation, acquisition contracts, service level agreements, security plan, or other relevant documents; [*reviewing*] for the requirement that information system developers/integrators, in consultation with associated security personnel (including security engineers):   * create and implement a security test and evaluation plan; * implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and * document the results of the security testing/evaluation and flaw remediation processes. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **SA-11(1)** | | DEVELOPER SECURITY TESTING |
| **SA-11(1).1**  **SA-11(1).1.1**  **SA-11(1).1.2** | | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization requires that information system developers/integrators employ code analysis tools to examine software for common flaws; and* 2. *the organization requires that information system developers/integrators document the results of the analysis.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with developer security testing responsibilities]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: SA-4, SA-5, SA-8  concurrent controls: CA-2, CM-4, SA-3, SA-10, SI-2  successor controls: CA-5, CA-6, CA-7 |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **SA-11(1).1.1.1** | | **Examine** system and services acquisition policy, procedures addressing information system developer/integrator security testing, solicitation documentation, acquisition contracts, service level agreements, security plan, or other relevant documents; [*reviewing*] for the requirement that information system developers/integrators employ code analysis tools to examine software for common flaws. |
|  | |  |
| **SA-11(1).1.2.1** | | **Examine** system and services acquisition policy, procedures addressing information system developer/integrator security testing, solicitation documentation, acquisition contracts, service level agreements, security plan, or other relevant documents; [*reviewing*] for the requirement that information system developers/integrators document the results from the code analysis tools employed to examine software for common flaws. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-11(2)** | DEVELOPER SECURITY TESTING |
| **SA-11(2).1**  **SA-11(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization requires that information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; vulnerability scanning results; information system risk assessment report; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with developer security testing responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: SA-4, SA-5, SA-8  concurrent controls: CA-2, CM-4, SA-3, SA-10, SI-2  successor controls: CA-5, CA-6, CA-7 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-11(2).1.1.1** | **Examine** system and services acquisition policy, procedures addressing information system developer/integrator security testing, solicitation documentation, acquisition contracts, service level agreements, security plan, or other relevant documents; [*reviewing*] for the requirement that information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-11(3)** | DEVELOPER SECURITY TESTING |
| **SA-11(3).1**  **SA-11(3).1.1**  **SA-11(3).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization requires that information system developers/integrators create a security test and evaluation plan; and* 2. *the organization requires that information system developers/integrators implement the plan under the witness of an independent verification and validation agent.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing information system developer/integrator security testing; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; security test and evaluation plan; security test and evaluation results report; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel with developer security testing responsibilities; independent verification and validation agent]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: SA-4, SA-5, SA-8  concurrent controls: CA-2, CM-4, SA-3, SA-10, SI-2  successor controls: CA-5, CA-6, CA-7 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-11(3).1.1.1** | **Examine** system and services acquisition policy, procedures addressing information system developer/integrator security testing, solicitation documentation, acquisition contracts, service level agreements, security plan, or other relevant documents; [*reviewing*] for the requirement that information system developers/integrators create a security test and evaluation plan. |
|  |  |
| **SA-11(3).1.2.1** | **Examine** system and services acquisition policy, procedures addressing information system developer/integrator security testing, solicitation documentation, acquisition contracts, service level agreements, security plan, or other relevant documents; [*reviewing*] for the requirement that information system developers/integrators implement the plan under the witness of an independent verification and validation agent. |