| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SA-10** | DEVELOPER CONFIGURATION MANAGEMENT | |
| **SA-10.1**  **SA-10.1.1**  **SA-10.1.1a**  **SA-10.1.1b**  **SA-10.1.1c**  **SA-10.1.1d**  **SA-10.1.2**  **SA-10.1.2a**  **SA-10.1.2b**  **SA-10.1.2c**  **SA-10.1.2d**  **SA-10.1.3**  **SA-10.1.4**  **SA-10.1.5** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization requires that information system developers/integrators:*   1. *perform configuration management during information system:*    * *design;*    * *development;*    * *implementation; and*    * *operation;* 2. *manage and control changes to the information system during:*    * *design;*    * *development;*    * *implementation; and*    * *modification;* 3. *implement only organization-approved changes;* 4. *document approved changes to the information system; and* 5. *track security flaws and flaw resolution.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system developer/integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records].  **Interview**: [*select from:* Organization personnel with information system security, acquisition, and contracting responsibilities; organization personnel with configuration management responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9, SA-4, SA-5, SA-8  concurrent controls: CM-2, CM-3, CM-4, SA-3, SI-2  successor controls: SA-11 |

|  |  |
| --- | --- |
| **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-10.1.1.1**  **SA-10.1.1.1.a**  **SA-10.1.1.1.b**  **SA-10.1.1.1.c**  **SA-10.1.1.1.d** | **Examine** system and services acquisition policy, procedures addressing information system developer/integrator configuration management, acquisition contracts, service level agreements, configuration management plan, security plan, or other relevant documents; [*reviewing*] for the requirement that information system developers/integrators perform configuration management during information system:   * + design;   + development;   + implementation; and   + operation. |
|  |  |
| **SA-10.1.2.1**  **SA-10.1.2.1.a**  **SA-10.1.2.1.b**  **SA-10.1.2.1.c**  **SA-10.1.2.1.d** | **Examine** system and services acquisition policy, procedures addressing information system developer/integrator configuration management, acquisition contracts, service level agreements, configuration management plan, security plan, or other relevant documents; [*reviewing*] for the requirement that information system developers/integrators manage and control changes to the information system during:   * + design;   + development;   + implementation; and   + modification. |
|  |  |
| **SA-10.1.3.1** | **Examine** system and services acquisition policy, procedures addressing information system developer/integrator configuration management, acquisition contracts, service level agreements, configuration management plan, security plan, or other relevant documents; [*reviewing*] for the requirement that information system developers/integrators implement only organization-approved changes. |
|  |  |
| **SA-10.1.4.1** | **Examine** system and services acquisition policy, procedures addressing information system developer/integrator configuration management, acquisition contracts, service level agreements, configuration management plan, security plan, or other relevant documents; [*reviewing*] for the requirement that information system developers/integrators document approved changes to the information system. |
|  |  |
| **SA-10.1.5.1** | **Examine** system and services acquisition policy, procedures addressing information system developer/integrator configuration management, acquisition contracts, service level agreements, configuration management plan, security plan, or other relevant documents; [*reviewing*] for the requirement that information system developers/integrators track security flaws and flaw resolution. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-10(1)** | DEVELOPER CONFIGURATION MANAGEMENT |
| **SA-10(1).1**  **SA-10(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization requires that information system developers/integrators provide an integrity check of software to facilitate organizational verification of software integrity after delivery.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system developer/integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9, SA-4, SA-5, SA-8  concurrent controls: CM-2, CM-3, SI-7  successor controls: SA-11 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-10(1).1.1.1** | **Examine** system and services acquisition policy, procedures addressing information system developer/integrator configuration management, acquisition contracts, service level agreements, configuration management plan, security plan, or other relevant documents; [*reviewing*] for the requirement that information system developers/integrators provide an integrity check of software to facilitate organizational verification of software integrity after delivery. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-10(2)** | DEVELOPER CONFIGURATION MANAGEMENT |
| **SA-10(2).1**  **SA-10(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization provides an alternative configuration management process with organizational personnel in the absence of a dedicated developer/integrator configuration management team.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-2, CM-3, CM-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-10(2).1.1.1** | **Examine** system and services acquisition policy, procedures addressing information system developer/integrator configuration management, configuration management plan, security plan, or other relevant documents; [*reviewing*] for an alternative configuration management process that provides organizational personnel in the absence of a dedicated developer/integrator configuration management team. |