| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **PL-2** | **SYSTEM SECURITY PLAN** | |
| **PL-2.1**  **PL-2.1.1**  **PL-2.1.1a**  **PL-2.1.1b**  **PL-2.1.1c**  **PL-2.1.1d**  **PL-2.1.1e**  **PL-2.1.1f**  **PL-2.1.1g**  **PL-2.1.1h**  **PL-2.1.1i**  **PL-2.1.2**  **PL-2.1.3**  **PL-2.1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization develops a security plan for the information system that:*    * *is consistent with the organization’s enterprise architecture;*    * *explicitly defines the authorization boundary for the system;*    * *describes the operational context of the information system in terms of mission and business processes;*    * *provides the security categorization of the information system including supporting rationale;*    * *describes the operational environment for the information system;*    * *describes relationships with or connections to other information systems;*    * *provides an overview of the security requirements for the system;*    * *describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplemental decisions; and*    * *is reviewed and approved by the authorizing official or designated representative prior to plan implementation;* 2. *the organization defines the frequency of security plan reviews;* 3. *the organization reviews the security plan in accordance with the organization-defined frequency; and* 4. *the organization updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security planning policy; procedures addressing security plan development and implementation; procedures addressing security plan reviews and updates; enterprise architecture documentation; security plan for the information system; records of security plan reviews and updates; other relevant documents or records].  **Interview**: [*select from:* Organization personnel with security planning and plan implementation responsibilities for the information system]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PM-1, PM-7, PM-9, PM-11  concurrent controls: CA-2, CA-3, CA-6, CA-7, CM-4, PL-4, PL-5, PL-6, PM-10, RA-2, RA-3  successor controls: CA-5, PM-4 |

|  |  |
| --- | --- |
| **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. |
| **PL-2.1.1.1** | **Examine** information system documentation; [*reviewing*] for a security plan for the information system. |
| **PL-2.1.1.2**  **PL-2.1.1.2.a**  **PL-2.1.1.2.b**  **PL-2.1.1.2.c**  **PL-2.1.1.2.d**  **PL-2.1.1.2.e**  **PL-2.1.1.2.f**  **PL-2.1.1.2.g**  **PL-2.1.1.2.h**  **PL-2.1.1.2.i** | **Examine** security plan; [*reviewing*] for evidence that the plan:   * + is consistent with the organization’s enterprise architecture;   + explicitly defines the authorization boundary for the system;   + describes the operational context of the information system in terms of mission and business processes;   + provides the security categorization of the information system including supporting rationale;   + describes the operational environment for the information system;   + describes relationships with or connections to other information systems;   + provides an overview of the security requirements for the system;   + describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplemental decisions; and   + is reviewed and approved by the authorizing official or designated representative prior to plan implementation. |
|  |  |
| **PL-2.1.2.1** | **Examine** security planning policy, procedures addressing security plan reviews and updates, security plan, or other relevant documents; [*reviewing*] for the frequency of security plan reviews. |
|  |  |
| **PL-2.1.3.1** | **Examine** security plan; [*reviewing*] for evidence that the plan is reviewed in accordance with the frequency identified in PL-2.1.2.1. |
|  |  |
| **PL-2.1.4.1** | **Examine** security planning policy, procedures addressing security plan reviews and updates, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to update the security plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments. |
| **PL-2.1.4.2** | **Examine** security plan and an agreed-upon [*basic*] sample of change control records addressing security plan revisions from changes to the information system/environment; [*reviewing*] for evidence that the measures identified in PL-2.1.4.1 are being applied.  Note to assessor: Change control records addressing security plan revisions may be maintained in the security plan, or maintained in change management software or document management software used by the organization. |
| **PL-2.1.4.3** | **Examine** security plan and an agreed-upon [*basic*] sample of change control records addressing security plan revisions from problems identified during plan implementation or security control assessments; [*reviewing*] for evidence that the measures identified in PL-2.1.4.1 are being applied. |
|  | |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **PL-2(1)** | SYSTEM SECURITY PLAN |
| **PL-2(1).1**  **PL-2(1).1.1**  **PL-2(1).1.1a**  **PL-2(1).1.1b**  **PL-2(1).1.1c**  **PL-2(1).1.1d**  **PL-2(1).1.2**  **PL-2(1).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization develops a security Concept of Operations (CONOPS) for the information system containing, at a minimum:*    * *the purpose of the system;*    * *a description of the system architecture;*    * *the security authorization schedule; and*    * *the security categorization and associated factors considered in determining the categorization;* 2. *the organization defines the frequency of reviews and updates to the CONOPS; and* 3. *the organization reviews and updates the CONOPS in accordance with the organization-defined frequency.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security planning policy; procedures addressing security CONOPS development; procedures addressing security CONOPS reviews and updates; security CONOPS for the information system; security plan for the information system; records of security CONOPS reviews and updates; other relevant documents or records].  **Interview**: [*select from:* Organization personnel with security planning and plan implementation responsibilities for the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PM-1, PM-7, PM-9  concurrent controls: CA-2, CA-3, CA-6, CA-7, CM-4, PL-4, PL-5, PL-6, RA-2, RA-3, PM-10  successor controls: CA-5, PM-4 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **PL-2(1).1.1.1** | **Examine** information system documentation; [*reviewing*] for a security Concept of Operations (CONOPS) for the information system. |
| **PL-2(1).1.1.2**  **PL-2(1).1.1.2.a**  **PL-2(1).1.1.2.b**  **PL-2(1).1.1.2.c**  **PL-2(1).1.1.2.d** | **Examine** security CONOPS; [*reviewing*] for evidence that the plan contains, at a minimum:   * + the purpose of the system;   + a description of the system architecture;   + the security authorization schedule; and   + the security categorization and associated factors considered in determining the categorization. |
|  |  |
| **PL-2(1).1.2.1** | **Examine** security planning policy, procedures addressing security CONOPS reviews and updates, security CONOPS, or security plan; [*reviewing*] for the frequency of reviews and updates to the CONOPS. |
|  |  |
| **PL-2(1).1.3.1** | **Examine** security CONOPS and other relevant documents resulting from CONOPS reviews and updates; [*reviewing*] for evidence that the plan is reviewed and updated in accordance with the frequency identified in PL-2(1).1.2.1. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **PL-2(2)** | SYSTEM SECURITY PLAN |
| **PL-2(2).1**  **PL-2(2).1.1**  **PL-2(2).1.1a**  **PL-2(2).1.1b**  **PL-2(2).1.1c**  **PL-2(2).1.1d**  **PL-2(2).1.1e** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization develops a functional architecture for the information system that identifies and maintains:*   * *external interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface;* * *user roles and the access privileges assigned to each role;* * *unique security requirements;* * *types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; and* * *restoration priority of information or information system services.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security planning policy; access control policy; contingency planning policy; security plan for the information system; contingency plan for the information system; information system design documentation; other relevant documents or records].  **Interview**: [*select from:* Organization personnel with security planning and plan implementation responsibilities for the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PM-1, PM-7, PM-9  concurrent controls: AC-2, AC-20, CA-3, PE-2, PL-4, PL-5, PL-6, RA-2, RA-3, CP-2, CP-10  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **PL-2(2).1.1.1** | **Examine** information system documentation; [*reviewing*] for a functional architecture for the information system. |
| **PL-2(2).1.1.2  PL-2(2).1.1.2.a**  **PL-2(2).1.1.2.b**  **PL-2(2).1.1.2.c**  **PL-2(2).1.1.2.d**  **PL-2(2).1.1.2.e** | **Examine** functional architecture; [*reviewing*] for evidence that the architecture identifies and maintains:   * external interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface; * user roles and the access privileges assigned to each role; * unique security requirements; * types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; and * restoration priority of information or information system services. |