| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **PM-1** | INFORMATION SECURITY PROGRAM PLAN | |
| **PM-1.1**  **PM-1.1.1**  **PM-1.1.1a**  **PM-1.1.1b**  **PM-1.1.1c**  **PM-1.1.1d**  **PM-1.1.1e**  **PM-1.1.2**  **PM-1.1.3**  **PM-1.1.4**  **PM-1.1.5** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization develops an information security program plan for the organization that:*    * *provides an overview of the requirements for the security program;*    * *provides a description of the security program management controls and common controls in place or planned for meeting security program requirements;*    * *provides sufficient information about the program management controls and common controls (including specification of parameters for any* assignment *and* selection *operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;*    * *includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance;*    * *is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations and the Nation;* 2. *the organization defines the frequency of information security program plan reviews;* 3. *the organization reviews the organization-wide information security program plan in accordance with the organization-defined frequency;* 4. *the organization revises the plan to address organizational changes and problems identified during plan implementation or security control assessments; and* 5. *the organization disseminates the most recent information security program plan to appropriate entities in the organization.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information security program policy; procedures addressing information security program plan development and implementation; procedures addressing information security program plan reviews and updates; information security program plan; program management controls documentation; common controls documentation; records of information security program plan reviews and updates; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with security planning and plan implementation responsibilities for the information security program]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PM-9,  concurrent controls: PM-7, PM-11  successor controls: PL-2, PM-2, PM-3, PM-4, PM-5, PM-6, PM-8, PM-10 |

|  |  |
| --- | --- |
| **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. |
| **PM-1.1.1.1** | **Examine** information security program documentation; [*reviewing*] for an information security program plan for the organization. |
| **PM-1.1.1.2**  **PM-1.1.1.2.a**  **PM-1.1.1.2.b**  **PM-1.1.1.2.c**  **PM-1.1.1.2.d**  **PM-1.1.1.2.e** | **Examine** information security program plan; [*reviewing*] for evidence that the plan:   * + provides an overview of the requirements for the security program;   + provides a description of the security program management controls and common controls in place or planned for meeting security program requirements;   + provides sufficient information about the program management controls and common controls (including specification of parameters for any *assignment* and *selection* operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;   + includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and   + is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations and the Nation. |
|  |  |
| **PM-1.1.2.1** | **Examine** information security program policy, procedures addressing information security program plan reviews and updates, information security program plan, or other relevant documents; [*reviewing*] for the frequency of information security program plan reviews. |
|  |  |
| **PM-1.1.3.1** | **Examine** information security program plan; [*reviewing*] for evidence that the plan is reviewed in accordance with the frequency identified in PM-1.1.2.1. |
|  |  |
| **PM-1.1.4.1** | **Examine** information security program policy, procedures addressing information security program plan reviews and updates, information security program plan, or other relevant documents; [*reviewing*] for the measures to be employed to update the information security program plan to address organizational changes and problems identified during plan implementation or security control assessments. |
| **PM-1.1.4.2** | **Examine** information security program plan and an agreed-upon [*basic*] sample of change control records addressing information security program plan revisions resulting from organizational changes; [*reviewing*] for evidence that the measures identified in PM-1.1.4.1 are being applied.  Note to assessor: Change control records addressing information security program plan revisions may be maintained in the information security program plan, or maintained in change management software or document management software used by the organization. |
| **PM-1.1.4.3** | **Examine** information security program plan and an agreed-upon [*basic*] sample of change control records addressing information security program plan revisions resulting from problems identified during plan implementation or security control assessments; [*reviewing*] for evidence that the measures identified in PM-1.1.4.1 are being applied. |
|  |  |
| **PM-1.1.5.1** | **Examine** information security program policy, procedures addressing information security program plan development, distribution and implementation, information security program plan, or other relevant documents; [*reviewing*] for the entities in the organization designated to receive the information security program plan. |
| **PM-1.1.5.2** | **Interview** an agreed-upon [*basic*] sample of organizational personnel designated within the entities identified in PM-1.1.5.1 to receive the information security program plan; conducting [*basic*] discussions for evidence that these individuals received the most recent information security program plan. |
|  | |