| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **PM-3** | INFORMATION SECURITY RESOURCES | |
| **PM-3.1**  **PM-3.1.1**  **PM-3.1.2**  **PM-3.1.3**  **PM-3.1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization includes in its capital planning and investment requests the resources needed to implement the information security program;* 2. *the organization documents all exceptions to the requirement that all capital planning and investment requests include the resources needed to implement the information security program;* 3. *the organization employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and* 4. *the organization makes the required information security resources available for expenditure as planned.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information security program policy; capital planning and investment policy; procedures addressing management and oversight for information security-related aspects of the capital planning and investment control process; capital planning and investment documentation; documentation of exceptions supporting capital planning and investment requests; business cases; Exhibit 300; Exhibit 53; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel managing and overseeing the information security-related aspects of the capital planning and investment control process]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PM-1, PM-9  concurrent controls: PM-4  successor controls: SA-2, SA-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. |
| **PM-3.1.1.1** | | **Examine** information security program policy, capital planning and investment control policy, system and services acquisition policy, procedures addressing management and oversight of information security aspects of the capital planning and investment control process, procedures addressing allocation of resources to information security program requirements, information security program plan, or other relevant documents; [*reviewing*] for the measures to be employed to include in capital planning and investment requests the resources needed to implement the information security program. |
| **PM-3.1.1.2** | | **Examine** organizational capital programming and budget documentation supporting capital planning and investment requests; [*reviewing*] for evidence that the measures identified in PM-3.1.1.1 are being applied to include in capital planning and investment requests the resources needed to implement the information security program. |
|  | |  |
| **PM-3.1.2.1** | | **Examine** information security program policy, capital planning and investment control policy, system and services acquisition policy, procedures addressing management and oversight of information security aspects of the capital planning and investment control process, procedures addressing allocation of resources to information security program requirements, information security program plan, or other relevant documents; [*reviewing*] for the measures to be employed to document all exceptions to the requirement that all capital planning and investment requests include the resources needed to implement the information security program. |
| **PM-3.1.2.2** | | **Examine** (if applicable) documentation of exceptions supporting capital planning and investment requests; [*reviewing*] for evidence that the measures identified in PM-3.1.2.1 are being applied to document all exceptions to the requirement that all capital planning and investment requests include the resources needed to implement the information security program.  Note to assessor: Execution of this assessor action may depend on the organization’s verbal confirmation regarding the existence or non-existence of such exceptions. |
|  | |  |
| **PM-3.1.3.1** | | **Examine** the organizational capital programming and budget documentation identified in PM-3.1.1.2; [*reviewing*] for evidence that a business case/Exhibit 300/Exhibit 53 is employed to record the resources required to implement the information security program. |
|  | |  |
| **PM-3.1.4.1** | | **Examine** information security program policy, capital planning and investment control policy, system and services acquisition policy, procedures addressing management and oversight of information security aspects of the capital planning and investment control process, procedures addressing allocation of resources to information security program requirements, information security program plan, or other relevant documents; [*reviewing*] for measures to be employed to make the required information security resources available for expenditure as planned. |
| **PM-3.1.4.2** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with management and oversight responsibilities for the information security aspects of the capital planning and investment control process; conducting [*basic*] discussions for evidence that the measures identified in PM-3.1.4.1 are being applied to make the required information security resources available for expenditure as planned. |
|  | | |