| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **PM-10** | SECURITY AUTHORIZATION PROCESS | |
| **PM-10.1**  **PM-10.1.1**  **PM-10.1.2**  **PM-10.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes;* 2. *the organization designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and* 3. *the organization fully integrates the security authorization processes into an organization-wide risk management program.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information security program policy; security assessment and authorization policy; risk management policy; procedures addressing security authorization processes; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with security authorization responsibilities for information systems; organizational personnel with risk management responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CA-5, PM-4, PM-9  concurrent controls: CA-2, CA-6, CA-7, CM-4, PL-2, PL-6  successor controls: None |
| **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-10.1.1.1** | | **Examine** information security program policy, security assessment and authorization policy, risk management policy, procedures addressing security authorization processes, information security program plan, or other relevant documents; [*reviewing*] for the security authorization processes to be employed to manage (i.e., document, track, and report) the security state of organizational information systems. |
| **PM-10.1.1.2** | | **Examine** security authorization packages for an agreed-upon [*basic*] sample of organizational information systems; [*reviewing*] for evidence that the measures identified in PM-10.1.1.1 are being applied.  Note to assessor: Security authorization packages should include (for example) the security plan, security assessment report, plan of action and milestones, and authorization statement. |
|  | |  |
| **PM-10.1.2.1** | | **Examine** information security program policy, security assessment and authorization policy, risk management policy, procedures addressing security authorization processes, information security program plan, or other relevant documents; [*reviewing*] for the specific roles and responsibilities within the organizational risk management process. |
| **PM-10.1.2.2** | | **Examine** information security program policy, security assessment and authorization policy, risk management policy, procedures addressing security authorization processes, information security program plan, or other relevant documents; [*reviewing*] for the organizational personnel designated to fulfill the roles and responsibilities identified in PM-10.1.2.1. |
| **PM-10.1.2.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel identified in PM-10.1.2.2; conducting [*basic*] discussions for evidence that these individuals fulfill the respective roles and responsibilities identified in PM-10.1.2.1. |
|  | |  |
| **PM-10.1.3.1** | | **Examine** risk management program documentation; [*reviewing*] for evidence that the security authorization processes identified in PM-10.1.1.1 are fully integrated into the organization-wide risk management program. |
|  | | |