| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **PM-4** | PLAN OF ACTION AND MILESTONES PROCESS | |
| **PM-4.1**  **PM-4.1.1**  **PM-4.1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization implements a process to maintain plans of action and milestones for the security program and the associated organizational information systems; and* 2. *the organization implements a process to document the remedial information security actions that mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information security program policy; plan of action and milestones policy; procedures addressing plan of action and milestones process; plan of action and milestones for the security program; plan of action and milestones for organizational information systems; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with plan of action and milestones development and implementation responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CA-2, CA-7, CM-4, PL-2, PL-6, PM-1, PM-9, RA-5  concurrent controls: PM-3, CA-5  successor controls: CA-6, 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-4.1.1.1** | | **Examine** information security program policy, plan of action and milestones policy, procedures addressing plan of action and milestones process, information security program plan, or other relevant documents; [*reviewing*] for the process to be employed to maintain plans of action and milestones for the security program and associated organizational information systems. |
| **PM-4.1.1.2** | | **Examine** plans of action and milestones for an agreed-upon [*basic*] sample of organizational information systems; [*reviewing*] for evidence that the process identified in PM-4.1.1.1 is being applied. |
| **PM-4.1.1.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with plan of action and milestones development and implementation responsibilities for the security program and associated organizational information systems; conducting [*basic*] discussions for further evidence that the process identified in PM-4.1.1.1 is being applied. |
|  | |  |
| **PM-4.1.2.1** | | **Examine** information security program policy, plan of action and milestones policy, procedures addressing plan of action and milestones process, information security program plan, or other relevant documents; [*reviewing*] for the process to be employed to document the remedial information security actions that mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. |
| **PM-4.1.2.2** | | **Examine** plans of action and milestones for an agreed-upon [*basic*] sample of organizational information systems; [*reviewing*] for evidence that the process identified in PM-4.1.2.1 is being applied. |
| **PM-4.1.2.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with plan of action and milestones development and implementation responsibilities for the security program and associated organizational information systems; conducting [*basic*] discussions for further evidence that the process identified in PM-4.1.2.1 is being applied. |
|  | | |