| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **PM-11** | MISSION / BUSINESS PROCESS DEFINITION | |
| **PM-11.1**  **PM-11.1.1**  **PM-11.1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and* 2. *the organization determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information security program policy; risk management policy; procedures addressing security categorization of organizational information and information systems; organizational mission/business processes; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with mission/business process definition responsibilities; organizational personnel with security categorization and risk management responsibilities for the information security program]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PM-9  concurrent controls: PM-1, PM-7, RA-2  successor controls: PL-2, PM-8 |
| **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-11.1.1.1** | | **Examine** organization mission statement and associated business process documentation; [*reviewing*] for the mission/business process definitions. |
| **PM-11.1.1.2** | | **Examine** mission/business process definitions; [*reviewing*] for evidence that mission/business processes are defined with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation arising from the operation and use of organizational information systems. |
|  | |  |
| **PM-11.1.2.1** | | **Examine** information security program policy, risk management policy, security assessment and authorization policy, procedures addressing security categorization of organizational information and information systems, procedures addressing security authorization processes, information security program plan, or other relevant documents; [*reviewing*] for the measures to be employed to determine information protection needs arising from the mission/business processes identified in PM-11.1.1.1 and revise the processes as necessary, until an achievable set of protection needs is obtained. |
| **PM-11.1.2.2** | | **Examine** security categorization results, organizational risk assessments, security plans, security control assessments, or other relevant documents for an agreed-upon [*basic*] sample of organizational information systems supporting the mission/business processes identified in PM-11.1.1.1; [*reviewing*] for evidence that the measures identified in PM-11.1.2.1 are being applied. |
| **PM-11.1.2.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with mission/business process definition responsibilities and/or organizational personnel with security categorization, security authorization, and risk management responsibilities for the information security program; conducting [*basic*] discussions for further evidence that the measures identified in PM-11.1.2.1 are being applied. |
|  | | |