| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **PM-9** | RISK MANAGEMENT STRATEGY | |
| **PM-9.1**  **PM-9.1.1**  **PM-9.1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and* 2. *the organization implements that strategy consistently across the organization.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information security program policy; risk management policy; procedures addressing risk management strategy development and implementation; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with risk management strategy development and implementation responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: None  successor controls: AC-1, AT-1, AU-1, CA-1, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1,  PE-1, PL-1, PL-2, PL-6, PM-1, PS-1, RA-1, RA-2, RA-3, SA-1, SC-1, SI-1 |
| **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-9.1.1.1** | | **Examine** risk management or information security program documentation; [*reviewing*] for an organization risk management strategy. |
| **PM-9.1.1.2** | | **Examine** organization risk management strategy; [*reviewing*] for evidence of a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems.  Note to assessor: A comprehensive strategy for managing risk should include (for example) risk identification, assessment, response, and monitoring methodologies. |
|  | |  |
| **PM-9.1.2.1** | | **Examine** information security program policy, risk management policy, procedures addressing risk management strategy development and implementation, information security program plan, or other relevant documents; [*reviewing*] for the measures to be employed to implement the strategy identified in PM-9.1.1.1 consistently across the organization. |
| **PM-9.1.2.2** | | **Examine** the measures identified in PM-9.1.2.1; [*reviewing*] for evidence that these measures are being applied. |
| **PM-9.1.2.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with risk management strategy development and implementation responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in PM-9.1.2.1 are being applied. |
|  | | |