| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **PM-6** | INFORMATION SECURITY MEASURES OF PERFORMANCE | |
| **PM-6.1**  **PM-6.1.1**  **PM-6.1.2**  **PM-6.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization develops information security measures of performance;* 2. *the organization monitors information security measures of performance; and* 3. *the organization reports on the results of information security measures of performance.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information security program policy; procedures addressing development, monitoring, and reporting of information security performance measures; information security performance metrics; information security performance measures; results of information security performance measures; other relevant documents or records]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PM-1, PM-9  concurrent controls: None  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-6.1.1.1** | | **Examine** information security program policy, procedures addressing development, monitoring, and reporting of information security performance measures, information security program plan, or other relevant documents; [*reviewing*] for the information security performance measures to be developed for the information security program. |
| **PM-6.1.1.2** | | **Examine** information security performance measures or metrics developed for the information security program; [*reviewing*] for evidence that the measures identified in PM-6.1.1.1 are being applied. |
| **PM-6.1.1.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for developing information security performance measures for the information security program; conducting [*basic*] discussions for further evidence of the measures identified in PM-6.1.1.1. |
|  | |  |
| **PM-6.1.2.1** | | **Examine** information security program policy, procedures addressing development, monitoring, and reporting of information security performance measures, information security program plan, or other relevant documents; [*reviewing*] for the process to be employed to monitor the information security performance measures identified in PM-6.1.1.1. |
| **PM-6.1.2.2** | | **Examine** monitoring records, audit records, or other relevant records for an agreed-upon [*basic*] sample of the information security performance measures or metrics identified in PM-6.1.1.1; [*reviewing*] for evidence that the process identified in PM-6.1.2.1 is being applied. |
| **PM-6.1.2.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for monitoring the information security performance measures identified in PM-6.1.1.1; conducting [*basic*] discussions for further evidence that the process identified in PM-6.1.2.1 is being applied. |
|  | |  |
| **PM-6.1.3.1** | | **Examine** information security program policy, procedures addressing development, monitoring, and reporting of information security performance measures, information security program plan, or other relevant documents; [*reviewing*] for the process to be employed to report on the results of the information security performance measures identified in PM-6.1.1.1. |
| **PM-6.1.3.2** | | **Examine** reports on results of an agreed-upon [*basic*] sample of the information security performance measures or metrics identified in PM-6.1.1.1; [*reviewing*] for evidence that the process identified in PM-6.1.3.1 is being applied. |
| **PM-6.1.3.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for reporting on results of the information security performance measures identified in PM-6.1.1.1; conducting [*basic*] discussions for further evidence that the process identified in PM-6.1.3.1 is being applied. |
|  | | |