| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **CA-5** | PLAN OF ACTION AND MILESTONES | |
| **CA-5.1**  **CA-5.1.1**  **CA-5.1.2**  **CA-5.1.3**  **CA-5.1.4**  **CA-5.1.4a**  **CA-5.1.4b**  **CA-5.1.4c** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization develops a plan of action and milestones for the information system;* 2. *the plan of action and milestones documents the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system;* 3. *the organization defines the frequency of plan of action and milestone updates; and* 4. *the organization updates the plan of action and milestones at an organization-defined frequency with findings from:*    * *security controls assessments;*    * *security impact analyses; and*    * *continuous monitoring activities.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security assessment and authorization policy; procedures addressing plan of action and milestones; security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; 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, RA-3, RA-5, SA-11, SI-2  concurrent controls: PM-4  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. |
| **CA-5.1.1.1** | | **Examine** information system documentation; [*reviewing*] for a plan of action and milestones for the information system. |
|  | |  |
| **CA-5.1.2.1** | | **Examine** an agreed-upon [*basic*] sample of controls in the security assessment report and the associated plan of action and milestones; [*reviewing*] for evidence that the plan of action and milestones documents the planned remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. |
|  | |  |
| **CA-5.1.3.1** | | **Examine** security assessment and authorization policy, procedures addressing plan of action and milestones, security plan, or other relevant documents; [*reviewing*] for the frequency for updating the plan of action and milestones. |
|  | |  |
| **CA-5.1.4.1**  **CA-5.1.4.1.a**  **CA-5.1.4.1.b**  **CA-5.1.4.1.c** | | **Examine** security assessment and authorization policy, procedures addressing plan of action and milestones, security plan, or other relevant documents; [*reviewing*] for the frequency identified in CA-5.1.3.1 for updating the plan of action and milestones with findings from:   * + security controls assessments;   + security impact analyses; and   + continuous monitoring activities. |
| **CA-5.1.4.2** | | **Examine** an agreed-upon [*basic*] sample of findings in the security assessment report and the associated plan of action and milestones; [*reviewing*] for evidence that the plan of action and milestones is updated in accordance with the frequency identified in CA-5.1.4.1.a. |
| **CA-5.1.4.3** | | **Examine** an agreed-upon [*basic*] sample of findings from security impact analyses and the associated plan of action and milestones; [*reviewing*] for evidence that the plan of action and milestones is updated in accordance with the frequency identified in CA-5.1.4.1.b. |
| **CA-5.1.4.4** | | **Examine** an agreed-upon [*basic*] sample of findings from continuous monitoring activities and the associated plan of action and milestones; [*reviewing*] for evidence that the plan of action and milestones is updated in accordance with the frequency identified in CA-5.1.4.1.c. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **CA-5(1)** | | PLAN OF ACTION AND MILESTONES |
| **CA-5(1).1**  **CA-5(1).1.1**  **CA-5(1).1.1a**  **CA-5(1).1.1b**  **CA-5(1).1.1c** | | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is:*   * *accurate;* * *up to date; and* * *readily available.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security assessment and authorization policy; procedures addressing plan of action and milestones; information system design documentation, information system configuration settings and associated documentation; plan of action and milestones; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with plan of action and milestones development and implementation responsibilities].  **Test**: [*select from:* Automated mechanisms for developing, implementing and maintaining plan of action and milestones]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CA-2, CA-7, CM-4, RA-3, RA-5, SA-11, SI-2  concurrent controls: CM-6, PM-4  successor controls: CA-6, PM-10 |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **CA-5(1).1.1**  **CA-5(1).1.1.a**  **CA-5(1).1.1.b**  **CA-5(1).1.1.c** | | **Examine** security plan, information system design documentation , or other relevant documents or records; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to help ensure that the plan of action and milestones for the information system is:   * accurate; * up to date; and * readily available. |
| **CA-5(1).1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of automated mechanisms identified in CA-5(1).1.a; [*reviewing*] for evidence that these mechanisms are configured to help ensure that the plan of action and milestones for the information system is accurate as identified in CA-5(1).1.a. |
| **CA-5(1).1.1.3** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of automated mechanisms identified in CA-5(1).1.b; [*reviewing*] for evidence that these mechanisms are configured to help ensure that the plan of action and milestones for the information system is up to date as identified in CA-5(1).1.b. |
| **CA-5(1).1.1.4** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of automated mechanisms identified in CA-5(1).1.c; [*reviewing*] for evidence that these mechanisms are configured to help ensure that the plan of action and milestones for the information system is readily available s as identified in CA-5(1).1.c. |