| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AC-5** | SEPARATION OF DUTIES | |
| **AC-5.1**  **AC-5.1.1**  **AC-5.1.2**  **AC-5.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization separates duties of individuals as necessary, to prevent malevolent activity without collusion;* 2. *the organization documents separation of duties; and* 3. *the organization implements separation of duties through assigned information system access authorizations.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing divisions of responsibility and separation of duties; information system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties].  **Test**: [*select from:* Automated mechanisms implementing separation of duties policy]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, IA-2  concurrent controls: AC-6, PS-2, PS-6  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. |
| **AC-5.1.1.1** | | **Examine** access control policy, procedures addressing divisions of responsibility and separation of duties, security plan, or other relevant documents; [*reviewing*] for measures to be employed to separate duties of individuals, as necessary, to prevent malevolent activity without collusion. |
| **AC-5.1.1.2** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties for the information system; conducting [*basic*] discussions for evidence that the measures identified in AC-5.1.1.1 are being applied. |
|  | |  |
| **AC-5.1.2.1** | | **Examine** access control policy, procedures addressing divisions of responsibility and separation of duties, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to document separation of duties for the information system. |
| **AC-5.1.2.2** | | **Examine** job descriptions, position descriptions, or other relevant documents for an agreed-upon [*basic*] sample of individuals providing information system support functions; [*reviewing*] for evidence that the measures identified in AC-5.1.2.1 are being applied |
|  | |  |
| **AC-5.1.3.1** | | **Examine** access control policy, procedures addressing divisions of responsibility and separation of duties, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to implement separation of duties through assigned information system access authorizations. |
| **AC-5.1.3.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-5.1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-5.1.3.1. |
| **AC-5.1.3.3** | | **Examine** access authorizations, access control profiles, and the duties and responsibilities documented for an agreed-upon [*basic*] sample of information system users; [*reviewing*] for evidence that the measures identified in AC-5.1.3.1 are being applied. |
| **AC-5.1.3.4** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-5.1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |