| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **PS-7** | THIRD-PARTY PERSONNEL SECURITY | |
| **PS-7.1**  **PS-7.1.1**  **PS-7.1.2**  **PS-7.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers;* 2. *the organization documents personnel security requirements for third-party providers; and* 3. *the organization monitors third-party provider compliance with personnel security requirements.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with personnel security responsibilities; third-party providers]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-5, PS-2  concurrent controls: CA-3, MA-4, MA-5, PL-4, PS-3, PS-6, PS-8, SA-4, SA-9  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. |
| **PS-7.1.1.1** | | **Examine** personnel security policy, procedures addressing third-party personnel security, security plan, or other relevant documents; [*reviewing*] for the personnel security requirements established for third-party providers of organizational information system services. |
| **PS-7.1.1.2** | | **Examine** personnel security requirements identified in PS-7.1.1.1; [*reviewing*] for security roles and responsibilities established for third-party providers of organizational information system services. |
|  | |  |
| **PS-7.1.2.1** | | **Examine** personnel security policy, procedures addressing third-party personnel security, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to document and enforce the personnel security requirements identified in PS-7.1.1.1 for third-party providers of organizational information system services. |
| **PS-7.1.2.2** | | **Examine** service level agreements, service delivery contracts, service acquisition contracts, maintenance service contracts, or other relevant documents for an agreed-upon [*basic*] sample of third-party providers of information system services; [*reviewing*] for evidence that the measures identified in PS-7.1.2.1 are being applied. |
|  | |  |
| **PS-7.1.3.1** | | **Examine** personnel security policy, procedures addressing third-party personnel security, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to monitor third-party provider compliance with the personnel security requirements identified in PS-7.1.1.1 and subsequently documented/enforced as identified in PS-7.1.2.1.  Note to assessor: Organizations may negotiate a “right-to-audit” clause with third-party providers to establish contractual terms and conditions for monitoring provider compliance with organizational security requirements. |
| **PS-7.1.3.2** | | **Examine** compliance monitoring records, compliance assessments, compliance audits, security assessments, other relevant documents for an agreed-upon [*basic*] sample of contractual agreements identified in PS-7.1.2.1 for third-party providers of information system services; [*reviewing*] for evidence that the measures identified in PS-7.1.3.1 are being applied. |
| **PS-7.1.3.3** | | **Examine** compliance monitoring process; [*observing*] for evidence that the measures identified in PS-7.1.3.1 are being applied.  Note to assessor: This assessor action can be performed if the assessment period coincides with the organization’s execution of the compliance monitoring process. |
| **PS-7.1.3.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with compliance monitoring responsibilities for third-party providers of information system services; conducting [*basic*] discussions for further evidence that the measures identified in PS-7.1.3.1 are being applied. |
|  | | |