| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SA-9** | EXTERNAL INFORMATION SYSTEM SERVICES | |
| **SA-9.1**  **SA-9.1.1**  **SA-9.1.2**  **SA-9.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;* 2. *the organization defines and documents government oversight, and user roles and responsibilities with regard to external information system services; and* 3. *the organization monitors security control compliance by external service providers.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with system and services acquisition responsibilities; external providers of information system services]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: SA-4, SA-5, SA-12  concurrent controls: CA-2, CA-3, CA-7, PS-7  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. |
| **SA-9.1.1.1** | | **Examine** system and services acquisition policy, procedures addressing external information system services, acquisition contracts, service level agreements, security plan, or other relevant documents; [*reviewing*] for the requirement that providers of external information system services comply with organizational information security requirements. |
| **SA-9.1.1.2** | | **Examine** system and services acquisition policy, procedures addressing external information system services, acquisition contracts, service level agreements, security plan, or other relevant documents; [*reviewing*] for the requirement that providers of external information system services employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. |
|  | |  |
| **SA-9.1.2.1** | | **Examine** system and services acquisition policy, procedures addressing external information system services, acquisition contracts, service level agreements, security plan, or other relevant documents; [*reviewing*] for the government oversight provisions, and user roles and responsibilities, with regard to external information system services. |
|  | |  |
| **SA-9.1.3.1** | | **Examine** system and services acquisition policy, procedures addressing external information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to monitor security control compliance by external service providers. |
| **SA-9.1.3.2** | | **Examine** an agreed-upon [*basic*] sample of security control assessment evidence from external providers of information system services, or other relevant documents; [*reviewing*] for evidence that the measures identified in SA-9.1.3.1 are being applied. |
| **SA-9.1.3.3** | | **Interview** external providers of information system services and/or an agreed-upon [*basic*] sample of organizational personnel with responsibilities for monitoring security control compliance by external service providers; conducting [*basic*] discussions for further evidence that the measures identified in SA-9.1.3.1 are being applied. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-9(1)** | EXTERNAL INFORMATION SYSTEM SERVICES |
| **SA-9(1).1**  **SA-9(1).1.1**  **SA-9(1).1.2**  **SA-9(1).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services;* 2. *the organization defines the senior organizational official designated to approve the acquisition or outsourcing of dedicated information security services; and* 3. *the designated senior organizational official approves the acquisition or outsourcing of dedicated information security services.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; risk assessment reports; other relevant documents or records].  **Interview:** [*select from:* Organizational personnel with information system security, acquisition, and contracting responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: SA-4, SA-5, SA-12  concurrent controls: CA-6, PS-7, RA-3  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-9(1).1.1.1** | **Examine** system and services acquisition policy, risk assessment policy, procedures addressing the integration of information security requirements and/or security specifications into the acquisition process, solicitation documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to conduct an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services. |
| **SA-9(1).1.1.2** | **Examine** an agreed-upon [*basic*] sample of organizational risk assessment reports; [*reviewing*] for evidence that the measures identified in SA-9(1).1.1.1 are being applied. |
| **SA-9(1).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system security, acquisition, and contracting responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in SA-9(1).1.1.1 are being applied. |
|  |  |
| **SA-9(1).1.2.1** | **Examine** system and services acquisition policy, procedures addressing the integration of information security requirements and/or security specifications into the acquisition process, security plan, or other relevant documents; [*reviewing*] for the senior organizational official designated to approve the acquisition or outsourcing of dedicated information security services. |
|  |  |
| **SA-9(1).1.3.1** | **Examine** an agreed-upon [*basic*] sample of acquisition contracts or other relevant acquisition-related documentation for information system services; [*reviewing*] for evidence that the senior organizational official identified in SA-9(1).1.2.1 approves the acquisition or outsourcing of dedicated information security services. |