| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AC-20** | USE OF EXTERNAL INFORMATION SYSTEMS | |
| **AC-20.1**  **AC-20.1.1**  **AC-20.1.1a**  **AC-20.1.1b**  **AC-20.1.2**  **AC-20.1.2a**  **AC-20.1.2b** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization identifies individuals authorized to:*    * *access the information system from the external information systems; and*    * *process, store, and/or transmit organization-controlled information using the external information systems; and* 2. *the organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:*    * *access the information system from the external information systems; and*    * *process, store, and/or transmit organization-controlled information using the external information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum security categorization for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for defining terms and conditions for use of external information systems to access organizational systems]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-2, AC-3, AC-4, AC-17, AC-19, CA-3, PL-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. |
| **AC-20.1.1.1**  **AC-20.1.1.1.a**  **AC-20.1.1.1.b** | | **Examine** access control policy, procedures addressing the use of external information systems, security plan, or other relevant documents; [*reviewing*] for the individuals authorized to:   * + access the information system from the external information systems; and   + process, store, and/or transmit organization-controlled information using the external information systems |
|  | |  |
| **AC-20.1.2.1**  **AC-20.1.2.1.a**  **AC-20.1.2.1.b** | | **Examine** access control policy, procedures addressing the use of external information systems, security plan, or other relevant documents; [*reviewing*] for the terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:   * + access the information system from the external information systems; and   + process, store, and/or transmit organization-controlled information using the external information system |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **AC-20(1)** | | USE OF EXTERNAL INFORMATION SYSTEMS |
| **AC-20(1).1**  **AC-20(1).1.1**  **AC-20(1).1.1.a**  **AC-20(1).1.1.b** | | **ASSESSMENT OBJECTIVE:**  *Determine if the organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:*   * *can verify the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan; or* * *has approved information system connection or processing agreements with the organizational entity hosting the external information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing the use of external information systems; security plan; information system connection or processing agreements; account management documents; other relevant documents or records]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CA-3, PL-4, SA-9  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **AC-20(1).1.1.1**  **AC-20(1).1.1.1.a**  **AC-20(1).1.1.1.b** | | **Examine** access control policy, procedures addressing the use of external information systems, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to permit only authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information when the organization:   * can verify the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan; or * has approved information system connection or processing agreements with the organizational entity hosting the external information system. |
| **AC-20(1).1.1.2** | | **Examine** records verifying the implementation of required security controls on the external information systems for an agreed-upon [*basic*] sample of external information systems used to access the organizational information system; [*reviewing*] for evidence that the measures identified in AC-20(1).1.1.1.a are being applied to verify the implementation of required security controls on external systems. |
| **AC-20(1).1.1.3** | | **Examine** documented connection approvals or processing agreements for an agreed-upon [*basic*] sample of external information systems used to access the organizational information system; [*reviewing*] for evidence that the measures identified in AC-20(1).1.1.1.b are being applied to approve information system connections or processing agreements. |
| **AC-20(1).1.1.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for authorizing individuals to use external information systems to access the organizational information system; [*reviewing*] for further evidence that the measures identified in AC-20(1).1.1.1.a are being applied to verify the implementation of required security controls on external systems. |
| **AC-20(1).1.1.5** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for authorizing individuals to use external information systems to access the organizational information system; [*reviewing*] for further evidence that the measures identified in AC-20(1).1.1.1.b are being applied to approve information system connections or processing agreements. |
|  | | |
| **ASSESSMENT – Control Enhancement 2** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **AC-20(2)** | | USE OF EXTERNAL INFORMATION SYSTEMS |
| **AC-20(2).1**  **AC-20(2).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing the use of external information systems; security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; other relevant documents or records]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: PL-4, SA-9  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **AC-20(2).1.1.1** | | **Examine** access control policy, procedures addressing the use of external information systems, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to limit the use of organization-controlled portable storage media by authorized individuals on external information systems. |
| **AC-20(2).1.1.2** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for controlling the use of portable storage media; [*reviewing*] for evidence that the measures identified in AC-20(2).1.1.1 are being applied. |