| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AC-21** | USER-BASED COLLABORATION AND INFORMATION SHARING | |
| **AC-21.1**  **AC-21.1.1**  **AC-21.1.2**  **AC-21.1.3**  **AC-21.1.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the circumstances where user discretion is required to facilitate information sharing;* 2. *the organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for the organization-defined circumstances;* 3. *the organization defines the information sharing circumstances and automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions; and* 4. *the organization employs organization-defined circumstances and automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing user-based collaboration and information sharing (including restrictions); information system design documentation; information system configuration settings and associated documentation; list of users authorized to make information sharing/collaboration decisions; list of information sharing circumstances requiring user discretion; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel responsible for making information sharing/collaboration decisions].  **Test**: [*select from:* Automated mechanisms or manual process implementing access authorizations supporting information sharing/user collaboration decisions]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-2, AC-3, AC-6, AU-13, CM-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-21.1.1.1** | | **Examine** access control policy, procedures addressing user-based collaboration and information sharing (including restrictions), security plan, or other relevant documents; [*reviewing*] for the circumstances where user discretion is required to facilitate information sharing. |
|  | |  |
| **AC-21.1.2.1** | | **Examine** access control policy, procedures addressing user-based collaboration and information sharing (including restrictions), security plan, or other relevant documents; [*reviewing*] for the measures to be employed to enable authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for the circumstances identified in AC-21.1.1.1. |
| **AC-21.1.2.2** | | **Examine** an agreed-upon [*basic*] sample of records used to facilitate information sharing decisions; [*reviewing*] for evidence that the measures identified in AC-21.1.2.1 are being applied to enable users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for information sharing circumstances. |
| **AC-21.1.2.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for making information sharing/collaboration decisions; [*reviewing*] for further evidence that the measures identified in AC-21.1.2.1 are being applied. |
|  | |  |
| **AC-21.1.3.1** | | **Examine** access control policy, procedures addressing user-based collaboration and information sharing (including restrictions), security plan, or other relevant documents; [*reviewing*] for the information sharing circumstances (i.e. access authorizations of sharing partners and access restrictions on information to be shared) to be considered when making information sharing decisions. |
| **AC-21.1.3.2** | | **Examine** access control policy, procedures addressing user-based collaboration and information sharing (including restrictions), security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms (and their configuration settings) or manual processes required to assist users in making information sharing/collaboration decisions based on the information sharing circumstances identified in AC-21.1.3.1. |
|  | |  |
| **AC-21.1.4.1** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-21.1.3.2, if applicable; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-21.1.3.2. |
| **AC-21.1.4.2** | | **Examine** an agreed-upon [*basic*] sample of records used to facilitate information sharing decisions; [*reviewing*] for evidence that the measures identified in AC-21.1.3.2 are being applied to assist users in making information sharing/collaboration decisions. |
| **AC-21.1.4.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for making information sharing/collaboration decisions; [*reviewing*] for further evidence that the measures identified in AC-21(1).1.3.2 are being applied. |
| **AC-21.1.4.4** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-21.1.3.2, if applicable; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-21(1)** | USER-BASED COLLABORATION AND INFORMATION SHARING |
| **AC-21(1).1**  **AC-21(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system employs automated mechanisms to enable authorized users to make information-sharing decisions based on access authorizations of sharing partners and access restrictions on information to be shared.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing user-based collaboration and information sharing (including restrictions); information system design documentation; information system configuration settings and associated documentation; system-generated list of users authorized to make information sharing/collaboration decisions; system-generated list of sharing partners and access authorizations; system-generated list of access restrictions regarding information to be shared; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing access authorizations supporting information sharing/user collaboration decisions]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-2, AC-3, AC-6, AU-13, CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-21(1).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to enable authorized users to make information-sharing decisions based on access authorizations of sharing partners and access restrictions on information to be shared. |
| **AC-21(1).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-21(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-21(1).1.1.1. |
| **AC-21(1).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-21(1).1.1.1; conducting [*basic*] testing for evidence these mechanisms are operating as intended. |