| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AC-3** | ACCESS ENFORCEMENT | |
| **AC-3.1**  **AC-3.1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system enforces approved authorizations for logical access to the system in accordance with applicable policy.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing access enforcement; information system configuration settings and associated documentation; list of approved authorizations (user privileges); information system audit records; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing access enforcement policy]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22,  AU-9, CM-5, IA-2, IA-4, IA-5, MA-3, MA-4, MA-5, MP-2, SA-7, SI-9  concurrent controls: AC-4 , 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-3.1.1.1** | | **Examine** access control policy, procedures addressing access enforcement, 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 enforce approved authorizations for logical access to the system in accordance with applicable policy. |
| **AC-3.1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-3.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-3.1.1.1. |
| **AC-3.1.1.3** | | **Examine** documentation describing the current user privileges on the information system for an agreed-upon [*basic*] sample of information system users, along with the list of approved authorizations (user privileges); [*reviewing*] for evidence that the user privileges on the information system are consistent with the approved user authorizations. |
| **AC-3.1.1.4** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-3.1.1.1; 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-3(1)** | | ACCESS ENFORCEMENT  [Withdrawn: Incorporated into AC-6]. |
| **AC-3(1).1** | | **ASSESSMENT OBJECTIVE:**  [Withdrawn: Incorporated into AC-6].  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  [Withdrawn: Incorporated into AC-6]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: N/A  concurrent controls: N/A  successor controls: N/A |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **N/A** | | N/A |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-3(2)** | ACCESS ENFORCEMENT |
| **AC-3(2).1**  **AC-3(2).1.1**  **AC-3(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines, in organizational policies and procedures, the privileged commands for which dual authorization is to be enforced; and* 2. *the information system enforces dual authorization based on organizational policies and procedures for organization-defined privileged commands.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing access enforcement and dual authorization; security plan; information system design documentation; information system configuration settings and associated documentation; list of privileged commands requiring dual authorization; list of approved authorizations (user privileges); other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with access enforcement responsibilities].  **Test**: [*select from:* Dual authorization mechanisms implementing access control policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, IA-2, IA-4, IA-5  concurrent controls: CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-3(2).1.1.1** | **Examine** access control policy, procedures addressing access enforcement and dual authorization, security plan, or other relevant documents; [*reviewing*] for the privileged commands for which dual authorization is to be enforced. |
|  |  |
| **AC-3(2).1.2.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to enforce dual authorization based on organizational policies for the privileged commands identified in AC-3(2).1.1.1. |
| **AC-3(2).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-3(2).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-3(2).1.2.1. |
| **AC-3(2).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-3(2).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-3(3)** | ACCESS ENFORCEMENT |
| **AC-3(3).1**  **AC-3(3).1.1**  **AC-3(3).1.2**  **AC-3(3).1.2a**  **AC-3(3).1.2b**  **AC-3(3).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the users and resources over which the information system is to enforce nondiscretionary access control policies;* 2. *the organization defines nondiscretionary access control policies to be enforced over the organization-defined set of users and resources, where the rule set for each policy specifies:*    * *access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and*    * *required relationships among the access control information to permit access; and* 3. *the information system enforces organization-defined nondiscretionary access control policies over the organization-defined set of users and resources.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; nondiscretionary access control policies; procedures addressing access enforcement; security plan; information system design documentation; information system configuration settings and associated documentation; list of users and resources requiring enforcement of nondiscretionary access control policies; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with access enforcement responsibilities].  **Test**: [*select from:* Automated mechanisms implementing nondiscretionary access control policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, IA-2, IA-4, IA-5  concurrent controls: CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-3(3).1.1.1** | **Examine** access control policy, nondiscretionary access control policies, procedures addressing access enforcement, security plan, or other relevant documents; [*reviewing*] for the list of users and resources over which the information system is to enforce nondiscretionary access control policies. |
|  |  |
| **AC-3(3).1.2.1**  **AC-3(3).1.2.1.a**  **AC-3(3).1.2.1.b** | **Examine** access control policy, nondiscretionary access control policies, procedures addressing access enforcement, security plan, or other relevant documents; [*reviewing*] for the access control policies to be enforced over the user and resources identified in AC-3(3).1.1.1, that specifies:   * + access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and   + required relationships among the access control information to permit access. |
|  |  |
| **AC-3(3).1.3.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to enforce the nondiscretionary access control policies identified in AC-3(3).1.2.1 over the users and resources identified in AC-3(3).1.1.1. |
| **AC-3(3).1.3.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-3(3).1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-3(3).1.3.1. |
| **AC-3(3).1.3.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-3(3).1.3.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-3(4)** | ACCESS ENFORCEMENT |
| **AC-3(4).1**  **AC-3(4).1.1**  **AC-3(4).1.1a**  **AC-3(4).1.1b  AC-3(4).1.1c** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system enforces a Discretionary Access Control (DAC) policy that:*   * *allows users to specify and control sharing by named individuals or groups of individuals, or by both;* * *limits propagation of access rights; and* * *includes or excludes access to the granularity of a single user.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; discretionary access control policy; procedures addressing access enforcement; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing discretionary access control policy]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, IA-2, IA-4, IA-5  concurrent controls: CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-3(4).1.1.1**  **AC-3(4).1.1.1.a**  **AC-3(4).1.1.1.b**  **AC-3(4).1.1.1.c** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to enforce a Discretionary Access Control (DAC) policy that:   * allows users to specify and control sharing by named individuals or groups of individuals, or by both; * limits propagation of access rights; and * includes or excludes access to the granularity of a single user. |
| **AC-3(4).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-3(4).1.1.1.a; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-3(4).1.1.1.a to allow users to specify and control sharing by named individuals or groups of individuals, or by both. |
| **AC-3(4).1.1.3** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-3(4).1.1.1.b; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-3(4).1.1.1.b to limit propagation of access rights. |
| **AC-3(4).1.1.4** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-3(4).1.1.1.c; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-3(4).1.1.1.c to include or exclude access to the granularity of a single user. |
| **AC-3(4).1.1.5** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-3(4).1.1.1.a; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in AC-3(4).1.1.1.a to allow users to specify and control sharing by named individuals or groups of individuals, or by both. |
| **AC-3(4).1.1.6** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-3(4).1.1.1.b; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in AC-3(4).1.1.1.b to limit propagation of access rights. |
| **AC-3(4).1.1.7** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-3(4).1.1.1.c; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in AC-3(4).1.1.1.c to include or exclude access to the granularity of a single user. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-3(5)** | ACCESS ENFORCEMENT |
| **AC-3(5).1**  **AC-3(5).1.1**  **AC-3(5).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the security-relevant information to which the information system prevents access except during secure, nonoperable system states; and* 2. *the information system prevents access to organization-defined security-relevant information except during secure, nonoperable system states.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing access enforcement; security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with access enforcement responsibilities].  **Test**: [*select from:* Automated mechanisms preventing access to security-relevant information within the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-6  concurrent controls: CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-3(5).1.1.1** | **Examine** access control policy, procedures addressing access enforcement, security plan, or other relevant documents; [*reviewing*] for the security-relevant information to which the information system prevents access except during secure, non-operable system states. |
| **AC-3(5).1.2.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to prevent access to the security-relevant information identified in AC-3(5).1.1.1, except during secure, non-operable system states. |
|  |  |
| **AC-3(5).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in AC-3(5).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-3(5).1.2.1. |
| **AC-3(5).1.2.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in AC-3(5).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 6** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-3(6)** | ACCESS ENFORCEMENT |
| **AC-3(6).1**  **AC-3(6).1.1**  **AC-3(6).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the user and/or system information to be encrypted or stored off-line in a secure location; and* 2. *the organization encrypts, or stores off-line in a secure location, organization-defined user and/or system information.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing access enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with access enforcement responsibilities].  **Test**: [*select from:* Automated mechanisms implementing access enforcement functions]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, MP-4, SC-13, SC-28  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-3(6).1.1.1** | **Examine** access control policy, procedures addressing access enforcement, security plan, or other relevant documents; [*reviewing*] for the user and/or system information to be encrypted or stored off-line in a secure location. |
|  |  |
| **AC-3(6).1.2.1** | **Examine** access control policy, procedures addressing access enforcement, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to encrypt, or store off-line in a secure location, the user and/or system information identified in AC-3(6).1.1.1. |
| **AC-3(6).1.2.2** | **Examine** the measures employed to encrypt (if applicable) an agreed-upon [*basic*] sample of user and/or system information identified in AC-3(6).1.1.1; [*reviewing*] for evidence that the measures identified in AC-3(6).1.2.1 are being applied to encrypt user and/or system information. |
| **AC-3(6).1.2.3** | **Examine** the measures employed to (if applicable) store off-line, in a secure location, an agreed-upon [*basic*] sample of user and/or system information identified in AC-3(6).1.1.1; [*reviewing*] for evidence that the measures identified in AC-3(6).1.2.1 are being applied to store off-line, in a secure location, user and/or system information. |