| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AC-6** | LEAST PRIVILEGE | |
| **AC-6.1**  **AC-6.1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, IA-2  concurrent controls: AC-5, 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-6.1.1.1** | | **Examine** account control policy, procedures addressing least privilege, 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 the concept of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. |
| **AC-6.1.1.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AC-6.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-6.1.1.1. |
| **AC-6.1.1.3** | | **Examine** assigned access authorizations (user privileges) and required functions necessary to accomplish assigned tasks for an agreed-upon [*basic*] sample of information system users; [*reviewing*] for evidence that the measures identified in AC-6.1.1.1 are being applied. |
| **AC-6.1.1.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for employing the concept of least privilege; conducting [*basic*] discussions for further evidence that the measures identified in AC-6.1.1.1 are being applied. |
| **AC-6.1.1.5** | | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AC-6.1.1.1; conducting [*basic*] testing for further evidence that these mechanisms are operating as intended. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **AC-6(1)** | | LEAST PRIVILEGE |
| **AC-6(1).1**  **AC-6(1).1.1**  **AC-6(1).1.2** | | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized; and* 2. *the organization explicitly authorizes access to the organization-defined security functions and security-relevant information.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing least privilege; list of security functions and security-relevant information for which access must be explicitly authorized; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, IA-2  concurrent controls: AC-17, SC-3, SC-11  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **AC-6(1).1.1.1** | | **Examine** access control policy, procedures addressing least privilege, security plan, or other relevant documents; [*reviewing*] for the security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized. |
|  | |  |
| **AC-6(1).1.2.1** | | **Examine** access control policy, procedures addressing least privilege, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to explicitly authorize access to the security functions and security-relevant information identified in AC-6(1).1.1.1. |
| **AC-6(1).1.2.2** | | **Examine** access authorization approvals for an agreed-upon [*basic*] sample of information system accounts with access to the security functions and security-relevant information identified in AC-6(1).1.1.1; [*reviewing*] for evidence that the measures identified in AC-6(1).1.2.1 are being applied to explicitly authorize access. |
| **AC-6(1).1.2.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for authorizing access to security functions and security-relevant information; conducting [*basic*] discussions for further evidence that the measures identified in AC-6(1).1.2.1 are being applied. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-6(2)** | LEAST PRIVILEGE |
| **AC-6(2).1**  **AC-6(2).1.1**  **AC-6(2).1.2**  **AC-6(2).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access; and* 2. *the organization requires that users of information system accounts, or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions; and* 3. *the organization, if deemed feasible, audits any use of privileged accounts, or roles, with access to organization-defined security functions or security-relevant information, when accessing other system functions.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing least privilege; list of system-generated security functions or security-relevant information assigned to information system accounts or roles; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, IA-2  concurrent controls: AC-17, SC-3, AU-2, AU-3, AU-6, AU-12  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-6(1).1.1.1** | **Examine** access control policy, procedures addressing least privilege, security plan, or other relevant documents; [*reviewing*] for the security functions or security-relevant information to which users of information system accounts, or roles, have access. |
|  |  |
| **AC-6(1).1.2.1** | **Examine** access control policy, procedures addressing least privilege, security plan, or other relevant documents; [*reviewing*] for the requirement that users of information system accounts, or roles, with access to the security functions or security-relevant information identified in AC-6(1).1.1.1, use non-privileged accounts when accessing other system functions. |
|  |  |
| **AC-6(2).1.3.1** | **Examine** access control policy, procedures addressing least privilege, security plan, or other relevant documents; [*reviewing*] for the measures to be employed, if deemed feasible, to audit any use of privileged accounts, or roles, with access to the security functions or security-relevant information identified in AC-6(1).1.1.1, when accessing other system functions. |
| **AC-6(2).1.3.2** | **Examine** an agreed-upon [*basic*] sample of information system audit records resulting from the use of privileged accounts or roles with access to the security functions or security-relevant information identified in AC-6(1).1.1.1, when accessing other system functions; [*reviewing*] for evidence that the measures identified in AC-6(2).1.3.1 are being applied. |
| **AC-6(2).1.3.3** | **Interview** an agreed-upon [*basic*] sample of organizational officials responsible for auditing the use of privileged accounts or roles; conducting [*basic*] discussions for evidence that the measures identified in AC-6(2).1.3.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-6(3)** | LEAST PRIVILEGE |
| **AC-6(3).1**  **AC-6(3).1.1**  **AC-6(3).1.2**  **AC-6(3).1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the privileged commands to which network access is to be authorized only for compelling operational needs;* 2. *the organization authorizes network access to organization-defined privileged commands only for compelling operational needs; and* 3. *the organization documents the rationale for authorized network access to organization-defined privileged commands in the security plan for the information system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing least privilege; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, IA-2  concurrent controls: None  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-6(3).1.1.1** | **Examine** access control policy, procedures addressing least privilege, security plan, or other relevant documents; [*reviewing*] for the privileged commands to which network access is to be authorized only for compelling operational needs. |
|  |  |
| **AC-6(3).1.2.1** | **Examine** access control policy, procedures addressing least privilege, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to authorize network access to the privileged commands identified in AC-6(3).1.1.1 only for compelling operational needs. |
|  |  |
| **AC-6(3).1.2.2** | **Examine** network access authorization approvals for an agreed-upon [*basic*] sample of accounts with network access to the privileged commands identified in AC-6(3).1.1.1; [*reviewing*] for evidence that the measures identified in AC-6(3).1.2.1 are being applied. |
| **AC-6(3).1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational officials responsible for authorizing network access to privileged commands; conducting [*basic*] discussions for further evidence that the measures identified in AC-6(3).1.2.1 are being applied. |
|  |  |
| **AC-6(3).1.3.1** | **Examine** security plan; [*reviewing*] for the rationale documented for authorized network access to the privileged commands identified in AC-6(3).1.1.1. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-6(4)** | LEAST PRIVILEGE |
| **AC-6(4).1**  **AC-6(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system provides separate processing domains to enable finer-grained allocation of user privileges.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing least privilege; 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 responsibilities for defining least privileges necessary to accomplish specified tasks]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, SC-2, SC-3, SC-32  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-6(4).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and configuration settings to be employed by the information system to provide separate processing domains to enable finer-grained allocation of user privilege. |
| **AC-6(4).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AC-6(4).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AC-6(4).1.1.1 |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-6(5)** | LEAST PRIVILEGE |
| **AC-6(5).1**  **AC-6(5).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization limits authorization to super user accounts on the information system to designated system administration personnel.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing least privilege; list of system-generated super user accounts; list of system administration personnel; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, IA-2, IA-4, IA-5  concurrent controls: MA-5  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-6(5).1.1.1** | **Examine** access control policy, procedures addressing least privilege, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to limit authorization to super user accounts to designated system administration personnel. |
| **AC-6(5).1.1.2** | **Examine** list of system-generated super user accounts and list of system administration personnel; [*reviewing*] for evidence that the measures identified in AC-6(5).1.1.1 are being applied. |
| **AC-6(5).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for authorizing super user accounts on the information system; conducting [*basic*] discussions for further evidence that the measures identified in AC-6(5).1.1.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 6** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AC-6(6)** | LEAST PRIVILEGE |
| **AC-6(6).1**  **AC-6(6).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization prohibits privileged access to the information system by non-organizational users.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Access control policy; procedures addressing least privilege; list of system-generated privileged accounts; list of non-organizational users; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-2, AC-3, IA-2, IA-8  concurrent controls: None  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AC-6(6).1.1.1** | **Examine** access control policy, procedures addressing least privilege, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to prohibit privileged access to the information system by non-organizational users. |
| **AC-6(6).1.1.2** | **Examine** list of system-generated privileged accounts and list of non-organizational users; [*reviewing*] for evidence that the measures identified in AC-6(6).1.1.1 are being applied. |
| **AC-6(6).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for authorizing privileged accounts on the information system; conducting [*basic*] discussions for further evidence that the measures identified in AC-6(6).1.1.1 are being applied. |