| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **PS-3** | PERSONNEL SCREENING | |
| **PS-3.1**  **PS-3.1.1**  **PS-3.1.2**  **PS-3.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization screens individuals prior to authorizing access to the information system;* 2. *the organization defines conditions requiring re-screening and, where re-screening is so indicated, the frequency of such re-screening; and* 3. *the organization re-screens individuals according to organization-defined conditions requiring re-screening and, where re-screening is so indicated, the organization-defined frequency of such re-screening.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Personnel security policy; procedures addressing personnel screening; records of screened personnel; security plan; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with personnel security responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PS-2  concurrent controls: None  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. |
| **PS-3.1.1.1** | | **Examine** personnel security policy, procedures addressing personnel screening, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to screen individuals prior to authorizing access to the information system. |
| **PS-3.1.1.2** | | **Examine** personnel screening records and access authorizations for anagreed-upon [*basic*] sample of individuals with access to the information system; [*reviewing*] for evidence that the measures identified in PS-3.1.1.1 are being applied. |
|  | |  |
| **PS-3.1.2.1** | | **Examine** personnel security policy, procedures addressing personnel re-screening, procedures addressing personnel screening, security plan, or other relevant documents; [*reviewing*] for the conditions requiring personnel re-screening and the frequency of such re-screening.  Note to assessor: The organization may define different re-screening conditions and frequencies for personnel accessing the information system. |
|  | |  |
| **PS-3.1.3.1** | | **Examine** personnel security policy, procedures addressing personnel re-screening, procedures addressing personnel screening, 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 identify personnel requiring re-screening in accordance with the conditions and frequency identified in PS-3.1.2.1 |
| **PS-3.1.3.2** | | **Examine** personnel security policy, procedures addressing personnel re-screening, procedures addressing personnel screening, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to re-screen individuals in accordance with the conditions and frequency identified in PS-3.1.2.1 |
| **PS-3.1.3.3** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in PS-3.1.3.1; [*reviewing*] for evidence that these mechanisms are configured as identified in PS-3.1.3.1. |
| **PS-3.1.3.4** | | **Examine** an agreed-upon [*basic*] sample of personnel records, personnel security status reports, personnel security activity reports, or other relevant documents used to identify personnel requiring (or that required) re-screening; [*reviewing*] for evidence that the mechanisms and configurations identified in PS-3.1.3.1 are being applied to identify personnel requiring re-screening in accordance with the conditions and frequency identified in PS-3.1.2.1. |
| **PS-3.1.3.5** | | **Examine** personnel re-screening records for an agreed-upon [*basic*] sample of personnel identified in PS-3.1.3.4; [*reviewing*] for evidence that individuals are re-screened in accordance with the conditions and frequency identified in PS-3.1.2.1. |
| **PS-3.1.3.6** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with personnel security responsibilities; conducting [*basic*] discussions for further evidence that individuals are re-screened in accordance with the conditions and frequency identified in PS-3.1.2.1. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **PS-3(1)** | PERSONNEL SCREENING |
| **PS-3(1).1**  **PS-3(1).1.1**  **PS-3(1).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization ensures that every user accessing an information system processing, storing, or transmitting classified information is cleared to the highest classification level of the information on the system; and* 2. *the organization ensures that every user accessing an information system processing, storing, or transmitting classified information is indoctrinated to the highest classification level of the information on the system.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Personnel security policy; procedures addressing personnel screening; records of screened personnel; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with personnel security responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PS-2  concurrent controls: AC-2, AC-3, MA-2, MA-3, MA-5, PE-2, PE-3, PL-4, PS-6, PS-7, SA-9  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **PS-3(1).1.1.1** | **Examine** personnel security policy, access control policy, physical and environmental protection policy, procedures addressing personnel screening, procedures addressing account management, procedures addressing physical access authorizations, security plan, or other relevant documents; [*reviewing*] for the highest level of classified information that the information system processes, stores, or transmits. |
| **PS-3(1).1.1.2** | **Examine** personnel security policy, access control policy, physical and environmental protection policy, procedures addressing personnel screening, procedures addressing account management, procedures addressing physical access authorizations, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to ensure that every user accessing the information system processing, storing, or transmitting classified information is cleared to the highest classification level as identified in PS-3(1).1.1.1. |
| **PS-3(1).1.1.3** | **Examine** security clearances (or personnel screening records as appropriate), account management records, and access authorizations for anagreed-upon [*basic*] sample of individuals with access to the information system; [*reviewing*] for evidence that the measures identified in PS-3(1).1.1.2 are being applied. |
| **PS-3(1).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with personnel security responsibilities, organizational personnel with account management responsibilities, and/or organizational personnel with physical access control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in PS-3(1).1.1.2 are being applied. |
|  |  |
| **PS-3(1).1.2.1** | **Examine** personnel security policy, access control policy, physical and environmental protection policy, procedures addressing personnel screening, procedures addressing account management, procedures addressing physical access authorizations, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to ensure that every user accessing the information system processing, storing, or transmitting classified information is indoctrinated to the highest classification level as identified in PS-3(1).1.1.1. |
| **PS-3(1).1.2.2** | **Examine** account management records, classified information nondisclosure agreements, and security indoctrination briefings (with signed acknowledgement forms) for the individuals identified in PS-3(1).1.1.3; [*reviewing*] for evidence that the measures identified in PS-3(1).1.2.1 are being applied.  Note to assessor: Physical or electronic signatures are acceptable as defined in organization policy or procedures. |
| **PS-3(1).1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with personnel security responsibilities, organizational personnel with account management responsibilities, and/or organizational personnel with physical access control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in PS-3(1).1.2.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **PS-3(2)** | PERSONNEL SCREENING |
| **PS-3(2).1**  **PS-3(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization formally indoctrinates every user accessing an information system that processes, stores, or transmits types of classified information requiring formal indoctrination for all of the relevant types of information on the system.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Personnel security policy; procedures addressing personnel screening; records of screened personnel; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with personnel security responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: PS-2  concurrent controls: AC-2, AC-3, MA-2, MA-3, MA-5, PE-2, PE-3, PL-4, PS-6, PS-7, SA-9  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **PS-3(2).1.1.1** | **Examine** personnel security policy, access control policy, physical and environmental protection policy, procedures addressing personnel screening, procedures addressing account management, procedures addressing physical access authorizations, security plan, or other relevant documents; [*reviewing*] for all relevant types of classified information requiring formal indoctrination of every user accessing the information system that processes, stores, or transmits such types of classified information. |
| **PS-3(2).1.1.2** | **Examine** personnel security policy, access control policy, physical and environmental protection policy, procedures addressing personnel screening, procedures addressing account management, procedures addressing physical access authorizations, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to formally indoctrinate every user accessing the information system that processes, stores, or transmits the types of classified information identified in PS-3(2).1.1.1. |
| **PS-3(2).1.1.3** | **Examine** account management records, classified information nondisclosure agreements, and security indoctrination briefings (with signed acknowledgement forms) for the individuals identified in PS-3(1).1.1.3; [*reviewing*] for evidence that the measures identified in PS-3(2).1.1.2 are being applied.  Note to assessor: Physical or electronic signatures are acceptable as defined in organization policy or procedures. |
| **PS-3(2).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with personnel security responsibilities, organizational personnel with account management responsibilities, and/or organizational personnel with physical access control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in PS-3(2).1.1.2 are being applied. |