| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 2 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **PE-3** | PHYSICAL ACCESS CONTROL | |
| **PE-3.1**  **PE-3.1.1**  **PE-3.1.2**  **PE-3.1.3**  **PE-3.1.4**  **PE-3.1.5** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);* 2. *the organization verifies individual access authorizations before granting access to the facility;* 3. *the organization controls entry to the facility containing the information system using physical access devices (e.g., keys, locks, combinations, card readers) and/or guards;* 4. *the organization controls access to areas officially designated as publicly accessible in accordance with the organization’s assessment of risk; and* 5. *the organization secures keys, combinations, and other physical access devices.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; information system entry and exit points; storage locations for physical access devices; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with physical access control responsibilities].  **Test**: [*select from:* Physical access control capability; physical access control devices]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-5, MA-2, MA-3, MA-4, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-6,  PE-7, PE-8, PE-10, PE-16, PE-18, PS-4, PS-5  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. |
| **PE-3.1.1.1** | | **Examine** physical and environmental protection policy, procedures addressing physical access control, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to enforce physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding the publicly accessible areas identified in PE-2.1.1.1). |
| **PE-3.1.1.2** | | **Examine** an agreed-upon [*basic*] sample of physical access points to the facility where the information system resides; [*observing*] for evidence that the measures identified in PE-3.1.1.1 are being applied. |
| **PE-3.1.1.3** | | **Examine** an agreed-upon [*basic*] sample of physical access control logs for the facility where the information system resides; [*reviewing*] for evidence that the measures identified in PE-3.1.1.1 are being applied. |
| **PE-3.1.1.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with physical access control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in PE-3.1.1.1 are being applied. |
|  | |  |
| **PE-3.1.2.1** | | **Examine** physical and environmental protection policy, procedures addressing physical access control, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to verify individual access authorizations before granting access to the facility. |
| **PE-3.1.2.2** | | **Examine** an agreed-upon [*basic*] sample of physical access control logs for the facility where the information system resides; [*reviewing*] for evidence that the measures identified in PE-3.1.2.1 are being applied. |
| **PE-3.1.2.3** | | **Examine** an agreed-upon [*basic*] sample of physical access points to the facility where the information system resides; [*observing*] for evidence that the measures identified in PE-3.1.2.1 are being applied. |
| **PE-3.1.2.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with physical access control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in PE-3.1.2.1 are being applied. |
|  | |  |
| **PE-3.1.3.1** | | **Examine** physical and environmental protection policy, procedures addressing physical access control, security plan, or other relevant documents; [*reviewing*] for the physical access security measures to be used to control entry to facilities containing the information system and that these measures include physical access devices (e.g., keys, locks, card readers) and/or guards. |
| **PE-3.1.3.2** | | **Examine** an agreed-upon [*basic*] sample of physical access control logs generated using the physical access security measures identified in PE-3.1.3.1; [*reviewing*] for evidence that the measures identified in PE-3.1.3.1 are being applied. |
| **PE-3.1.3.3** | | **Examine** an agreed-upon [*basic*] sample of physical access points to the facility where the information system resides; [*observing*] for evidence that the measures identified in PE-3.1.3.1 are being applied. |
| **PE-3.1.3.4** | | **Test** an agreed-upon [*basic*] sample of the physical access security measures identified in PE-3.1.3.1; conducting [*basic*] testing using simulated events or conditions for further evidence that these measures are operating as intended. |
|  | |  |
| **PE-3.1.4.1** | | **Examine** physical and environmental protection policy, procedures addressing physical access control, organizational risk assessment, security plan, or other relevant documents; [*reviewing*] for the areas within the facility that are officially designated as publicly accessible as identified in PE-2.1.1.1 and for the measures to be employed, if any, to control access to those areas.  Note to assessor: If the result of this assessor action is that either (1) no areas are designated as publicly accessible or (2) no physical access control measures for publicly accessible spaces are identified, there is no need to perform assessor actions PE-3.1.4.2 through PE-3.1.4.4. |
| **PE-3.1.4.2** | | **Examine** an agreed-upon [*basic*] sample of physical access control logs generated for an agreed-upon [*basic*] sample of areas identified in PE-3.1.4.1; [*reviewing*] for evidence that the measures identified in PE-3.1.4.1 are being applied. |
| **PE-3.1.4.3** | | **Examine** an agreed-upon [*basic*] sample of areas identified in PE-3.1.4.1; [*observing*] for evidence that the measures identified in PE-3.1.4.1 are being applied. |
| **PE-3.1.4.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with physical access control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in PE-3.1.4.1 are being applied. |
|  | |  |
| **PE-3.1.5.1** | | **Examine** physical and environmental protection policy, procedures addressing physical access control, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to secure keys, combinations, or other physical access devices. |
| **PE-3.1.5.2** | | **Examine** an agreed-upon [*basic*] sample of storage locations for physical access devices; [*observing*] for evidence that the measures identified in PE-3.1.5.1 are being applied. |
| ASSESSMENT – Base Control, Part 2 of 2 | | |
| **PE-3.2**  **PE-3.2.1**  **PE-3.2.2**  **PE-3.2.3**  **PE-3.2.4** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the frequency for conducting inventories of physical access devices;* 2. *the organization inventories physical access devices in accordance with the organization-defined frequency;* 3. *the organization defines the frequency of changes to combinations and keys; and* 4. *the organization changes combinations and keys in accordance with the organization-defined frequency, and when keys are lost, combinations are compromised, or individuals are transferred or terminated.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Physical and environmental protection policy; procedures addressing physical access control; security plan; physical access control logs or records; inventory records of physical access devices; records of key and lock combination changes; storage locations for physical access devices; other relevant documents or records].  **Test**: [*select from:* Physical access control devices]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: PE-2  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\*\*** |
| **PE-3.2.1.1** | | **Examine** physical and environmental protection policy, procedures addressing physical access control, security plan, or other relevant documents; [*reviewing*] for the frequency for conducting inventories of physical access devices. |
|  | |  |
| **PE-3.2.2.1** | | **Examine** physical and environmental protection policy, procedures addressing physical access control, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to inventory physical access devices in accordance with the frequency identified in PE-3.2.1.1. |
| **PE-3.2.2.2** | | **Examine** an agreed-upon [*basic*] sample ofinventory records of physical access devices; [*reviewing*] for evidence that the measures identified in PE-3.2.2.1 are being applied. |
| **PE-3.2.2.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with physical access control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in PE-3.2.2.1 are being applied. |
|  | |  |
| **PE-3.2.3.1** | | **Examine** physical and environmental protection policy, procedures addressing physical access control, security plan, or other relevant documents; [*reviewing*] for the frequency for changing combinations and keys. |
|  | |  |
| **PE-3.2.4.1** | | **Examine** physical and environmental protection policy, procedures addressing physical access control, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to change combinations and keys in accordance with the frequency identified in PE-3.2.3.1, and when keys are lost, combinations are compromised, or individuals are transferred or terminated. |
| **PE-3.2.4.2** | | **Examine** an agreed-upon [*basic*] sample ofrecords of key and lock combination changes; [*reviewing*] for evidence that the measures identified in PE-3.2.4.1 are being applied. |
| **PE-3.2.4.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with physical access control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in PE-3.2.4.1 are being applied. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **PE-3(1)** | | PHYSICAL ACCESS CONTROL |
| **PE-3(1).1**  **PE-3(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; information system entry and exit points; list of areas within the facility containing high concentrations of information system components or information system components requiring additional physical protection; other relevant documents or records]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-5, MA-2, MA-4, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-6, PE-7,  PE-8, PE-10, PE-16, PE-18, PS-4, PS-5  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **PE-3(1).1.1.1** | | **Examine** physical and environmental protection policy, procedures addressing physical access control, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to enforce physical access authorizations to the information system independent of the physical access control for the facility. |
| **PE-3(1).1.1.2** | | **Examine** an agreed-upon [*basic*] sample of areas within the facility containing high concentrations of information system components or information system components requiring additional physical protection; [*observing*] for evidence that the measures identified in PE-3(1).1.1.1 are being applied. |
| **PE-3(1).1.1.3** | | **Examine** an agreed-upon [*basic*] sample of physical access control logs for areas within the facility containing high concentrations of information system components or information system components requiring additional physical protection; [*reviewing*] for evidence that the measures identified in PE-3(1).1.1.1 are being applied. |
| **PE-3(1).1.1.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with physical access control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in PE-3(1).1.1.1 are being applied. |
|  | | |
| **ASSESSMENT – Control Enhancement 2** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **PE-3(2)** | | PHYSICAL ACCESS CONTROL |
| **PE-3(2).1**  **PE-3(2).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; records of security checks; facility layout documentation; information system entry and exit points; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with physical access control responsibilities]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: MA-2, MA-4, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-6, PE-7, PE-8,  PE-10, PE-16, PE-18, PS-4, PS-5  successor controls: None |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **PE-3(2).1.1.1** | | **Examine** physical and environmental protection policy, procedures addressing physical access control, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to perform security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components. |
| **PE-3(2).1.1.2** | | **Examine** an agreed-upon [*basic*] sample of security check records; [*reviewing*] for evidence that the measures identified in PE-3(2).1.1.1 are being applied. |
| **PE-3(2).1.1.3** | | **Examine** an agreed-upon [*basic*] sample of physical boundary locations of the facility or information system; [*observing*] for evidence that the measures identified in PE-3(2).1.1.1 are being applied. |
| **PE-3(2).1.1.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with physical access control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in PE-3(2).1.1.1 are being applied. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **PE-3(3)** | PHYSICAL ACCESS CONTROL |
| **PE-3(3).1**  **PE-3(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; facility surveillance records; facility layout documentation; information system entry and exit points; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with physical access control responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: MP-2, MP-4, PE-2, PE-6, PE-7, PE-8, PE-16, PE-18  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **PE-3(3).1.1.1** | **Examine** physical and environmental protection policy, procedures addressing physical access control, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to guard, alarm, and monitor every physical access point to the facility where the information system resides 24 hours a day, 7 days per week. |
| **PE-3(3).1.1.2** | **Examine** an agreed-upon [*basic*] sample of physical access points to the facility where the information system resides; [*observing*] for evidence that the measures identified in PE-3(3).1.1.1 are being applied. |
| **PE-3(3).1.1.3** | **Examine** an agreed-upon [*basic*] sample of physical access control logs for the facility where the information system resides; [*reviewing*] for evidence that the measures identified in PE-3(3).1.1.1 are being applied. |
| **PE-3(3).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with physical access control responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in PE-3(3).1.1.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **PE-3(4)** | PHYSICAL ACCESS CONTROL |
| **PE-3(4).1**  **PE-3(4).1.1**  **PE-3(4).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines information system components to be protected from unauthorized physical access using lockable physical casings; and* 2. *the organization uses lockable physical casings to protect organization-defined information system components from unauthorized physical access.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Physical and environmental protection policy; procedures addressing physical access control; security plan; list of information system components requiring protection through lockable physical casings; lockable physical casings; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: MP-2, MP-4, PE-2, PE-4, PE-5, PE-6, PE-8, PE-10, PE-16, PE-18  successor controls: None |
| **PE-3(4).1.1.1** | **Examine** physical and environmental protection policy, procedures addressing physical access control, security plan, or other relevant documents; [*reviewing*] for the information system components to be protected from unauthorized physical access using lockable physical casings. |
|  |  |
| **PE-3(4).1.2.1** | **Examine** an agreed-upon [*basic*] sample of information system components identified in PE-3(4).1.1.1; [*observing*] for evidence that these components are protected using lockable physical casings. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **PE-3(5)** | PHYSICAL ACCESS CONTROL |
| **PE-3(5).1**  **PE-3(5).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system detects/prevents physical tampering or alteration of hardware components within the system.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; information system design documentation; other relevant documents or records].  **Test**: [*select from:* Physical access control capability]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-5, CM-6, PE-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **PE-3(5).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and associated configuration settings to be employed to detect/prevent physical tampering or alteration of hardware components within the system. |
| **PE-3(5).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in PE-3(5).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in PE-3(5).1.1.1. |
| **PE-3(5).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and associated configuration settings identified in PE-3(5).1.1.1; 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)** | |
| **PE-3(6)** | PHYSICAL ACCESS CONTROL |
| **PE-3(6).1**  **PE-3(6).1.1**  **PE-3(6).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the frequency of unannounced attempts to be included in a penetration testing process to bypass or circumvent security controls associated with physical access points to the facility; and* 2. *the organization employs a penetration testing process that includes unannounced attempts, in accordance with the organization-defined frequency, to bypass or circumvent security controls associated with physical access points to the facility.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Physical and environmental protection policy; procedures addressing physical access control; procedures addressing penetration testing; rules of engagement and associated documentation; penetration test results; security plan; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CA-2,CA-7, RA-5  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **PE-3(6).1.1.1** | **Examine** physical and environmental protection policy, procedures addressing physical access control, procedures addressing penetration testing, security plan, or other relevant documents; [*reviewing*] for the frequency of unannounced attempts to be included in the penetration testing process to bypass or circumvent security controls associated with physical access points to the facility. |
|  |  |
| **PE-3(6).1.2.1** | **Examine** physical and environmental protection policy, procedures addressing physical access control, procedures addressing penetration testing, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to implement a penetration testing process that includes unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility, in accordance with the frequency identified in PE-3(6).1.1.1. |
| **PE-3(6).1.2.2** | **Examine** an agreed-upon [*basic*] sample of penetration test results; [*reviewing*] for evidence that the measures identified in PE-6(1).1.2.1 are being applied. |