| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **MP-4** | MEDIA STORAGE | |
| **MP-4.1**  **MP-4.1.1**  **MP-4.1.1a**  **MP-4.1.1b**  **MP-4.1.1c**  **MP-4.1.2**  **MP-4.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines:*    * *types of digital and non-digital media physically controlled and securely stored within designated controlled areas;*    * *controlled areas designated to physically control and securely store the media;*    * *security measures to physically control and securely store the media within designated controlled areas;* 2. *the organization physically controls and securely stores organization-defined information system media within organization-defined controlled areas using organization-defined security measures; and* 3. *the organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; security plan; information system media; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system media protection and storage responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: MP-2, RA-2, RA-3  concurrent controls: AC-3, AC-19, CP-6, CP-9, MP-5, PE-2, PE-3, PE-18, SC-28, SC-34,  SI-12  successor controls: MP-6 |
| **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. |
| **MP-4.1.1.1**  **MP-4.1.1.1.a**  **MP-4.1.1.1.b**  **MP-4.1.1.1.c** | | **Examine** information system media protection policy, physical and environmental protection policy, procedures addressing media storage protections, procedures addressing physical access control, security plan, or other relevant documents; [*reviewing*] for the:   * digital and non-digital media containing information to be physically controlled and securely stored within designated controlled areas; * controlled areas designated to physically control and securely store the media identified in MP-4.1.1.1a; and * security measures to be employed to physically control and securely store the media identified in MP-4.1.1.1.a within the designated controlled areas identified in MP-4.1.1.1b. |
|  | |  |
| **MP-4.1.2.1** | | **Examine** the security measures employed to physically control and securely store an agreed-upon [*basic*]sample of the information system media identified in MP-4.1.1.1.a within the designated controlled areas identified in MP-4.1.1.1.b; [*observing*] for evidence that the measures identified in MP-4.1.1.1.c are being applied. |
| **MP-4.1.2.2** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system media protection and storage responsibilities for the information system media identified in MP-4.1.1.1.a; conducting [*basic*] discussions for further evidence that the measures identified in MP-4.1.1.1.c are being applied to physically control and securely store the media identified in MP-4.1.1.1.a within the designated controlled areas identified in MP-4.1.1.1.b. |
|  | |  |
| **MP-4.1.3.1** | | **Examine** information system media protection policy, physical and environmental protection policy, procedures addressing media sanitization and disposal, security plan, or other relevant documents; [*reviewing*] for the equipment, techniques, and procedures to be employed to destroy or sanitize information system media. |
| **MP-4.1.3.2** | | **Examine** information system media protection policy, physical and environmental protection policy, procedures addressing media storage protections, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to protect information system media until the media are destroyed or sanitized using the equipment, techniques, and procedures identified in MP-4.1.3.1. |
| **MP-4.1.3.3** | | **Examine** the measures employed to protect information system media until the media are to be destroyed or sanitized using the equipment, techniques, and procedures identified in MP-4.1.3.1; [*observing*] for evidence that the measures identified in MP-4.1.3.2 are being applied. |
| **MP-4.1.3.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system media protection and storage responsibilities; conducting [*basic*] discussions for further evidence that measures identified in MP-4.1.3.2 are being applied. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **MP-4(1)** | MEDIA STORAGE |
| **MP-4(1).1**  **MP-4(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs cryptographic mechanisms to protect information in storage.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control devices; access control records; audit records; other relevant documents or records].  **Test**: [*select from:* Cryptographic mechanisms protecting information in storage]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: MP-2, RA-3  concurrent controls: AC-3, CM-6, CP-6, CP-9, SC-12, SC-13, SC-28, SC-34  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **MP-4(1).1.1.1** | **Examine** information system media protection policy, procedures addressing media storage protections, security plan, or other relevant documents; [*reviewing*] for the types of information in storage identified by the organization as requiring the use of approved cryptographic mechanisms for protection.  Note to assessor: Examples of information in storage include user information, authenticator content, and configurations for routers, firewalls, gateways, and intrusion detection systems. |
| **MP-4(1).1.1.2** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the cryptographic mechanisms and their configuration settings to be employed to protect the types of information in storage identified in MP-4(1).1.1.1. |
| **MP-4(1).1.1.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the cryptographic mechanisms identified in MP-4(1).1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in MP-4(1).1.1.2. |
| **MP-4(1).1.1.4** | **Test** an agreed-upon [*basic*] sample of the cryptographic mechanisms and their configuration settings identified in MP-4(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |