| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SC-28** | PROTECTION OF INFORMATION AT REST | |
| **SC-28.1**  **SC-28.1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system* *protects the confidentiality and integrity of information at rest.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing protection of information at rest; information system design documentation; information system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; list of information at rest requiring confidentiality and integrity protections; other relevant documents or records].  **Test**: [*select from:* Automated mechanisms implementing confidentiality and integrity protections for information at-rest]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-3, AC-4, CM-6, CP-9, IA-2, MP-2, MP-4, PE-3, SC-7, SC-13, SI-7  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. |
| **SC-28.1.1.1** | | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to protect the confidentiality and integrity of information at rest. |
| **SC-28.1.1.2** | | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the automated mechanisms identified in SC-28.1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-28.1.1.1. |
| **SC-28.1.1.3** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-28.1.1.1; 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)** | |
| **SC-28(1)** | PROTECTION OF INFORMATION AT REST |
| **SC-28(1).1**  **SC-28(1).1.1**  **SC-28(1).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information at rest unless otherwise protected by alternative physical measures; and* 2. *the organization employs cryptographic mechanisms to prevent unauthorized modification of information at rest unless otherwise protected by alternative physical measures.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing protection of information at rest; information system design documentation; information system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; other relevant documents or records].  **Test**: [*select from:* Cryptographic mechanisms implementing confidentiality and integrity protections for information at-rest]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, MP-2, MP-4, PE-3, SC-13, SI-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-28(1).1.1.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the cryptographic mechanisms and their configuration settings to be employed to prevent unauthorized disclosure of information at rest unless otherwise protected by alternative physical measures. |
| **SC-28(1).1.1.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the cryptographic mechanisms identified in SC-28(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-28(1).1.1.1. |
| **SC-28(1).1.1.3** | **Test** an agreed-upon [*basic*]sample of the cryptographic mechanisms and their configuration settings identified in SC-28(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **SC-28(1).1.2.1** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the cryptographic mechanisms and their configuration settings to be employed to prevent unauthorized modification of information at rest unless otherwise protected by alternative physical measures. |
| **SC-28(1).1.2.2** | **Examine** documentation describing the current configuration settings for anagreed-upon [*basic*] sample of the cryptographic mechanisms identified in SC-28(1).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-28(1).1.2.1. |
| **SC-28(1).1.2.3** | **Test** an agreed-upon [*basic*]sample of the cryptographic mechanisms and their configuration settings identified in SC-28(1).1.2.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |