| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SC-34** | NON-MODIFIABLE EXECUTABLE PROGRAMS | |
| **SC-34.1**  **SC-34.1.1**  **SC-34.1.2**  **SC-34.1.3**  **SC-34.1.3a**  **SC-34.1.3b** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the applications that are to be loaded and executed from hardware-enforced, read-only media;* 2. *the organization defines the information system components for which the operating environment and organization-defined applications are loaded and executed from hardware-enforced, read-only media; and* 3. *the* *information system, at organization-defined information system components, loads and executes:*    * *the operating environment from hardware-enforced, read-only media; and*    * *organization-defined applications from hardware-enforced, read-only media.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; information system design documentation; information system configuration settings and associated documentation; information system architecture; list of operating system components to be loaded from hardware-enforced, read-only media; list of applications to be loaded from hardware-enforced, read-only media; media used to load and execute information system operating environment; media used to load and execute information system applications; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel installing, configuring, and/or maintaining the information system]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-19, CM-6, MP-2, MP-4  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-34.1.1.1** | | **Examine** system and communications protection policy, security plan, or other relevant documents; [*reviewing*] for the applications that are to be loaded and executed from hardware-enforced, read-only media. |
|  | |  |
| **SC-34.1.2.1** | | **Examine** system and communications protection policy, security plan, or other relevant documents; [*reviewing*] for the information system components for which the operating environment and the applications identified in SC-34.1.2.1 are loaded and executed from hardware-enforced, read-only media. |
|  | |  |
| **SC-34.1.3.1**  **SC-34.1.3.1.a**  **SC-34.1.3.1.b** | | E**xamine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to load and execute, at information system components identified in SC-34.1.2.1:   * + the operating environment from hardware-enforced, read-only media; and   + applications identified in SC-34.1.1.1 from hardware-enforced, read-only media. |
| **SC-34.1.3.2** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in SC-34.1.3.1.a; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-34.1.3.1.a to load and execute the operating environment from hardware-enforced, read-only media. |
| **SC-34.1.3.3** | | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in SC-34.1.3.1.b; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-34.1.3.1.b to load and execute the applications identified in SC-34.1.1.1. |
| **SC-34.1.3.4** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-34.1.3.1.a; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in SC-34.1.3.1.a to load and execute the operating environment from hardware-enforced, read-only media. |
| **SC-34.1.3.5** | | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-34.1.3.1.b; conducting [*basic*] testing for evidence that these mechanisms are operating as intended in SC-34.1.3.1.b to load and execute the applications identified in SC-34.1.1.1. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-34(1)** | NON-MODIFIABLE EXECUTABLE PROGRAMS |
| **SC-34(1).1**  **SC-34(1).1.1**  **SC-34(1).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the information system components to be employed with no writeable storage; and* 2. *the organization employs organization-defined information system components with no writeable storage that are persistent across component restart or power on/off.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; information system design documentation; information system configuration settings and associated documentation; information system architecture; list of information system components to be employed without writeable storage capability; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-19  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-34(1).1.1.1** | **Examine** system and communications protection policy, security plan, or other relevant documents; [*reviewing*] for the types information system components to be employed with no writeable storage. |
|  |  |
| **SC-34(1).1.2.1** | **Examine** inventory of information system components; [*reviewing*] for evidence that the information system components identified in SC-34(1).1.1.1 are employed with no writeable storage that are persistent across component restart or power on/off. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-34(2)** | NON-MODIFIABLE EXECUTABLE PROGRAMS |
| **SC-34(2).1**  **SC-34(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization protects the integrity of the information on read-only media.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing protection of information on read-only media; information system design documentation; information system configuration settings and associated documentation; information system architecture; other relevant documents or records].  **Test**: [*select from:* Organizational capability for protecting information integrity on read-only media]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-19, CM-6, SC-28, SI-7  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-34(2).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 integrity of the information on read-only media. |
| **SC-34(2).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*]sample of the automated mechanisms identified in SC-34(2).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in SC-34(2).1.1.1 to protect the integrity of the information on read-only media. |
| **SC-34(2).1.1.3** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in SC-34(2).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended to protect the integrity of the information on read-only media. |