| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SC-31** | COVERT CHANNEL ANALYSIS | |
| **SC-31.1**  **SC-31.1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization requires that information system developers/integrators perform a covert channel analysis to identify those aspects of system communication that are potential avenues for covert storage and timing channels.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing covert channel analysis; information system design documentation; information system configuration settings and associated documentation; covert channel analysis documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with covert channel analysis responsibilities; information system developers/integrators]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, SA-10, SA-11  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-31.1.1.1** | | **Examine** system and communications protection policy, procedures addressing covert channel analysis, security plan, or other relevant documents; [*reviewing*] for the requirement that information system developers/integrators perform a covert channel analysis to identify those aspects of system communication that are potential avenues for covert storage and timing channels. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SC-31(1)** | COVERT CHANNEL ANALYSIS |
| **SC-31(1).1**  **SC-31(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization tests a subset of the vendor-identified covert channel avenues to determine if such channels are exploitable.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and communications protection policy; procedures addressing covert channel analysis; information system design documentation; information system configuration settings and associated documentation; list of vendor-identified covert channel avenues or exploits; covert channel analysis documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with covert channel analysis responsibilities; information system developers/integrators].  **Test**: [*select from:* Covert channel avenues to determine if such channels are exploitable]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-4, CA-2, RA-5  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SC-31(1).1.1.1** | **Examine** system and communications protection policy, procedures addressing covert channel analysis, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to test a subset of the vendor-identified covert channel avenues to determine if channels are exploitable. |
| **SC-31(1).1.1.2** | **Examine** organizational test records for an agreed-upon [*basic*] sample of vendor-identified covert channel avenues; [*reviewing*] for evidence that the measures identified in SC-31(1).1.1.1 are being applied. |
| **SC-31(1).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with covert channel testing and analysis responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in SC-31(1).1.1.1 are being applied. |