| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **SA-5** | INFORMATION SYSTEM DOCUMENTATION | |
| **SA-5.1**  **SA-5.1.1**  **SA-5.1.1a**  **SA-5.1.1b**  **SA-5.1.1c**  **SA-5.1.2**  **SA-5.1.2a**  **SA-5.1.2b**  **SA-5.1.2c**  **SA-5.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:*    * *secure configuration, installation, and operation of the information system;*    * *effective use and maintenance of the security features/functions; and*    * *known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;* 2. *the organization obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:*    * *user-accessible security features/functions and how to effectively use those security features/functions;*    * *methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and*    * *user responsibilities in maintaining the security of the information and information system; and* 3. *the organization documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing information system documentation; information system documentation including administrator and user guides; records documenting attempts to obtain unavailable or nonexistent information system documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9, SA-2, PM-3, PM-7, SA-4, SA-8, SA-13, SC-2, SC-3  concurrent controls: CM-2, CM-6  successor controls: SA-6, SA-7, SA-9, SA-10, SA-11 |

|  |  |
| --- | --- |
| **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. |
| **SA-5.1.1.1**  **SA-5.1.1.1.a**  **SA-5.1.1.1.b**  **SA-5.1.1.1.c** | **Examine** system and services acquisition policy, procedures addressing information system documentation, solicitation documentation, acquisition documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to obtain administrator documentation for the information system that describes:   * secure configuration, installation, and operation of the information system; * effective use and maintenance of the security features/functions; and * known vulnerabilities regarding configuration and use of administrative functions. |
| **SA-5.1.1.2** | **Examine** an agreed-upon [*basic*] sample of administrator documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5.1.1.1.a are being applied to obtain administrator documentation for the information system that describes secure configuration, installation, and operation of the information system. |
| **SA-5.1.1.3** | **Examine** an agreed-upon [*basic*] sample of administrator documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5.1.1.1.b are being applied to obtain administrator documentation for the information system that describes effective use and maintenance of the security features/functions. |
| **SA-5.1.1.4** | **Examine** an agreed-upon [*basic*] sample of administrator documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5.1.1.1.c are being applied to obtain administrator documentation for the information system that describes known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. |
| **SA-5.1.1.5** | **Examine** system and services acquisition policy, procedures addressing information system documentation, solicitation documentation, acquisition documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to protect administrator documentation for the information system. |
| **SA-5.1.1.6** | **Examine** the measures employed to protect administrator documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5.1.1.5 are being applied. |
| **SA-5.1.1.7** | **Examine** access control policy, physical access control policy, security planning policy, procedures addressing information system documentation, security plan, or other relevant documents; [*reviewing*] for the authorized personnel to whom administrator documentation for the information system is to be made available. |
| **SA-5.1.1.8** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for protecting administrator documentation for the information system; conducting [*basic*] discussions for further evidence that the measures identified in SA-5.1.1.5 are being applied to protect administrator documentation for the information system. |
| **SA-5.1.1.9** | **Interview** an agreed-upon [*basic*] sample of the authorized personnel identified in SA-5.1.1.7; conducting [*basic*] discussions for evidence that administrator documentation for the information system is made available to these individuals. |
|  |  |
| **SA-5.1.2.1**  **SA-5.1.2.1.a**  **SA-5.1.2.1.b**  **SA-5.1.2.1.c** | **Examine** system and services acquisition policy, procedures addressing information system documentation, solicitation documentation, acquisition documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to obtain user documentation for the information system that describes:   * user-accessible security features/functions and how to effectively use those security features/functions; * methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and * user responsibilities in maintaining the security of the information and information system. |
| **SA-5.1.2.2** | **Examine** an agreed-upon [*basic*] sample of user documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5.1.2.1.a are being applied to obtain user documentation for the information system that describes user-accessible security features/functions and how to effectively use those security features/functions. |
| **SA-5.1.2.3** | **Examine** an agreed-upon [*basic*] sample of user documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5.1.2.1.b are being applied to obtain user documentation for the information system that describes methods for user interaction with the information system, which enables individuals to use the system in a more secure manner. |
| **SA-5.1.2.4** | **Examine** an agreed-upon [*basic*] sample of user documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5.1.2.1.c are being applied to obtain user documentation for the information system that describes user responsibilities in maintaining the security of the information and information system. |
| **SA-5.1.2.5** | **Examine** system and services acquisition policy, procedures addressing information system documentation, solicitation documentation, acquisition documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to protection user documentation for the information system. |
| **SA-5.1.2.6** | **Examine** the measures employed to protect user documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5.1.2.5 are being applied. |
| **SA-5.1.2.7** | **Examine** access control policy, physical access control policy, security planning policy, procedures addressing information system documentation, security plan, or other relevant documents; [*reviewing*] for the authorized personnel to whom user documentation for the information system is to be made available. |
| **SA-5.1.2.8** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for protecting user documentation for the information system; conducting [*basic*] discussions for further evidence that the measures identified in SA-5.1.2.5 are being applied to protect user documentation for the information system. |
| **SA-5.1.2.9** | **Interview** an agreed-upon [*basic*] sample of the authorized personnel identified in SA-5.1.2.7; conducting [*basic*] discussions for evidence that user documentation for the information system is made available to these individuals. |
|  |  |
| **SA-5.1.3.1** | **Examine** system and services acquisition policy, procedures addressing information system documentation, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to document attempts to obtain information system documentation when such documentation is either unavailable or nonexistent. |
| **SA-5.1.3.2** | **Examine** an agreed-upon [*basic*] sample of records documenting attempts to obtain unavailable or nonexistent information system documentation; [*reviewing*] for evidence that the measures identified in SA-5.1.3.1 are being applied. |
| **SA-5.1.3.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with information system documentation responsibilities; conducting [*basic*] discussions for further evidence that the measures identified in SA-5.1.3.1 are being applied. |
|  | |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-5(1)** | INFORMATION SYSTEM DOCUMENTATION |
| **SA-5(1).1**  **SA-5(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9, SA-2, PM-3, PM-7, SA-4, SA-8, SA-13, SC-2, SC-3  concurrent controls: CM-2, CM-6  successor controls: SA-6, SA-7, SA-9, SA-10, SA-11 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-5(1).1.1.1** | **Examine** system and services acquisition policy, procedures addressing information system documentation, solicitation documentation, acquisition documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to obtain vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing. |
| **SA-5(1).1.1.2** | **Examine** an agreed-upon [*basic*] sample of vendor/manufacturer documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5(1).1.1.1 are being applied. |
| **SA-5(1).1.1.3** | **Examine** system and services acquisition policy, procedures addressing information system documentation, solicitation documentation, acquisition documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to protect vendor/manufacturer documentation for the information system. |
| **SA-5(1).1.1.4** | **Examine** the measures employed to protect vendor/manufacturer documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5(1).1.1.3 are being applied. |
| **SA-5(1).1.1.5** | **Examine** access control policy, physical access control policy, security planning policy, procedures addressing information system documentation, security plan, or other relevant documents; [*reviewing*] for the authorized personnel to whom vendor/manufacturer documentation for the information system is to be made available. |
| **SA-5(1).1.1.6** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for protecting vendor/manufacturer documentation for the information system; conducting [*basic*] discussions for further evidence that the measures identified in SA-5(1).1.1.3 are being applied. |
| **SA-5(1).1.1.7** | **Interview** an agreed-upon [*basic*] sample of the authorized personnel identified in SA-5(1).1.1.5; conducting [*basic*] discussions for evidence that vendor/manufacturer documentation for the information system is made available to these individuals. |
|  | |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-5(2)** | INFORMATION SYSTEM DOCUMENTATION |
| **SA-5(2).1**  **SA-5(2).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system security documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9, SA-2, PM-3, PM-7, SA-4, SA-8, SA-13, SC-2, SC-3  concurrent controls: CM-2, CM-6  successor controls: SA-6, SA-7, SA-9, SA-10, SA-11 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-5(2).1.1.1** | **Examine** system and services acquisition policy, procedures addressing information system documentation, solicitation documentation, acquisition documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to obtain vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing. |
| **SA-5(2).1.1.2** | **Examine** an agreed-upon [*basic*] sample of vendor/manufacturer documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5(2).1.1.1 are being applied. |
| **SA-5(2).1.1.3** | **Examine** system and services acquisition policy, procedures addressing information system documentation, solicitation documentation, acquisition documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to protect vendor/manufacturer documentation for the information system. |
| **SA-5(2).1.1.4** | **Examine** the measures employed to protect vendor/manufacturer documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5(2).1.1.3 are being applied. |
| **SA-5(2).1.1.5** | **Examine** access control policy, physical access control policy, security planning policy, procedures addressing information system documentation, security plan, or other relevant documents; [*reviewing*] for the authorized personnel to whom vendor/manufacturer documentation for the information system is to be made available. |
| **SA-5(2).1.1.6** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for protecting vendor/manufacturer documentation for the information system; conducting [*basic*] discussions for further evidence that the measures identified in SA-5(2).1.1.3 are being applied to protect vendor/manufacturer documentation for the information system. |
| **SA-5(2).1.1.7** | **Interview** an agreed-upon [*basic*] sample of the authorized personnel identified in SA-5(2).1.1.5; conducting [*basic*] discussions for evidence that vendor/manufacturer documentation for the information system is made available to these individuals. |
|  | |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-5(3)** | INFORMATION SYSTEM DOCUMENTATION |
| **SA-5(3).1**  **SA-5(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9, SA-2, PM-3, PM-7, SA-4, SA-8, SA-13, SC-2, SC-3  concurrent controls: CM-2, CM-6  successor controls: SA-6, SA-7, SA-9, SA-10, SA-11 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-5(3).1.1.1** | **Examine** system and services acquisition policy, procedures addressing information system documentation, solicitation documentation, acquisition documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to obtain vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing. |
| **SA-5(3).1.1.2** | **Examine** an agreed-upon [*basic*] sample of vendor/manufacturer documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5(3).1.1.1 are being applied. |
| **SA-5(3).1.1.3** | **Examine** system and services acquisition policy, procedures addressing information system documentation, solicitation documentation, acquisition documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to protect vendor/manufacturer documentation for the information system. |
| **SA-5(3).1.1.4** | **Examine** the measures employed to protect vendor/manufacturer documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5(3).1.1.3 are being applied. |
| **SA-5(3).1.1.5** | **Examine** access control policy, physical access control policy, security planning policy, procedures addressing information system documentation, security plan, or other relevant documents; [*reviewing*] for the authorized personnel to whom vendor/manufacturer documentation for the information system is to be made available. |
| **SA-5(3).1.1.6** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for protecting vendor/manufacturer documentation for the information system; conducting [*basic*] discussions for further evidence that the measures identified in SA-5(3).1.1.3 are being applied |
| **SA-5(3).1.1.7** | **Interview** an agreed-upon [*basic*] sample of the authorized personnel identified in SA-5(3).1.1.5; conducting [*basic*] discussions for evidence that vendor/manufacturer documentation for the information system is made available to these individuals. |
|  | |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-5(4)** | INFORMATION SYSTEM DOCUMENTATION |
| **SA-5(4).1**  **SA-5(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the low-level design of the information system in terms of modules and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system security documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9, SA-2, PM-3, PM-7, SA-4, SA-8, SA-13, SC-2, SC-3  concurrent controls: CM-2, CM-6  successor controls: SA-6, SA-7, SA-9, SA-10, SA-11 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-5(4).1.1.1** | **Examine** system and services acquisition policy, procedures addressing information system documentation, solicitation documentation, acquisition documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to obtain vendor/manufacturer documentation that describes the low-level design of the information system in terms of modules and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing. |
| **SA-5(4).1.1.2** | **Examine** an agreed-upon [*basic*] sample of vendor/manufacturer documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5(4).1.1.1 are being applied. |
| **SA-5(4).1.1.3** | **Examine** system and services acquisition policy, procedures addressing information system documentation, solicitation documentation, acquisition documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to protect vendor/manufacturer documentation for the information system. |
| **SA-5(4).1.1.4** | **Examine** the measures employed to protect vendor/manufacturer documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5(4).1.1.3 are being applied. |
| **SA-5(4).1.1.5** | **Examine** access control policy, physical access control policy, security planning policy, procedures addressing information system documentation, security plan, or other relevant documents; [*reviewing*] for the authorized personnel to whom vendor/manufacturer documentation for the information system is to be made available. |
| **SA-5(4).1.1.6** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for protecting vendor/manufacturer documentation for the information system; conducting [*basic*] discussions for further evidence that the measures identified in SA-5(4).1.1.3 are being applied. |
| **SA-5(4).1.1.7** | **Interview** an agreed-upon [*basic*] sample of the authorized personnel identified in SA-5(4).1.1.5; conducting [*basic*] discussions for evidence that vendor/manufacturer documentation for the information system is made available to these individuals. |
|  | |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **SA-5(5)** | INFORMATION SYSTEM DOCUMENTATION |
| **SA-5(5).1**  **SA-5(5).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization obtains, protects as required, and makes available to authorized personnel, the source code for the information system to permit analysis and testing.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* System and services acquisition policy; procedures addressing information system documentation; information system design documentation; information system source code documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-9, SA-2, PM-3, PM-7, SA-4, SA-8, SA-13, SC-2, SC-3  concurrent controls: CM-2, CM-6  successor controls: SA-6, SA-7, SA-9, SA-10, SA-11 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **SA-5(5).1.1.1** | **Examine** system and services acquisition policy, procedures addressing information system documentation, solicitation documentation, acquisition documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to obtain the source code for the information system to permit analysis and testing. |
| **SA-5(5).1.1.2** | **Examine** an agreed-upon [*basic*] sample of source code documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5(5).1.1.1 are being applied. |
| **SA-5(5).1.1.3** | **Examine** system and services acquisition policy, procedures addressing information system documentation, solicitation documentation, acquisition documentation, acquisition contracts for information system services, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to protect source code documentation for the information system. |
| **SA-5(5).1.1.4** | **Examine** the measures employed to protect source code documentation for the information system; [*reviewing*] for evidence that the measures identified in SA-5(5).1.1.3 are being applied. |
| **SA-5(5).1.1.5** | **Examine** access control policy, physical access control policy, security planning policy, procedures addressing information system documentation, security plan, or other relevant documents; [*reviewing*] for the authorized personnel to whom source code documentation for the information system is to be made available. |
| **SA-5(5).1.1.6** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with responsibilities for protecting source code documentation for the information system; conducting [*basic*] discussions for further evidence that the measures identified in SA-5(5).1.1.3 are being applied. |
| **SA-5(5).1.1.7** | **Interview** an agreed-upon [*basic*] sample of the authorized personnel identified in SA-5(5).1.1.5; conducting [*basic*] discussions for evidence that source code documentation for the information system is made available to these individuals. |