| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 1 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AT-2** | SECURITY AWARENESS | |
| **AT-2.1**  **AT-2.1.1**  **AT-2.1.2**  **AT-2.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users and when required by system changes;* 2. *the organization defines the frequency of refresher security awareness training;* 3. *the organization provides refresher security awareness training in accordance with the organization-defined frequency;*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; security plan; training records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel comprising the general information system user community]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: None  successor controls: AT-4 |
| **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. |
| **AT-2.1.1.1** | | **Examine** security awareness and training policy, procedures addressing security awareness training implementation, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to provide basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users and when required by system changes. |
|  | |  |
| **AT-2.1.1.2** | | **Examine** training records for an agreed-upon [*basic*] sample of information system users; [*reviewing*] for evidence that the measures identified in AT-2.1.1.1 are being applied. |
|  | |  |
| **AT-2.1.2.1** | | **Examine** security awareness and training policy, security plan, or other relevant documents; [*reviewing*] for the frequency of refresher security awareness training. |
|  | |  |
| **AT-2.1.3.1** | | **Examine** training records for an agreed-upon [*basic*] sample of information system users; [*reviewing*] for evidence that refresher security awareness training is provided in accordance with the frequency identified in AT-2.1.2.1. |
|  | | |
| **ASSESSMENT – Control Enhancement 1** | | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | | |
| **AT-2(1)** | | SECURITY AWARENESS |
| **AT-2(1).1**  **AT-2(1).1.1** | | **ASSESSMENT OBJECTIVE:**  *Determine if the organization includes practical exercises in security awareness training that simulate actual cyber attacks.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Security awareness and training policy; procedures addressing security awareness training implementation; security awareness training curriculum; security awareness training materials; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel that participate in security awareness training]. |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: None  successor controls: AT-4 |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **AT-2(1).1.1.1** | | **Examine** security awareness and training policy, procedures addressing security awareness training implementation, security plan, or other relevant documents; [*reviewing*] for the practical exercises to be included in security awareness training that simulate actual cyber attacks. |
| **AT-2(1).1.1.2** | | **Examine** an agreed-upon [*basic*] sample of security awareness training materials associated with the security awareness training curriculum; [*reviewing*] for evidence that the exercises identified in AT-2(1).1.1.1 are being applied. |