**AWARENESS AND TRAINING (AT)**

**AT-1: Security Awareness and Training Policy and Procedures**

NIST SP 800-53 Objective: The organization develops, disseminates, and reviews/updates [*Assignment: organization defined frequency]:*

a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

Control Translation: Ensure security awareness and training policy and procedures are in place.

Notes: The organizational risk management strategy is a key factor in the development of the security awareness and training policy. Related control: PM-9. This control can be applied at the General level.

How to test and evaluate: Examine SSP and Security Awareness and Training Policy (if available). Verify that the policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance of organization/agency.

Technology specific: General, All

**AT-2: Security Awareness**

NIST SP 800-53 Objective: 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, when required by system changes, and [*Assignment: organization-defined frequency]* thereafter.

Control Translation: Ensure basic security awareness and training is available to all information system users.

Notes: The content for training should include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.

How to test and evaluate: Examine SSP and Security Awareness and Training Policy (if available). Verify that the security awareness policy and procedures include awareness techniques such as displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events. Examine samples of completed user training and verify that it is completed at least annually.

Technology specific: General, All

**AT-3: Security Training**

NIST SP 800-53 Objective: The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency] thereafter.*

Control Translation: Ensure security awareness and training is available to all information system users based on assigned roles and responsibilities.

Notes: The organization also provides the training necessary for these individuals to carry out their responsibilities related to operations security within the context of the organization’s information security program. Related controls: AT-2, SA-3.

How to test and evaluate: Examine SSP and Security Awareness and Training Policy (if available). Verify that the security awareness policy and procedures include awareness techniques such as displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

Technology specific: All

**AT-4: Security Training Records**

NIST SP 800-53 Objective: The organization:

a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and

b. Retains individual training records for [*Assignment: organization-defined time period].*

Control Translation: Ensure basic security awareness training and specific system security training activities for each information system user recorded and retained.

Notes: Evidence for AC-2 at the General level. AC-5/AC-6 can be applied to this at the General/Technical.

How to test and evaluate: Examine SSP and Security Awareness and Training Policy (if available). While an organization may deem that organizationally mandated individual training programs and the development of individual training plans are necessary, this control does not mandate either. Documentation for specialized training may be maintained by individual supervisors at the option of the organization.

Technology specific: All