NIST 800-171 r3

03.02 Awareness and Training

03.02.02 — Role-Based Training

Overview

This control ensures that organizations provide security training to personnel based on their roles and responsibilities. The training is tailored to the security requirements of the systems to which personnel have access and is updated regularly or when required by system changes.

Implementation Guidance

Identify the roles within your organization that require security training. Develop a training program tailored to each role, ensuring it covers the security requirements of the systems to which personnel have access. Schedule regular training sessions and updates, and additional sessions following certain events or system changes.

Suggested Evidence

- Training schedules and attendance records
- Training materials and content updates
- Documentation of system changes or events that triggered additional training

Assessment Guidance

Documentation to Review

- security awareness and training policy and procedures
- procedures for security training implementation
- codes of federal regulations
- security training curriculum
- security training materials
- training records
- system security plan
- other relevant documents or records

Personnel to Interview

- personnel with responsibilities for role-based security training
- personnel with assigned system security roles and responsibilities

Processes and Mechanisms to Test

- mechanisms for managing role-based security training and awareness

03.02.02 — Role-Based Training

Official Description:
Organizations determine the content and frequency of security training based on the assigned duties, roles, and responsibilities of individuals and the security requirements of the systems to which personnel have authorized access. In addition, organizations provide system developers, enterprise architects, security architects, software developers, systems integrators, acquisition/procurement officials, system and network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation, security assessors, and personnel with access to system-level software with security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities that cover physical, personnel, and technical controls. Such training can include policies, procedures, tools, and artifacts for the security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs.

SR-03.02.02

- ☐ SR-03.02.02.a – a: Provide role-based security training to organizational personnel:
  - ☐ SR-03.02.02.a.01 – 01: Before authorizing access to the system or CUI, before performing assigned duties, and [Assignment: organization-defined frequency] thereafter
  - ☐ SR-03.02.02.a.02 – 02: When required by system changes or following [Assignment: organization-defined events].
- ☐ SR-03.02.02.b – b: Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

DS-A.03.02.02.a.01[01]
role-based security training is provided to organizational personnel before authorizing access to the system or CUI.

DS-A.03.02.02.a.01[02]
role-based security training is provided to organizational personnel before performing assigned duties.

DS-A.03.02.02.a.01[03]
role-based security training is provided to organizational personnel *<A.03.02.02.ODP[01]: frequency>* after initial training.

- ➔ ***A.03.02.02.ODP[01]***
  the frequency at which to provide role-based security training to assigned personnel after initial training is defined.

DS-A.03.02.02.a.02
role-based security training is provided to organizational personnel when required by system changes or following *<A.03.02.02.ODP[02]: events>*.

- ➔ ***A.03.02.02.ODP[02]***
  events that require role-based security training are defined.

03.02.02 — Role-Based Training

DS-A.03.02.02.b[01]
role-based security training content is updated *<A.03.02.02.ODP[03]: frequency>.*

➔ ***A.03.02.02.ODP[03]***
the frequency at which to update role-based security training content is defined.

DS-A.03.02.02.b[02]
role-based security training content is updated following *<A.03.02.02.ODP[04]: events>*.

➔ ***A.03.02.02.ODP[04]***
events that require role-based security training content updates are defined.

Is role-based security training provided to organizational personnel before authorizing access to the system or CUI?

Is role-based security training provided to organizational personnel before performing assigned duties?

Is role-based security training provided to organizational personnel at a defined frequency after initial training?

- **What is the frequency at which to provide role-based security training to assigned personnel after initial training?**

★ **Required: at least every 12 months**

Is role-based security training provided to organizational personnel when required by system changes or following defined events?

- **What events require additional role-based security training?**

★ **Required: significant1, novel incidents, or significant1 changes to risks**

03.02.02 — Role-Based Training

Is role-based security training content updated at a defined frequency?

- **What is the frequency at which to update role-based security training content?**

★ **Required: at least every 12 months**

Is role-based security training content updated following defined events?

- **What events require updates to the role-based security training content?**

★ **Required: significant1, novel incidents, or significant1 changes to risks**

Evidence: