AT.L2-3.2.2

Awareness & Training

Role-Based Training

"Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities."

Objectives

[a]
Information security-related duties, roles, and responsibilities are defined.

[b]
Information security-related duties, roles, and responsibilities are assigned to designated personnel.

[c]
Personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.

Key Discussion Points

Define the Roles:
Security roles must be formally defined — sys admin, incident responder, data custodian, security officer — before training can be assigned.

Assign to People:
Each security role must be assigned to a named individual. Undefined or unassigned roles cannot be trained.

Different from 3.2.1:
Awareness (3.2.1) influences behavior broadly. Role-based training builds specific knowledge and skills for a defined job function.

Before Role Assumption:
Training should be completed before personnel assume their security-related duties — not after.

Assessment Methods

EXAMINE

Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; system security plan; training records.

INTERVIEW

Personnel with responsibilities for role-based security training; personnel with assigned system security roles and responsibilities; personnel with information security responsibilities; personnel representing the general system user community.

TEST

Mechanisms managing role-based security training; mechanisms managing security awareness training.

AT.L2-3.2.2

AWARENESS & TRAINING — Role-Based Training

Plain English

What this control is really saying:

General awareness tells everyone to be careful. Role-based training tells the IT admin exactly how to manage access controls, tells the incident responder what to do when an alarm fires, and tells the data steward how to handle and mark CUI. The roles are different — the training must be too.

How it is used:

- The IT admin completes role-specific training on secure configuration, patch management, and access control administration before assuming the role.
- The incident response lead is trained on the IR plan, escalation procedures, and DIBCAC reporting requirements specific to that role.
- When the company upgrades to a new firewall, the admin assigned to manage it receives targeted training on the new platform before taking it live.
- Role-based training records are maintained separately from general awareness records and tied to specific job functions.

Real World Example

The Scenario

Acme Defense has three staff with defined security roles in their SSP: IT administrator, data custodian, and incident response lead. The SSP was completed by an RP consultant six months ago. No training has been provided since roles were assigned.

What the assessor finds

The IT admin cannot describe the access control procedures documented in the SSP. The IR lead has never read the incident response plan. No role-based training records exist for any of the three assigned security roles.

SPRS Score Impact

3.2.2 carries a point value of 5. An SSP with roles defined but untrained personnel is a paper exercise — assessors will verify actual knowledge and capability, not just document existence.

What Good Looks Like

Security roles formally defined and documented in SSP, each role assigned to a named individual, role-specific training completed before duties assumed, training records maintained by role, refreshed when responsibilities change.

Common Gaps

What assessors actually find in the field:

✗ **No roles defined**

Security roles have never been formally defined — nobody knows what their specific security responsibilities are.

✗ **Roles defined but untrained**

The IT admin is listed as the system administrator in the SSP but has received no training specific to that security role.

✗ **Awareness treated as role training**

The general phishing awareness course is cited as satisfying this control — it does not.

✗ **Training after the fact**

Staff assume security duties and receive training months later — or not at all.

✗ **No training records by role**

General training records exist but cannot be linked to specific security roles or responsibilities.