AT.L2-3.2.1

Awareness & Training

Role-Based Risk Awareness

"Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems."

Objectives

[a]
Security risks associated with organizational activities involving CUI are identified.

[b]
Policies, standards, and procedures related to the security of the system are identified.

[c]
Managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.

[d]
Managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.

Key Discussion Points

All Personnel:
Everyone with access to CUI systems must receive security awareness training — not just IT staff.

Risk Awareness:
Training must cover the actual threats — phishing, social engineering, CUI handling, and insider risk.

Recurring, Not One-Time:
Annual refresher training is required — a one-time onboarding session does not satisfy this control.

Documented Records:
Training completion must be documented with dates and personnel names — verbal acknowledgment is not enough.

Assessment Methods

EXAMINE

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

INTERVIEW

Personnel with responsibilities for security awareness training; personnel with information security responsibilities; personnel composing the general system user community; personnel with responsibilities for role-based awareness training.

TEST

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

AT.L2-3.2.1

AWARENESS & TRAINING — Role-Based Risk Awareness

Plain English

What this control is really saying:

You can't secure what people don't understand. Security awareness training makes sure every person with access to CUI knows what the risks are, what the rules are, and what their responsibilities are. Policy documents nobody reads don't count.

How it is used:

- Annual security awareness training is delivered via KnowBe4 and completion is tracked in the LMS.
- Training covers CUI identification, handling requirements, phishing recognition, and incident reporting.
- New employees complete training within 30 days of hire before being granted access to CUI systems.
- Training completion records are maintained and reviewed annually as part of the security program review.

Real World Example

The Scenario

Acme Defense is a 45-person machine shop with 12 employees who handle CUI engineering drawings. The owner instituted a 'common sense' approach to security. There is no formal training program and no learning management system.

What the assessor finds

No training records exist for any employee. Three staff interviewed cannot explain what CUI is or how it should be handled. The owner says 'we talk about it at meetings' — no documentation, no curriculum, no completion tracking.

SPRS Score Impact

3.2.1 carries a point value of 5. Assessors who find no training records will also find the human vulnerabilities to match — untrained staff are the most reliable attack vector in any DIB environment.

What Good Looks Like

Annual security awareness training for all personnel, CUI-specific content included, new hire training within 30 days, completion tracked in LMS with dated records, training materials reviewed and updated annually.

Common Gaps

What assessors actually find in the field:

✗ **No training program**

No security awareness training exists — employees have never received formal training on CUI or cybersecurity.

✗ **One-time onboarding only**

Employees received a brief orientation when hired years ago but no refresher training has occurred since.

✗ **No training records**

The owner says everyone 'knows the rules' but cannot produce any documentation of training completion.

✗ **IT staff only**

Only IT staff received training — shop floor workers and administrative staff handle CUI without any training.

✗ **Generic content**

Generic cybersecurity posters are on the wall but no training specifically addresses CUI, DFARS, or CMMC.