AT.L2-3.2.3

Awareness & Training

Insider Threat Awareness

"Provide security awareness training on recognizing and reporting potential indicators of insider threat."

Objectives

[a]

Potential indicators associated with insider threats are identified.

[b]

Security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.

Key Discussion Points

Behavioral Indicators:
Job dissatisfaction, unauthorized access attempts, unexplained wealth, workplace violence, and policy violations are all listed indicators.

Managers vs. Employees:
Manager training focuses on observing team member behavior changes. Employee training focuses on general observation and reporting.

Reporting Channels:
Training must cover how to report concerns — employees need to know the procedure, not just the indicators.

Can Be Integrated:
Insider threat content does not require a separate course — it may be integrated into the standard security awareness program.

Assessment Methods

EXAMINE

Security awareness and training policy; procedures addressing security awareness training; security awareness training curriculum and materials; insider threat policy and procedures; system security plan.

INTERVIEW

Personnel that participate in security awareness training; personnel with responsibilities for basic security awareness training; personnel with information security responsibilities.

TEST

Mechanisms managing insider threat training.

AT.L2-3.2.3

AWARENESS & TRAINING — Insider Threat Awareness

Plain English

What this control is really saying:

The insider threat isn't just the disgruntled employee — it's also the well-meaning one who clicks the wrong link or takes CUI home on a USB drive. This control requires training everyone to recognize the warning signs and know where to report them before damage is done.

How it is used:

- Annual security awareness training includes a dedicated insider threat module covering behavioral indicators and reporting procedures.
- Manager training includes a specific section on observing unusual behavioral changes in team members — extended hours with no assigned project, sudden financial change, unexplained access attempts.
- Employees are trained on the company's anonymous reporting channel and what constitutes a reportable concern.
- Insider threat indicators are updated annually based on current law enforcement bulletins and threat intelligence.

Real World Example

The Scenario

Acme Defense has a general security awareness program covering phishing and password hygiene. The program was last updated in 2022. The company handles CUI daily and has had three employees with elevated access voluntarily resign in the past year.

What the assessor finds

No insider threat module exists in any training material. Neither managers nor employees can name a single behavioral indicator or identify the reporting procedure. No anonymous reporting channel exists.

SPRS Score Impact

3.2.3 carries a point value of 5. Insider threats account for a significant percentage of CUI incidents in the DIB — and an untrained workforce is the least likely to recognize or report them.

What Good Looks Like

Insider threat module integrated into annual awareness training, behavioral indicators documented and current, managers receive tailored training on team observation, anonymous reporting channel established, all completion documented.

Common Gaps

What assessors actually find in the field:

✗ **No insider threat content**

Security awareness training covers phishing and passwords but never mentions insider threat indicators or behaviors.

✗ **No reporting procedure**

Employees have no idea how or where to report a concern about a coworker — no channel has been established.

✗ **Indicators not defined**

The organization has never identified what behavioral indicators it considers relevant to their environment.

✗ **Managers not trained**

General employees got some training but managers — who are best positioned to observe behavioral changes — received nothing.

✗ **Awareness treated as sufficient**

The organization believes general cybersecurity awareness covers this requirement — the specific insider threat content is absent.