Cyber Security Champion Network Practice Training Course

15 – 19 March 2027
Addis Ababa

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Cyber Security Champion Network Practice Training Course

Ref: 764_223982 **Date:** 15 – 19 March 2027 **Location:** Addis Ababa **Fees:** 4500 Euro

Overview

Cyber Security Champion Network Practice Training Course is a one-week intermediate course for departmental champions, awareness coordinators, and business representatives who leave with a Champion Network Activation Pack. Participants turn security policy into local habits through peer influence, risk observation, micro-awareness activities, escalation routes, and adoption measures. The course separates champion responsibilities from technical security operations and builds coordination with specialist teams. Agile Leaders Training Center develops cyber security champion network practice.

Who Should Attend

- Business-unit functions responsible for representing local security concerns
- Awareness functions responsible for coordinating employee communication
- Risk and compliance functions responsible for reinforcing control behaviors
- People and learning functions responsible for workplace learning activities
- Security liaison functions responsible for connecting teams with specialists

The course assumes participants can communicate workplace guidance and coordinate colleagues, and leaves out technical incident response, penetration testing, AI security governance, and certification preparation.

Departments and Industries

The course supports departments and industries that depend on distributed security participation.

- Information security, risk, compliance, and internal control
- Human resources, learning, communications, and business operations
- Financial services and digital commerce
- Healthcare and education services
- Energy, transport, telecommunications, and public services

Learning Objectives

By the end of this course, participants will be able to:

- Apply a charter to define champion responsibilities
- Analyze local behavior and workflow risks
- Build peer messages and micro-awareness activities
- Use escalation routes for observed concerns
- Evaluate participation and adoption evidence
- Build a Champion Network Activation Pack

Course Agenda

Day 1: Define the Champion Role

- Champion Network Purpose and Boundary Map
- Role Charter and Responsibility Matrix
- Stakeholder Influence and Support Map
- Security Culture Behavior Observation Model
- Champion Ethics and Confidentiality Checklist

Day 2: Observe Local Security Risks

- Business Workflow Risk Walkthrough Method
- Unsafe Behavior Observation Card
- Local Risk Signal Classification Guide
- Concern Validation Question Set
- Risk Referral Decision Tree

Day 3: Influence Safer Team Habits

- Peer Conversation Planning Canvas
- Micro-Awareness Activity Design Sheet
- Audience and Barrier Segmentation Matrix
- Behavior Prompt and Reinforcement Toolkit
- Resistance Response Conversation Guide

Day 4: Coordinate and Measure the Network

- Security Team Escalation Route Map
- Champion Meeting and Handover Template
- Activity and Participation Evidence Log
- Behavior Adoption Indicator Scorecard
- Network Review and Improvement Cycle

Day 5: Practice Champion Network Delivery

- Exercise: Draft a Role Charter and Stakeholder Map
- Exercise: Diagnose Local Risk Signals
- Exercise: Deliver a Peer Awareness Conversation
- Exercise: Escalate and Record a Workplace Concern
- Capstone: Champion Network Activation Pack

Practical Exercises

The course uses suggested activities based on finance, healthcare, education, energy, and service operations.

- Suggested activity: map a department workflow and classify observable risk signals.
- Suggested activity: design and facilitate a short peer-awareness intervention for a defined behavior.
- Suggested activity: route a concern through an escalation scenario and record the handover.
- Suggested activity: assemble governance, communication, evidence, and measurement artifacts into an activation pack.

FAQs

Who suits cyber security champion network training, and what does it assume?

Departmental champions, awareness coordinators, business representatives, and risk or compliance staff suit the training; it assumes participants can communicate guidance and coordinate colleagues.

How does cyber security champion network training differ from general awareness training?

Champion network training develops people who influence peers, observe local risks, coordinate escalation, and track adoption, while general awareness training mainly strengthens an individual employee's safe behavior.

What should a cyber security champion role charter contain?

A champion role charter should contain purpose, scope, responsibilities, boundaries, time commitment, stakeholders, escalation routes, confidentiality expectations, activity records, and review arrangements.

How can cyber security champions measure behavior adoption?

Cyber security champions can measure adoption through participation records, repeated observations, manager feedback, question themes, reporting quality, completion of agreed actions, and changes in selected workplace behaviors.

AGILE LEADERS
Training Center

How should cyber security champions escalate a concern?

Cyber security champions should validate observable facts, avoid independent investigation, protect sensitive details, use the approved route, record the handover, and follow the specialist team's instructions.

Conclusion

Participants take back a Champion Network Activation Pack combining role boundaries, stakeholder maps, local-risk tools, peer activities, escalation routes, and adoption measures. It changes informal advocacy into a coordinated workplace practice. The pack supports consistent champion activity, clearer handovers, visible participation, and recurring improvement.