ISO 28000 Lead Implementer for Supply Chain Security

24 – 28 May 2027
Addis Ababa

AGILE LEADERS
Training Center

ISO 28000 Lead Implementer for Supply Chain Security

Ref: 103600647_225443 **Date:** 24 – 28 May 2027 **Location:** Addis Ababa **Fees:** 6000 Euro

Overview

Global distribution networks face sophisticated disruptions spanning facility breaches, transit tampering, contraband insertion, and critical cargo losses. The ISO 28000 Lead Implementer for Supply Chain Security course prepares protective specialists to build, deploy, and maintain an end-to-end security management system. Rather than focusing on external audit checklists, this curriculum targets the structural blueprints, mitigation architectures, and governance mechanisms required to safeguard cross-border freight movements and hub facilities. Participants master threat profiling, protective protocols, and process integration across multimodal corridors. This course is delivered by Agile Leaders Training Center.

Who Should Attend

- Corporate security officers and protective advisors establishing organizational safeguarding frameworks.
- Freight logistics consultants designing physical and procedural barrier architectures.
- Asset protection directors managing secure transit lanes and distribution nodes.
- Supply network resilience managers overseeing vendor integrity and partner compliance.
- Implementation leads steering enterprises toward formal certification readiness.

Departments and Industries

This masterclass supports protection strategists and operational leaders across high-value transit networks.

- International Freight Forwarding and Intermodal Distribution
- Maritime Terminal Operations and Container Yard Administration
- Aviation Cargo Logistics and Airside Freight Hubs
- Pharmaceutical, High-Tech, and High-Value Asset Manufacturing
- Third-Party Logistics Warehousing and Fleet Depots

Learning Objectives

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

- Direct the establishment of an organizational security management system aligned with international best practice.
- Conduct thorough vulnerability appraisal across physical facilities, digital touchpoints, and transport corridors.
- Construct robust mitigation architectures that neutralize illicit interference and asset diversion.
- Enforce protective protocols covering driver dispatch, container seals, and perimeter defence.
- Implement freight corridor protection measures through verified vendor screening and real-time tracking.
- Coordinate executive review routines, corrective action roadmaps, and certification audit readiness.

Course Agenda

Day 1: Project Initiation and Governance Architecture

- Scope definition and baseline appraisal for organizational security management
- Translating standard requirements into enterprise-level protective blueprints
- Leadership commitment, resource allocation, and protective governance chartering
- Stakeholder mapping, statutory mandates, and cross-border trade pact alignment
- Establishing the implementation steering committee and project timetable
- Initial gap analysis against international safeguarding specifications

Day 2: Threat Appraisal and Mitigation Architecture

- Methodologies for threat identification across static depots and transit links
- Conducting methodical vulnerability appraisal across supply workflows
- Qualitative and quantitative risk calculation for likelihood and severity
- Designing proportional mitigation architectures and treatment roadmaps
- Documented information architecture: protective policies, manuals, and records
- Formulating measurable security targets and resilience objectives

Day 3: Safeguard Deployment and Transit Protections

- Perimeter fortification, electronic surveillance, and access containment systems
- Freight corridor protection protocols for long-haul trucking and intermodal links
- Tamper-evident sealing, container verification routines, and cargo tracking
- Vetting external transport providers, contractors, and third-party warehouse operators
- Workforce screening, security culture cultivation, and role-specific drills
- Emergency escalation plans, crisis protocols, and business resumption playbooks

Day 4: Performance Verification and Continual Hardening

- Formulating security key performance indicators and control dashboards
- Conducting rigorous internal implementation reviews and process verifications
- Investigating security breaches, root cause derivation, and corrective action workflows
- Management review preparation: presenting protective maturity metrics to executives
- Managing operational change, contractor handoffs, and process modifications
- Pre-assessment readiness reviews for independent conformity verification

Day 5: Verification Readiness and Capstone Synthesis

- Reviewing implementation competency domains and practical execution criteria
- Aligning operational evidence with independent registrar evaluation benchmarks
- Overcoming implementation roadblocks across distributed distribution networks
- Facilitating continuous improvement through preventative threat countermeasures
- Developing a defensible transition roadmap from legacy practices to standard alignment
- Capstone implementation scenario presentation and individual execution clinic

Practical Exercises

Participants apply practical templates and tools to solve complex distribution challenges.

- Formulate a comprehensive vulnerability appraisal matrix for an intermodal cargo terminal.
- Draft an organizational security policy and accountability framework for dispatch hubs.
- Design high-security protective protocols for high-theft transit routes.
- Structure a corrective action plan resolving identified physical perimeter vulnerabilities.

FAQs

What specific qualifications or prerequisites are needed before enrolling in this programme?

No formal prerequisites are required. However, delegates benefit from prior exposure to freight logistics, corporate protective services, or facility operations. The curriculum focuses on building practical execution capability rather than elementary theory.

How is the daily schedule organized across the one week?

Each day provides four to five hours of structured instructional delivery, scenario problem-solving, and template drafting, totaling twenty to twenty-five direct learning hours across the programme.

What distinguishes lead implementer responsibilities from lead auditor duties?

Lead implementers construct, embed, and oversee the daily operational protective safeguards, policies, and workflows inside the enterprise. Lead auditors perform periodic, objective assessments to judge whether that established setup satisfies conformity criteria.

Conclusion

Enterprises with fortified trade lanes safeguard their profitability, commercial reputation, and workforce safety. By participating in this course, professionals gain actionable capabilities to design, deploy, and refine dependable mitigation architectures that withstand modern cargo threats and satisfy rigorous independent verification benchmarks.