

ISO 28000 Foundation Supply Chain Security Course

22 – 26 February 2027
London

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

ISO 28000 Foundation Supply Chain Security Course

Ref: 103600646_109923 **Date:** 22 – 26 February 2027 **Location:** London **Fees:** 6500 Euro

Overview

Global trade networks require consistent safeguards against illicit interference, pilferage, contraband introduction, and facility breaches. The ISO 28000 Foundation Supply Chain Security Course provides an introductory baseline overview of protective frameworks and international standard terminology without entering into complex execution engineering or audit execution scope. Participants gain conceptual familiarity with security management systems, core definitions, asset protection principles, and organizational context mapping across international trade corridors. This one-week foundational syllabus is delivered by Agile Leaders Training Center.

Who Should Attend

- New entrants to loss prevention, freight custody, and protective asset coordination roles.
- Warehouse supervisors and terminal coordinators seeking foundational standard literacy.
- Procurement administrators and vendor vetting clerks requiring an introductory understanding of partner verification.
- Corporate compliance assistants and documentation officers supporting protective governance initiatives.
- Cross-functional department liaisons collaborating with specialized security management units.

Departments and Industries

This entry-level programme introduces core protective principles across diverse freight and industrial sectors.

- Distribution Centres and Third-Party Freight Depots
- Maritime Freight Terminals and Port Boundary Facilities
- Air Freight Forwarding and Cross-Dock Handling Facilities
- Intermodal Rail and Road Haulage Fleets
- Wholesale Distribution, Import-Export, and Commercial Warehousing

Learning Objectives

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

- Define essential protective concepts, standard terminology, and structural clauses.
- Identify external and internal factors influencing organizational protection boundaries.
- Recognize how leadership commitment and organizational policy shape protective cultures.
- Distinguish basic threat identification concepts from detailed engineering treatments.
- Interpret documentation, awareness, and communication duties within protective frameworks.
- Support organizational initiatives with fundamental understanding of review cycles.

Course Agenda

Day 1: Standard Orientation and Baseline Principles

- Origins, intent, and high-level structure of international protective specifications
- Key terminology: assets, threats, vulnerabilities, and custody handovers
- The Plan-Do-Check-Act cycle applied to foundational security governance
- Differentiating foundation literacy from lead implementer and auditor roles
- Recognizing organizational boundaries, transit corridors, and facility perimeters
- Daily reflection on foundational protection concepts and terminology

Day 2: Contextual Analysis and Governance Commitments

Reviewing external stakeholder expectations and statutory operating baselines
Mapping interested parties: customs bodies, consignors, carriers, and consignees
Leadership accountability, governance visibility, and policy formulation
Assigning roles, custodial responsibilities, and reporting authorities
Establishing protective objectives aligned with broader business continuity
Daily reflection on leadership commitment and contextual boundary definitions

Day 3: Threat Identification and Basic Vulnerability Concepts

- Categorizing vulnerabilities across physical premises, cargo transit, and records
- Distinguishing threat recognition from advanced engineering calculations
- Basic vulnerability mapping for warehouses, yards, and intermodal transfers
- Overview of preventive countermeasures and custody verification routines
- Supplier integrity principles and baseline vendor vetting expectations
- Daily reflection on recognizing vulnerabilities without technical assessment formulas

Day 4: Support Mechanisms, Awareness, and Documentation

- Identifying essential organizational resources for baseline protection
- Staff competence matrices, onboarding briefings, and vigilance habits
- Internal and external communication channels during disruption events
- Controlling documented information: access permissions, records, and revisions
- Incident reporting protocols and initial notification escalation paths
- Daily reflection on information integrity and workforce awareness routines

Day 5: Review Cycles and Continual Improvement Baselines

- Fundamental methods for monitoring routine facility and custody safeguards
- Understanding the purpose of internal reviews and executive oversight
- Recognizing nonconformities and recording basic corrective action details
- Continual improvement principles for everyday distribution routines
- Clarifying organizational pathways toward advanced practitioner development
- Course review and synthesis of introductory standard requirements

FAQs

What prerequisites are required before enrolling in this foundation course?

No prior exposure to standard frameworks, facility protection certifications, or formal audits is required. The curriculum provides an entry-level introduction accessible to participants from varied operational and commercial backgrounds.

Does this programme prepare participants to conduct professional audits or lead implementations?

No. This training provides an introductory baseline overview of supply chain security management concepts without implementation or audit scope. Specialized implementation leadership and third-party audit credentials require separate, advanced-level programmes.

How does this foundation course differ from longer multi-week certifications?

This one-week course concentrates strictly on foundational awareness, standard terminology, and governance structure, avoiding extended technical calculations or specialized examination prep.