ISO 28000 Supply Chain Security Lead Auditor Training

18 – 22 April 2027
Nairobi

AGILE LEADERS
Training Center

ISO 28000 Supply Chain Security Lead Auditor Training

Ref: 103600648_110064 **Date:** 18 – 22 April 2027 **Location:** Nairobi **Fees:** 6000 Euro

Overview

Supply chain operations face complex security threats spanning cargo theft, smuggling, unauthorized access, and disruption across international transit corridors. The ISO 28000 Supply Chain Security Lead Auditor Training equips professionals with the competencies required to plan, conduct, report, and manage audits of a Supply Chain Security Management System SCSMS. Participants master ISO 28000 requirements, threat and vulnerability assessment protocols, and ISO 19011 audit guidelines to evaluate physical, operational, and supplier security controls. Through realistic scenarios and structured audit simulations, professionals build the capability to assess supply chain resilience and lead audit teams. This course is delivered by Agile Leaders Training Center.

Who Should Attend

- Lead auditors and internal auditors auditing supply chain security operations.
- Supply chain security managers and logistics security specialists.
- Freight forwarding, transport, and cargo terminal security officers.
- Risk, compliance, and governance professionals overseeing supply chains.
- Security and management system consultants preparing organizations for ISO 28000.
- Technical specialists and quality managers participating in SCSMS audit teams.

Departments and Industries

This course supports audit, security, and operations functions across global freight, transportation, and production networks.

- Logistics, Freight Forwarding, and Multi-Modal Cargo Operations
- Maritime Shipping, Seaport Terminals, and Container Handling Facilities
- Aviation Ground Handling, Air Cargo, and Courier Services
- Warehousing, Distribution Hubs, and Fulfilment Networks
- Manufacturing Plants and Industrial Assembly Facilities
- Critical Infrastructure, Energy, Food, and Pharmaceutical Supply Chains

Learning Objectives

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

- Interpret ISO 28000 requirements and core SCSMS principles in operational contexts.
- Apply ISO 19011 auditing principles to first-party, second-party, and third-party security audits.
- Establish audit scope, objectives, criteria, and resource allocations for security assessments.
- Execute Stage 1 documentation reviews and Stage 2 on-site security verification activities.
- Gather and evaluate objective audit evidence using risk-based sampling and interviewing techniques.
- Formulate and document traceable nonconformity statements and evaluate corrective action plans.
- Conduct structured opening and closing meetings and deliver formal audit conclusions.
- Manage an SCSMS audit programme aligned with organizational risk profiles and continual improvement.

Course Agenda

Day 1: ISO 28000 Requirements and Supply Chain Security Context

- Purpose, scope, and operational architecture of ISO 28000
- Supply chain security management system components and stakeholder boundaries
- Threat identification, vulnerability evaluations, and supply chain security risk assessments
- Security policies, measurable objectives, security targets, and management programmes
- Operational security controls across facilities, cargo transit, and personnel screening
- Continual improvement and management review requirements within an SCSMS

Day 2: Audit Principles and Audit Preparation

- Application of ISO 19011 audit guidelines to supply chain security audits
- Differences between internal, supplier qualification, and formal certification audits
- Auditor ethics, professional objectivity, independence, and information confidentiality
- Determining audit objectives, scope boundaries, evaluation criteria, and feasibility
- Audit team assignment, resource distribution, and technical expert integration
- Developing risk-based audit plans, security checklists, and working papers

Day 3: Conducting Stage 1 and Stage 2 Audits

- Executing the formal opening meeting and confirming communication protocols
- Stage 1 documentation review of security policies, procedures, and risk registers
- Stage 2 audit execution and on-site verification of physical and digital security controls
- Evidence collection techniques across personnel interviews, observation, and record checks
- Audit sampling methodologies and evaluation of evidence corroboration and sufficiency
- Managing audit trails, escort guides, observers, and challenging on-site situations

Day 4: Audit Findings, Nonconformities, and Reporting

- Analyzing audit evidence against ISO 28000 criteria and security benchmarks
- Categorizing findings into conformity, observations, and nonconformities
- Drafting clear, traceable, and evidence-supported nonconformity reports
- Synthesizing findings to establish defensible audit conclusions and recommendations
- Facilitating the closing meeting and presenting audit conclusions to leadership
- Evaluating root cause analyses, corrective action plans, and follow-up verification

Day 5: Audit Programme Management and Lead Auditor Practice

- Designing, monitoring, and improving an organization-wide SCSMS audit programme
- Managing audit programme risks, resource allocation, records, and data security
- Evaluating auditor competence, performance indicators, and audit team collaboration
- Coordinating combined management system audits and multi-site security evaluations
- Simulated end-to-end ISO 28000 audit covering planning through reporting
- Resolving scenario-based lead auditor dilemmas in supply chain environments

Practical Exercises

Participants complete applied exercises to build audit execution capabilities and professional judgement.

- Suggested activity: Formulate an ISO 28000 audit checklist targeting cargo handling and physical access controls.
- Suggested activity: Review a simulated Stage 1 security risk assessment to determine audit feasibility.
- Suggested activity: Draft an evidence-based nonconformity statement based on a simulated transit security breach.
- Suggested activity: Role-play a lead auditor conducting a formal closing meeting with facility leadership.

FAQs

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

Formal prerequisites are not mandatory. However, prior knowledge of ISO management systems, supply chain operations, security practices, risk management, or internal auditing principles is recommended for participants.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day is structured to run for four to five hours, including interactive exercises and discussions. The five-day course comprises approximately 20 to 25 hours of active instruction.

What is the difference between an ISO 28000 internal auditor and a lead auditor?

An internal auditor primarily conducts audits within an organization. A lead auditor manages the entire audit process, directs the audit team, evaluates complex evidence, presents findings during closing meetings, and oversees reporting and corrective-action verification.

Conclusion

This training delivers the practical skills needed to evaluate supply chain security practices systematically. By mastering ISO 28000 requirements, evidence gathering, and ISO 19011 auditing principles, participants gain the capability to lead audits that reinforce security controls, mitigate operational vulnerabilities, and support supply chain resilience across complex international networks.