Supply Chain Security Management: ISO 28000, AEO and Cargo Integrity

9 – 13 May 2027
Jeddah - Corniche four-star



Supply Chain Security Management: ISO 28000, AEO and Cargo Integrity

Ref: 427_13938 **Date:** 9 – 13 May 2027 **Location:** Jeddah - Corniche four-star **Fees:** 19500 SAR

Introduction:

Supply chain security management often stops at the warehouse fence, while cargo is stolen, tampered with or used to smuggle contraband at handover points, in transit and through partners nobody vetted. This Core Concept course gives logistics, security and customs compliance managers a working method to assess threats across nodes and routes, apply an ISO 28000 security management system, protect containers and seals, track shipments and screen partners and personnel against Authorized Economic Operator security criteria. Participants produce a Cargo Security Plan and AEO Security Readiness Self-Assessment for their own operation.

Course Objectives:

- Map the cargo threats of theft, pilferage, tampering, smuggling and terrorism to each node, handover point and transport leg of an operation
- Set up and maintain an ISO 28000 security management system with a security policy, objectives, operational controls and performance evaluation
- Assess the security criteria that customs administrations apply to Authorized Economic Operators under the WCO SAFE Framework and close the gaps found
- Specify container and seal integrity checks, cargo tracking and in-transit controls for road, sea and air shipments
- Vet business partners, carriers and personnel against documented security requirements and keep evidence for audits
- Run supply chain security audits, report and investigate cargo security incidents and feed corrective actions back into the security plan

Target Audience:

- Managers responsible for warehouse, distribution centre and cross-dock operations where cargo is received, stored and dispatched
- Managers responsible for transport, freight forwarding and carrier operations that move cargo between nodes
- Security managers responsible for protecting cargo, logistics facilities and the people who handle goods
- Customs compliance managers responsible for trade security partnerships and authorised operator status
- Procurement and supplier managers responsible for onboarding and monitoring logistics service providers
- Quality, audit and risk managers responsible for management system audits across logistics operations

Course Outline:

Day 1: Supply Chain Security Landscape and Cargo Threat Picture

- Cargo Crime Typology: Theft, Pilferage, Hijacking and Fictitious Pickups
- Tampering, Concealment and Smuggling Methods Using Legitimate Shipments
- Terrorism and Weapons Risks in Containerised and Consolidated Freight
- Node and Route Map of an End-to-End Shipment With Custody Transfer Points
- Cargo Security Current-State Self-Assessment Questionnaire

Day 2: ISO 28000 Security Management System and the WCO SAFE Framework

- ISO 28000 Clause Structure: Context, Leadership, Planning, Support, Operation, Evaluation and Improvement
- Security Policy, Objectives and Plan-Do-Check-Act Cycle for Logistics Operations
- Integrating the Security Management System With ISO 9001, ISO 14001 and ISO 22301
- WCO SAFE Framework Pillars: Customs-to-Customs and Customs-to-Business Cooperation
- Authorized Economic Operator Security Criteria: Information, Employee and Premises Integrity

Day 3: Securing Nodes, Containers and Shipments in Transit

- Security Risk Assessment Matrix for Warehouses, Yards and Transport Routes
- Logistics Facility Controls: Perimeter, Loading Docks, Trailer Yards and Cargo Cages
- Container Pre-Loading Structural Inspection and Seal Affixing, Verification and Logging Procedure
- Cargo Tracking With GPS, RFID and Electronic Seals and In-Transit Exception Alerts
- Advance Electronic Cargo Information and Manifest-to-Load Reconciliation

Day 4: Partners, Personnel, Information Security and Incident Response

- Business Partner Security Questionnaire, Tiering and Contract Security Clauses
- Personnel Security: Pre-Employment Screening, Access Rights and Insider Threat Indicators
- Shipping Data Protection and Cyber Threats to Logistics Systems at Overview
- Cargo Security Incident Reporting, Seal Breach Investigation and Evidence Chain
- Supply Chain Security Internal Audit Programme and Corrective Action Tracking

Day 5: Case Studies and Cargo Security Plan Build

- Case Study: Seal Anomaly and Concealed Contraband in a Full Container Load
- Case Study: Cargo Theft Pattern Across a Multi-Carrier Distribution Network
- AEO Security Readiness Self-Assessment Scoring and Gap Prioritisation
- Security KPI Set: Seal Discrepancies, Partner Compliance and Incident Closure Time
- Cargo Security Plan Assembly and Peer Review

Skills You Will Gain:

- Cargo Threat Mapping
- Security Management System Implementation
- Node and Route Risk Assessment
- Container and Seal Integrity Control
- Shipment Tracking Oversight
- Business Partner Security Vetting
- Security Incident Investigation
- Supply Chain Security Auditing

Why Attend This Course:

- Return with a Cargo Security Plan and AEO Security Readiness Self-Assessment built on your own operation
- Find where custody of goods changes hands without checks and set controls at each of those points
- Brief drivers, dock teams and partners on seal, loading and exception procedures they can follow on shift
- Compare cargo security practice with peers from manufacturing, retail, freight forwarding, oil and gas and pharmaceutical supply chains

Conclusion:

Cargo stays secure when every node, route, partner and person in the chain works to the same documented controls. The course moves from the cargo threat picture through the ISO 28000 security management system and AEO criteria under the WCO SAFE Framework, to facility, container, seal and tracking controls, then to partner vetting, personnel and information security, audits and incident response. The final day applies these methods to case studies and closes with a Cargo Security Plan and AEO Security Readiness Self-Assessment ready for internal review.