

Anti-Counterfeit Supply Chain Control Training Course

26 – 30 September 2027
Nairobi

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Anti-Counterfeit Supply Chain Control Training Course

Ref: 1778_233673 **Date:** 26 – 30 September 2027 **Location:** Nairobi **Fees:** 4500 Euro

Overview

Anti-Counterfeit Supply Chain Control is a one-week advanced course for supply-chain, procurement, quality, brand-protection, compliance, logistics, warehouse, security, and product-integrity functions. Participants build an Anti-Counterfeit Supply Chain Control and Response Plan connecting counterfeit-threat analysis, supplier controls, authentication, serialization, traceability, custody, channel monitoring, incident evidence, withdrawal, recall, and improvement. Agile Leaders Training Center presents anti-counterfeit supply chain control as coordinated prevention, detection, and response.

Who Should Attend

- Supply-chain and procurement functions responsible for supplier and channel integrity
- Quality and product-integrity functions responsible for authenticity and release decisions
- Brand-protection, compliance, legal, and security functions managing counterfeit incidents
- Logistics and warehouse functions responsible for custody, receiving, storage, and dispatch controls
- E-commerce, marketplace, distributor, and channel-management functions monitoring diversion and suspect listings

The course assumes participants manage products, suppliers, logistics, quality evidence, channels, or investigations and excludes legal advice, laboratory-specialist training, and sector-specific regulatory certification.

Departments and Industries

The course supports product-authenticity decisions across physical and digital supply channels.

- Supply chain, procurement, supplier quality, logistics, and warehousing
- Brand protection, product integrity, compliance, legal, security, and investigations
- Pharmaceutical, medical-device, automotive, electronics, and industrial-parts supply chains
- Consumer goods, cosmetics, apparel, food, and retail distribution
- E-commerce platforms, marketplaces, distributors, freight operators, and third-party logistics providers

Learning Objectives

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

- Analyze counterfeit threats, vulnerable routes, products, suppliers, and channels.
- Design supplier, contract, authentication, and product-identification controls.
- Evaluate serialization, traceability, chain-of-custody, and data-integrity evidence.
- Strengthen receiving, warehouse, e-commerce, marketplace, and diversion controls.
- Direct counterfeit incident triage, evidence preservation, escalation, withdrawal, and recall.
- Integrate partner collaboration, audit findings, metrics, and corrective actions.

Course Agenda

Day 1: Counterfeit Threat and Exposure Analysis

- Counterfeit Threat Actor and Entry-Route Map
- Product Attractiveness and Harm-Risk Matrix
- Supplier, Geography, and Channel Vulnerability Profile
- Authentic, Suspect, Counterfeit, and Diverted Product Decision Tree
- Anti-Counterfeit Control Ownership and Escalation Register

Day 2: Supplier and Authentication Controls

- Supplier Qualification and Beneficial-Ownership Review File
- Contractual Authenticity, Audit, Notification, and Remedy Clause Set
- ISO 22383 Authentication Solution Selection and Evaluation Grid
- Overt, Covert, Forensic, and Digital Authentication Layer Model
- Packaging, Label, Component, and Security-Feature Change Control

Day 3: Identification, Traceability, and Custody

- ISO 22378 Object Identification and Participant Due-Diligence Map
- Unique Identifier, Serialization, Aggregation, and Verification Flow
- Chain-of-Custody Event and Authorized-Participant Record
- Identifier Issuance, Access-Log, and Data-Integrity Control Checklist
- Receiving Inspection, Quarantine, Release, and Warehouse Status Board

Day 4: Channel Monitoring and Incident Response

- E-Commerce Listing, Marketplace Seller, and Small-Parcel Triage Grid
- Diversion, Grey-Market, Return, and Reverse-Logistics Control Map
- Suspect Product Intake and Incident-Severity Classification
- Evidence Preservation, Case Handoff, and Information-Sharing Protocol
- Withdrawal, Recall, Channel Notification, and Corrective-Action File

AGILE LEADERS
Training Center

Day 5: Anti-Counterfeit Control Simulation

- Exercise: Map a Counterfeit Entry Route and Product-Risk Profile
- Exercise: Select Authentication Layers and Supplier Controls
- Exercise: Validate Serialization, Custody, and Receiving Evidence
- Exercise: Resolve a Marketplace Counterfeit Incident and Recall Decision
- Capstone Exercise: Build the Anti-Counterfeit Supply Chain Control and Response Plan

Practical Exercises

The course uses suggested activities to turn product, supplier, channel, custody, and incident evidence into controlled decisions.

- Suggested activity: map counterfeit exposure for automotive parts and consumer cosmetics.
- Suggested activity: compare authentication layers and test supplier-control coverage.
- Suggested activity: trace identifiers, custody events, access logs, and receiving discrepancies.
- Suggested activity: triage a suspect marketplace listing and coordinate evidence, withdrawal, and corrective action.

FAQs

Who suits anti-counterfeit supply chain training, and what does it assume?

Anti-counterfeit supply chain training suits professionals who manage products, suppliers, logistics, channels, quality evidence, security, or investigations and assumes working knowledge of organizational supply-chain responsibilities.

How does anti-counterfeit supply chain training differ from general traceability training?

Anti-counterfeit supply chain training connects traceability with threat analysis, authentication, supplier controls, channel monitoring, evidence handling, and incident response rather than treating product movement records as the sole objective.

How should supply chains select product-authentication controls?

Supply chains should select authentication controls after evaluating product risk, likely counterfeit methods, users, inspection conditions, identifier governance, evidence needs, system interoperability, control layering, and performance-testing criteria.

What evidence supports a counterfeit-product incident decision?

Counterfeit-product incident decisions draw on product identifiers, packaging and feature checks, custody events, supplier records, purchase and shipping data, images, samples, access logs, marketplace information, and authorized expert findings.

How do anti-counterfeit controls address e-commerce and diversion?

Anti-counterfeit controls address e-commerce and diversion through seller screening, listing monitoring, small-parcel triage, authorized-channel mapping, return controls, test purchases, data sharing, escalation routes, and documented action against suspect products.

Conclusion

Participants take back an Anti-Counterfeit Supply Chain Control and Response Plan. It aligns product and supplier risk, authentication, identifiers, custody, receiving, channel monitoring, incident evidence, withdrawal, recall, metrics, and improvement. The plan makes responsibilities, decision criteria, records, escalation, partner handoffs, and corrective action visible across physical and digital supply channels.