CONCEPT

Anti-Counterfeiting and Brand Protection: Product Authentication and Channel Integrity

29 August – 2 September 2027
Riyadh - KAFD district five-star



Anti-Counterfeiting and Brand Protection: Product Authentication and Channel Integrity

Ref: 498_16730 **Date:** 29 August – 2 September 2027 **Location:** Riyadh - KAFD district five-star **Fees:** 20000 SAR

Introduction:

Counterfeit, grey-market and diverted products slip into distribution channels through unvetted suppliers, leaky distributors and online marketplaces, eroding revenue, exposing customers to unsafe goods and damaging trust in the brand. This Core Concept course gives supply chain, brand protection, legal, quality and security staff a working anti-counterfeiting and brand protection method: map product fraud risk across the chain, select layered authentication features, tighten partner controls, monitor marketplaces, work with customs and respond to incidents. Participants produce a Brand Protection Programme and Authentication Plan for one of their own product lines.

Course Objectives:

- Classify counterfeit, grey-market, diversion and tampering threats and estimate their business impact for a product portfolio
- Map product fraud risk across the supply and distribution chain using the general principles of ISO 22380
- Select layered overt, covert and digital authentication features, serialisation and track-and-trace against ISO 12931 and ISO 22383 performance criteria
- Apply anti-counterfeit controls and audits to suppliers, contract manufacturers and authorised distributors
- Run marketplace monitoring, takedown requests, test purchases and investigation referrals and coordinate border measures with customs
- Lead counterfeit incident response and recall decisions and track a brand protection programme with KPIs

Target Audience:

- Supply chain and distribution functions responsible for supplier onboarding, channel partners and product flow
- Brand protection functions responsible for detecting, investigating and removing counterfeit and diverted products
- Legal and IP functions responsible for trademark portfolios, enforcement actions and partner contracts
- Quality functions responsible for packaging specifications, complaint handling and product recall
- Corporate security functions responsible for investigations, evidence handling and liaison with enforcement bodies
- E-commerce and channel sales functions responsible for online marketplaces and authorised reseller networks

Course Outline:

Day 1: Counterfeit, Grey-Market and Diversion Threat Landscape

- Counterfeiting, Grey-Market Parallel Trade, Product Diversion and Tampering Typology
- Business Impact Model: Lost Revenue, Safety Harm, Warranty Cost and Brand Trust Erosion
- Product Fraud Entry Points From Component Suppliers to Retail Shelf and Online Listing
- Product Fraud Risk Heat Map by Product Line, Channel and Market Segment
- Brand Protection Maturity Self-Assessment Questionnaire

Day 2: Authentication Standards and Product Security Technologies

- ISO 22380 General Principles for Product Fraud Risk and the ISO 22380-Series Structure
- ISO 12931 and ISO 22383 Performance Criteria for Authentication Solutions for Material Goods
- Overt, Covert and Forensic Features: Holograms, Colour-Shifting Inks, Micro-Printing and Taggants
- Tamper-Evident Packaging, Security Labels and Closure Design Choices
- Unit-Level Serialisation, RFID and NFC Tags, QR Codes and Digital Product IDs With ISO 22381 Interoperability

Day 3: Supplier, Distributor and Online Channel Controls

- Supplier Anti-Counterfeit Clauses, Scrap and Overrun Control and Component Traceability Audits
- Authorised Distributor Agreements, Territory Rules and Channel Audit Checklist
- Serial Number Scan Data Analytics to Detect Diversion and Cloned Codes
- E-Commerce and Marketplace Monitoring Workflow With Listing Evidence Capture
- Notice-and-Takedown Requests, Seller Escalation and Repeat Infringer Tracking

Day 4: Investigations, Enforcement and Incident Response

- Test Purchase Protocol, Sample Chain of Custody and Genuine-Versus-Suspect Comparison Report
- Investigation Case File: Source Tracing, Evidence Handling and Referral Decision Criteria
- Recording Trademarks and Other IP Rights With Customs and Border Measures Cooperation
- Counterfeit Incident Response Playbook: Triage, Stakeholder Notification and Product Recall
- ISO 22384 Protection Plan Monitoring and Brand Protection KPI Set

Day 5: Case Work and Brand Protection Programme Build

- Case Study: Counterfeit Spare Parts Entering an Industrial Aftermarket Channel
- Case Study: Grey-Market Diversion of Cosmetics Through Online Resellers
- Authentication Feature Selection Matrix for a Chosen Product Line
- Brand Protection Programme Governance: Roles, Budget Case and Cross-Functional Working Group
- Brand Protection Programme and Authentication Plan Drafting and Peer Review

Skills You Will Gain:

- Product Fraud Risk Mapping
- Authentication Feature Selection
- Serialisation and Track-and-Trace Oversight
- Distributor Channel Auditing
- Online Marketplace Enforcement
- Test Purchase Evidence Handling
- Counterfeit Incident Management
- Brand Protection KPI Reporting

Why Attend This Course:

- Return with a Brand Protection Programme and Authentication Plan for one of your own product lines
- Spot where genuine product leaks into unauthorised channels and where fakes enter before customers find them
- Brief packaging, legal and sales colleagues with one shared evidence standard for suspect products
- Compare brand protection practice with peers from pharmaceuticals, consumer goods, automotive parts and electronics

Conclusion:

Counterfeits and diverted goods are contained when authentication, partner controls, online monitoring and enforcement work as one programme rather than separate efforts. The week moves from the threat landscape and product fraud risk mapping, through ISO 12931, the ISO 22380 series and the authentication technologies behind them, to supplier, distributor and marketplace controls, then to test purchases, investigations, customs cooperation, incident response and KPIs. The final day applies these methods to multi-sector cases and closes with a Brand Protection Programme and Authentication Plan ready for internal review.