Digital Fraud Risk Management and Controls Course

28 February – 4 March 2027
Nairobi

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Digital Fraud Risk Management and Controls Course

Ref: 1243_191840 **Date:** 28 February – 4 March 2027 **Location:** Nairobi **Fees:** 4500 Euro

Overview

Digital Fraud Risk Management and Controls Course is a one-week advanced programme for professionals responsible for fraud exposure across digital identities, customer journeys, accounts, devices, online payments, platforms, and connected services. Participants connect fraud typologies with threat intelligence, journey mapping, identity proofing, authentication, transaction monitoring, device and behavioural signals, case operations, investigations, privacy, customer protection, redress, third-party dependencies, control testing, and continuous improvement.

Each participant develops a Digital Fraud Risk and Control Playbook for a selected digital service. The playbook contains a fraud threat model, journey-risk map, control architecture, signal catalogue, detection scenarios, alert and case workflow, investigation boundaries, privacy safeguards, victim-response design, performance dashboard, and improvement backlog. Agile Leaders Training Center presents digital fraud management as a continuously tested operating system across people, process, data, technology, and governance.

Who Should Attend

- Fraud-risk, fraud-strategy, fraud-operations, and financial-crime professionals
- Digital banking, payments, e-commerce, platform, and customer-journey leaders
- Identity, access, authentication, cybersecurity, and threat-intelligence teams
- Data analytics, model-risk, decision-science, and monitoring professionals
- Compliance, privacy, legal, internal audit, and operational-risk specialists
- Investigators, dispute, chargeback, complaints, and customer-protection teams
- Product, engineering, vendor-management, and third-party assurance functions

The course assumes participants support fraud decisions or digital services. It does not provide hacking instruction, legal advice, law-enforcement authority, or a substitute for competent technical, privacy, investigative, and regulatory review.

AGILE LEADERS
Training Center

Learning Objectives

- Map digital fraud exposure across identities, devices, accounts, transactions, channels, and third parties
- Distinguish cyber intrusion, social engineering, authorised payment manipulation, identity fraud, and internal abuse
- Design layered preventive, detective, responsive, and recovery controls
- Strengthen identity proofing, authentication, account recovery, and customer redress
- Turn data and threat signals into explainable detection scenarios and alert priorities
- Govern cases, evidence, privacy, referrals, and cross-functional response
- Measure control effectiveness, customer impact, false positives, losses, and emerging threats
- Continuously test and improve fraud controls as tactics and technology change

Practical Work Product

Participants build a Digital Fraud Risk and Control Playbook containing:

- Digital service and customer-journey map
- Fraud typology and threat model
- Identity and account control architecture
- Signal and data-source catalogue
- Detection-scenario and threshold library
- Alert, case, escalation, and referral workflow
- Privacy, fairness, and customer-redress safeguards
- Control performance dashboard
- Ninety-day improvement backlog

Day 1: Digital Fraud Landscape and Journey Risk

- Digital ecosystems, trust boundaries, dependencies, and attack surfaces
- Fraud actors, motivation, capability, collaboration, and industrialised fraud services
- Social engineering, impersonation, phishing, business-email compromise, scams, and authorised payment manipulation
- Account takeover, synthetic identity, application fraud, mule activity, internal abuse, and collusion
- Mapping exposure through onboarding, login, account change, payment, support, recovery, and closure

Workshop: build a customer-journey risk map linking actors, methods, opportunities, consequences, and existing controls.

AGILE LEADERS
Training Center

Day 2: Digital Identity, Authentication, and Account Protection

- Identity proofing risk, evidence, authoritative sources, and verification decisions
- Stolen, fabricated, synthetic, manipulated, and compromised identity patterns
- Authentication assurance, device binding, biometrics, passkeys, step-up controls, and recovery risk
- SIM swaps, proxy and IP indicators, device tenure, account age, and unusual change events
- Privacy risk, accessibility, bias, customer friction, failed checks, appeals, and redress

Workshop: design an identity and account-protection control architecture with assurance levels, exceptions, compensating controls, and residual-risk decisions.

Day 3: Signals, Detection, and Fraud Analytics

- Transaction, device, network, behavioural, identity, customer, and threat-intelligence signals
- Detection rules, scenarios, scores, models, thresholds, velocity, linkage, and sequence
- Leading indicators, data quality, feature drift, model limitations, and explainability
- Alert prioritisation, false positives, false negatives, capacity, queues, and service levels
- Testing detection coverage against typologies and adversary adaptation

Workshop: create a signal catalogue and detection library with logic, data lineage, thresholds, ownership, testing, and review frequency.

Day 4: Cases, Investigation, Response, and Customer Protection

- Alert enrichment, triage, case creation, severity, ownership, and escalation
- Evidence integrity, timelines, access controls, documentation, and decision records
- Boundaries between fraud operations, cybersecurity, compliance, privacy, legal, HR, and law enforcement
- Transaction holds, account restrictions, step-up checks, customer contact, and proportional intervention
- Victim support, complaints, disputes, reimbursement decisions, redress, and communication

Workshop: design an end-to-end case and response workflow for a coordinated account-takeover and payment-fraud event.

Day 5: Governance, Control Effectiveness, and Adaptation

- Fraud risk appetite, ownership, committees, authorities, escalation, and reporting
- Third-party identity, payment, data, cloud, platform, and outsourced-operation dependencies
- Metrics for attempted and realised fraud, prevented loss, detection quality, case outcomes, customer impact, and cost
- Control testing, scenario replay, red-team findings, incident lessons, and remediation verification
- Threat monitoring, continuous evaluation, change governance, and the ninety-day improvement backlog

Capstone: present and challenge the Digital Fraud Risk and Control Playbook before a simulated fraud governance committee.

Training Methods

- Digital fraud cases and customer-journey threat mapping
- Identity, signal, detection, and control-design workshops
- Alert, case, response, and redress simulations
- Control-testing and performance-measurement exercises
- Peer review of fraud playbooks and improvement backlogs

Course Outcomes

Participants leave able to connect evolving digital fraud methods with layered controls, usable signals, accountable decisions, proportionate response, and measurable performance. They can improve fraud protection while addressing privacy, fairness, customer friction, and redress rather than optimising loss reduction in isolation.

Frequently Asked Questions

Is this a cybersecurity course?

No. It addresses fraud risk and controls across digital services and interfaces with cybersecurity where the same event involves both compromise and fraud.

Does the course teach offensive hacking?

No. It studies fraud methods for defensive risk assessment, detection, response, and governance only.

Is it limited to banks?

No. The methods apply to payments, fintech, e-commerce, platforms, telecommunications, government services, and other digital organisations.

What will I produce?

You will complete a Digital Fraud Risk and Control Playbook covering journeys, threats, identity, signals, detection, cases, redress, metrics, and improvement.