



AUDITING AND GOVERNANCE RISK AND COMPLIANCE | AGRC-019

AI-Driven Fraud Detection in Banking

Contact

+31 85 7444446
info@aractech.com
<https://aractech.com>

Address

Waarderweg 50, 2031PB Haarlem - Netherlands.

Course content

Why Attend

Financial fraud represents a significant and evolving threat to the banking industry. The rapid expansion of digital banking, instant payments, mobile financial services, and interconnected financial platforms has created new opportunities for fraudsters to exploit vulnerabilities in banking systems, customer interactions, and transaction processes.

Traditional fraud detection systems often rely on predefined rules, manual investigations, and historical fraud patterns. Although these approaches remain important, they can struggle to identify emerging fraud techniques, sophisticated transaction networks, and rapidly changing criminal behaviours. High volumes of false alerts can also overwhelm investigation teams, increase operational costs, and delay legitimate customer transactions.

Course Methodology

- The programme combines instructor-led discussions, banking fraud case studies, AI and machine learning demonstrations, analytical workshops, fraud detection simulations, and model governance exercises.
- Participants work with illustrative banking datasets containing transaction histories, customer behaviour indicators, payment information, account relationships, fraud labels, and investigation outcomes.
- Practical activities demonstrate fraud data preparation, feature engineering, anomaly detection, classification techniques, alert scoring, model performance evaluation, and investigation prioritisation.
- The programme is designed for both technical and non-technical banking professionals. Technical concepts are explained through practical applications, while advanced analytical exercises illustrate how fraud detection models can be developed, evaluated, and deployed within banking environments.

Course Objectives

- Explain the major types of banking fraud and their evolving risk characteristics
- Understand the applications of artificial intelligence and machine learning in fraud detection
- Identify and prepare relevant banking transaction and behavioural data
- Apply supervised and unsupervised learning concepts to fraud detection scenarios
- Understand anomaly detection and behavioural analytics techniques

Course content

- Evaluate fraud detection models using appropriate performance metrics

| Target Audience

- This course is suitable for:
- Banking fraud prevention and detection managers
- Financial crime compliance professionals
- Banking risk management specialists

Course outline

Detailed course outline

Day-by-day outline for AI-Driven Fraud Detection in Banking.

Day 1 - Banking Fraud Landscape and Foundations of AI-Driven Detection

- 09:00-09:39 | Understanding the banking fraud landscape, including payment fraud, account takeover, identity fraud, card fraud, authorised push payment scams, and fraudulent account activity
- 09:39-10:18 | Examining the limitations of traditional rule-based fraud detection systems and the opportunities presented by AI, machine learning, and advanced analytics
- 10:18-10:57 | Exploring the fraud detection lifecycle, including prevention, monitoring, alert generation, investigation, case resolution, and feedback mechanisms
- 10:57-11:00 | Understanding the fundamentals of supervised learning, unsupervised learning, anomaly detection, and predictive analytics in banking fraud management
- 11:00-11:30 | Coffee break
- 11:30-12:05 | Understanding the fundamentals of supervised learning, unsupervised learning, anomaly detection, and predictive analytics in banking fraud management (continued)
- 12:05-12:43 | Identifying relevant fraud data sources, including transaction records, customer profiles, device information, digital channel activity, and historical investigation outcomes
- 12:43-14:00 | Practical workshop: Analysing banking fraud scenarios and identifying opportunities for AI-driven detection across customer journeys and payment processes

Course outline

Detailed course outline

Day-by-day outline for AI-Driven Fraud Detection in Banking.

Day 2 - Fraud Data Analytics, Machine Learning and Anomaly Detection

- 09:00-09:34 | Preparing banking fraud datasets through data cleaning, validation, integration, transformation, and the handling of missing or inconsistent information
- 09:34-10:41 | Developing fraud detection features using transaction frequency, payment amounts, account activity, behavioural deviations, geographic signals, and customer history
- 10:41-11:00 | Understanding supervised classification algorithms, including logistic regression, decision trees, random forests, and gradient boosting techniques
- 11:00-11:30 | Coffee break
- 11:30-11:45 | Understanding supervised classification algorithms, including logistic regression, decision trees, random forests, and gradient boosting techniques (continued)
- 11:45-12:19 | Exploring unsupervised learning methods, including clustering, isolation forests, and anomaly scoring for detecting previously unidentified suspicious patterns
- 12:19-12:53 | Addressing class imbalance, limited fraud labels, data leakage, and the challenges of training models on rare fraudulent events
- 12:53-14:00 | Analytical workshop: Designing and evaluating a machine learning fraud detection model using illustrative banking transaction data and risk indicators

Course outline

Detailed course outline

Day-by-day outline for AI-Driven Fraud Detection in Banking.

Day 3 - Advanced Fraud Analytics, Behavioural Intelligence and Network Detection

- 09:00-09:39 | Applying behavioural analytics to identify deviations from normal customer transaction patterns, account usage, login activity, and payment behaviour
- 09:39-10:18 | Understanding graph analytics and network-based detection techniques for identifying suspicious relationships between accounts, devices, beneficiaries, and transactions
- 10:18-10:57 | Exploring the use of sequential and temporal analysis to detect unusual transaction sequences, rapid account activity, and coordinated fraud attempts
- 10:57-11:00 | Examining AI applications in identity verification, digital onboarding, document fraud detection, and account takeover prevention
- 11:00-11:30 | Coffee break
- 11:30-12:05 | Examining AI applications in identity verification, digital onboarding, document fraud detection, and account takeover prevention (continued)
- 12:05-12:43 | Evaluating fraud risk scoring techniques that combine machine learning outputs, business rules, behavioural signals, and contextual risk information
- 12:43-14:00 | Case study: Investigating a simulated coordinated banking fraud network using behavioural indicators, transaction relationships, and risk-based alert prioritisation

Course outline

Detailed course outline

Day-by-day outline for AI-Driven Fraud Detection in Banking.

Day 4 - Real-Time Fraud Detection, Model Performance and Investigation Integration

- 09:00-09:39 | Understanding real-time fraud detection architectures involving transaction data streams, feature generation, model scoring, decision engines, and automated alerts
- 09:39-10:18 | Evaluating fraud model performance using precision, recall, F1-score, precision-recall curves, false-positive rates, and financial loss-based measures
- 10:18-10:57 | Establishing risk thresholds and decision strategies that balance fraud prevention, customer experience, investigation capacity, and operational costs
- 10:57-11:00 | Integrating AI-generated alerts with fraud investigation workflows, case management systems, analyst feedback, and escalation procedures
- 11:00-11:30 | Coffee break
- 11:30-12:05 | Integrating AI-generated alerts with fraud investigation workflows, case management systems, analyst feedback, and escalation procedures (continued)
- 12:05-12:43 | Monitoring model performance for data drift, changing fraud patterns, declining detection effectiveness, and the need for model recalibration or retraining
- 12:43-14:00 | Practical exercise: Designing a real-time fraud monitoring workflow with model performance indicators, alert thresholds, investigation priorities, and customer protection controls

Course outline

Detailed course outline

Day-by-day outline for AI-Driven Fraud Detection in Banking.

Day 5 - Responsible AI, Fraud Model Governance and Banking Implementation Strategy

- 09:00-09:34 | Establishing governance arrangements for AI-driven fraud detection covering model ownership, validation, documentation, approval, accountability, and independent oversight
- 09:34-10:08 | Understanding explainable AI techniques and the importance of interpreting fraud risk scores, model decisions, and contributing risk factors
- 10:08-10:42 | Assessing privacy, data protection, fairness, cybersecurity, and third-party technology risks associated with banking AI systems
- 10:42-11:00 | Evaluating relevant regulatory and supervisory expectations for financial crime controls, model risk management, operational resilience, and automated decision-making
- 11:00-11:30 | Coffee break
- 11:30-11:46 | Evaluating relevant regulatory and supervisory expectations for financial crime controls, model risk management, operational resilience, and automated decision-making (continued)
- 11:46-12:53 | Developing implementation roadmaps covering business requirements, data readiness, technology selection, pilot testing, integration, model monitoring, and continuous improvement
- 12:53-14:00 | Capstone exercise: Developing and presenting a Comprehensive AI-Driven Banking Fraud Detection Framework incorporating fraud risk assessment, data architecture, machine learning techniques, behavioural analytics, fraud scoring, real-time monitoring, investigation workflows, model governance, and implementation priorities

Seminar dates

Available seminar dates

Live dates and pricing for AI-Driven Fraud Detection in Banking generated from the course details page.

Date	Location	Format	Fee
------	----------	--------	-----

No seminar dates are currently available.