
AI-Driven Fraud Analytics and Real-Time Transaction Monitoring Training Course

13 – 17 December 2026
Kuala Lumpur





AI-Driven Fraud Analytics and Real-Time Transaction Monitoring Training Course

Ref: 241_18663 **Date:** 13 – 17 December 2026 **Location:** Kuala Lumpur **Fees:** 4000 GBP

Programme Summary

AI-driven fraud analytics and real-time transaction monitoring is the subject of this five-day training course for fraud, financial crime and risk leaders at advanced level, culminating in an AI fraud detection roadmap for one product or payment channel. Fraud now moves at the speed of instant payments, and rule-based alerts either miss new schemes or bury analysts in false positives. The approach moves from fraud risk governance, through detection models and network analytics, to validation and operating design. Mars Training Centre UK delivers this programme in AI-driven fraud analytics.

The Business Case

Every undetected scheme becomes a direct loss, and every unnecessary alert costs analyst time and frustrates genuine customers. Machine learning can score transactions instantly and reveal hidden links between accounts, if its outputs are explainable and validated. Leaders who govern these models inside the fraud risk management programme catch more fraud with fewer interventions.

- Fraud Losses: Fall as anomaly and supervised models detect emerging schemes earlier.
- False Positive Rate: Drops as risk scores replace blunt rules and alert queues are prioritised.
- Investigation Cycle Time: Shortens as network analytics surface linked accounts and fraud rings.

Principles and Evidence Base

- COSO/ACFE Fraud Risk Management Guide: Its five principles frame where AI detection fits the fraud programme in Session 1.
- Supervised and Unsupervised Learning: Classification and anomaly detection methods structure the model comparison in Session 2.
- Graph Analytics: Network relationships between accounts, devices and counterparties underpin fraud ring detection in Session 3.
- ISO/IEC 42001: Its AI management system requirements shape model governance and validation controls in Session 4.

Intended Participants

- Leaders accountable for fraud losses and fraud risk management programmes.
- Heads of financial crime who oversee transaction monitoring and alert operations.
- Senior risk, compliance and model risk leaders who approve detection models.
- Internal audit leaders who assure the effectiveness of anti-fraud controls.
- Payments and digital channel leaders balancing fraud control with customer experience.



The programme serves fraud, financial crime, risk, audit and payments functions in banking, insurance, telecommunications and government revenue agencies.

Learning Outcomes

1. Participants will be able to diagnose gaps in current fraud detection against the fraud risk management principles.
2. Participants will be able to evaluate supervised and anomaly detection models for a given fraud typology.
3. Participants will be able to design real-time scoring and alert prioritisation that reduces false positives.
4. Participants will be able to apply network analytics to identify linked accounts and organised schemes.
5. Participants will be able to construct validation and explainability requirements for fraud models.
6. Participants will be able to justify an AI fraud detection roadmap to senior management.

Programme Structure

Day 1: Fraud Risk Governance and AI Opportunity

Where does current fraud detection fall short, and where can AI help?

- COSO/ACFE Fraud Risk Management Guide Principles
- Fraud Typologies Across Payments, Lending and Claims
- Rule-Based Detection Performance Review
- Fraud Data Sources: Transactions, Devices and Customer Behaviour
- AI Detection Use-Case Map and Maturity Assessment

Day 2: Detection Models for AI-Driven Fraud Analytics

Which modelling approaches detect known and emerging fraud most reliably?

- Supervised Classification Using Labelled Fraud Cases
- Unsupervised Anomaly Detection for New Schemes
- Behavioural Profiling and Feature Design
- Class Imbalance, Label Quality and Feedback Loops
- Precision, Recall and Cost-Weighted Model Comparison

Day 3: Real-Time Monitoring and Network Analytics

How are risky transactions stopped in time and fraud rings exposed?



- Real-Time Transaction Scoring Architecture
- Risk-Based Alert Thresholds and Queue Prioritisation
- Graph Analytics for Linked Accounts and Mule Networks
- Customer Friction and Step-Up Authentication Decisions
- Case Management Integration and Analyst Feedback

Day 4: Model Validation, Explainability and Governance

Can each fraud model be trusted, explained and defended?

- ISO/IEC 42001 Controls for Fraud Detection Models
- Independent Model Validation and Back-Testing
- Explainability of Alerts for Analysts and Customers
- Model Drift Monitoring and Adversarial Adaptation
- Data Privacy and Fairness in Fraud Decisions

Day 5: Applying AI-Driven Fraud Analytics

Is the fraud detection roadmap ready for senior management approval?

- Closing Day 1 Detection Gaps With Selected Models
- Setting Day 3 Thresholds for the Chosen Channel
- Embedding Day 4 Validation in the Model Lifecycle
- Operating Model, Skills and Analyst Workflow Design
- Completing the AI Fraud Detection Roadmap

Methodology

The programme combines data workshops with case analysis. Participants compare rule-based and model-based alerts on sample transaction data, trace a fraud ring through a network graph and draft validation requirements. Cases are drawn from card payments, insurance claims and telecommunications subscription fraud.

- Suggested activity: Comparing false positive rates of rules and a scoring model on the same data.
- Suggested activity: Mapping a mule account network from transaction links.
- Suggested activity: Writing an alert explanation an analyst can act on.

Capstone Output

Each participant completes an AI fraud detection roadmap for one product or channel. It contains a gap assessment, selected models, threshold and alert design, validation and explainability requirements and an operating model. It is presented to senior management as the basis for the next detection investment.



Frequently Asked Questions

Is AI-driven fraud analytics training suitable for senior fraud and risk leaders?

Yes. It is set at advanced level for leaders who own fraud losses or model approval, and assumes no programming background.

Which frameworks does the AI-driven fraud analytics programme rest on?

It rests on the COSO/ACFE Fraud Risk Management Guide, supervised and unsupervised learning, graph analytics and ISO/IEC 42001.

How is the roadmap from AI-driven fraud analytics training used at work?

You can use it to prioritise detection investment, set alert thresholds and agree validation rules with model risk and audit.

How does AI-driven fraud analytics differ from a fraud investigation programme?

It focuses on detecting fraud with models and real-time monitoring, while investigation programmes address evidence gathering and interviews after fraud is suspected.