



AI Applications in Open Banking and Embedded Finance Course

9 – 13 August 2027
Kuala Lumpur

AI Applications in Open Banking and Embedded Finance Course

Ref: 282_124051 **Date:** 9 – 13 August 2027 **Location:** Kuala Lumpur **Fees:** 5200 Euro

Overview

AI Applications in Open Banking and Embedded Finance Course is a five-day foundation course for open-banking product managers, finance leaders, partnership teams, risk teams, and digital-finance transformation professionals, who leave with an AI-Enabled Open Banking Use-Case and Control Blueprint. Participants map ecosystem roles, consent journeys, transaction evidence, cash-flow insights, personalization, partner risk, fraud signals, human review, governance, and value measures. Agile Leaders Training Center provides training in AI applications for open banking and embedded finance.

Who Should Attend

- Open-banking product teams responsible for services and customer journeys
- Finance teams responsible for transaction and cash-flow insights
- Partnership teams responsible for ecosystem roles and service handoffs
- Risk teams responsible for consent, fraud, third-party, and model oversight
- Data teams responsible for permitted access and evidence quality
- Transformation leaders responsible for adoption and ecosystem value

The course assumes participants contribute to open-banking, embedded-finance, product, partnership, risk, or transformation decisions and leaves out coding, API development, model construction, technical integration, and vendor-product administration.

Departments and Industries

The course supports governed AI applications across open-banking and embedded-finance ecosystems.

- Retail and commercial banking product functions
- Payments, lending, and cash-management teams
- Digital-finance and embedded-finance providers
- Data, risk, fraud, compliance, and internal-control teams
- Retail, accounting, and business-platform partners
- Cooperative finance and financial-inclusion providers

Learning Objectives

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



- Analyze ecosystem roles, journeys, consent, and data flows
- Evaluate transaction and cash-flow evidence for AI use cases
- Design personalization and decision-support boundaries
- Apply partner, fraud, privacy, and governance controls
- Build adoption and ecosystem-value measures
- Create an open-banking use-case and control blueprint

Course Agenda

Day 1: Ecosystem and Consent Context

- Open-Banking Participant and Value Exchange Map
- Customer Consent and Service Journey Canvas
- Data Purpose, Permission, and Minimization Register
- Participant Handoff and Accountability Matrix
- AI Open-Banking Use-Case Framing Template

Day 2: Transaction and Cash-Flow Insights

- Account and Transaction Data Evidence Inventory
- Transaction Classification and Merchant Pattern Tree
- Cash-Flow Variability and Affordability Signal Sheet
- Data Quality, Freshness, and Missingness Checklist
- Insight Confidence and Human Review Decision Table

Day 3: Customer and Partner Applications

- Customer Need and Financial Context Map
- Personalization, Suitability, and Explanation Matrix
- Embedded-Finance Journey and Service Blueprint
- Partner Dependency and Third-Party Risk Register
- Customer Outcome and Ecosystem Value Scorecard

Day 4: Fraud and Responsible Controls

- Transaction Anomaly and Fraud Signal Library
- Alert, Investigation, and Escalation Workflow
- NIST AI RMF Open-Finance Risk Canvas
- Privacy, Fairness, Human Oversight, and Appeal Checklist
- Open-Banking AI Monitoring and Incident Dashboard



Day 5: Open-Banking Blueprint Practice

- Suggested Exercise: Map Participants and Consent Journeys
- Suggested Exercise: Build Transaction and Cash-Flow Insights
- Suggested Exercise: Design Customer and Partner Applications
- Suggested Exercise: Define Fraud and Responsible Controls
- Capstone Exercise: AI-Enabled Open Banking Use-Case and Control Blueprint

Practical Exercises

The course uses suggested activities that turn ecosystem and transaction evidence into governed AI decisions.

- Suggested activity: map participants, value exchange, customer consent, data purposes, handoffs, and accountability
- Suggested activity: classify transactions, assess cash-flow signals, test data quality, and record confidence
- Suggested activity: design personalization and embedded-finance journeys, review partners, and define outcomes
- Suggested activity: map fraud signals, set human oversight, define incidents, and build the blueprint

FAQs

Who suits AI in open banking and embedded finance training?

AI in open banking and embedded finance training suits product, finance, partnership, risk, fraud, data, and transformation teams. It assumes ecosystem decision experience and requires no coding or API development.

How does open-banking AI differ from general banking AI training?

Open-banking AI focuses on consented data exchange, participant handoffs, transaction insights, embedded journeys, partner dependencies, and ecosystem controls. General banking AI covers a wider range of internal customer, operations, fraud, credit, and governance applications.

How can teams use transaction data responsibly for AI insights?

Teams should define purpose, permission, minimization, ownership, quality, retention, access, confidence, customer explanation, human review, monitoring, and withdrawal of consent before using transaction data.

What risks require controls in AI-enabled open banking?

Controls should address consent failure, excess data use, poor transaction classification, unsuitable personalization, partner dependency, fraud, bias, privacy, weak explanation, unsupported decisions, service interruption, and unclear accountability.



What belongs in an AI-Enabled Open Banking Use-Case and Control Blueprint?

The blueprint includes participants, journeys, consent, data flows, use cases, transaction signals, decision boundaries, partners, risks, controls, owners, measures, monitoring, incidents, and review decisions.

Conclusion

Participants take back an AI-Enabled Open Banking Use-Case and Control Blueprint connecting ecosystem roles, consent, transaction evidence, customer applications, partner risk, and value. The blueprint makes permissions, handoffs, human review, controls, ownership, and monitoring visible across participants. It supports responsible ecosystem decisions while retaining customer control and accountable judgment.