



Open Banking API Integration and Operations Course

2 – 6 May 2027
Muscat

Open Banking API Integration and Operations Course

Ref: 451_136365 **Date:** 2 – 6 May 2027 **Location:** Muscat **Fees:** 5700 Euro

Overview

Open Banking API Integration and Operations Course is a five-day intermediate course for product, integration, architecture, technology, operations, risk, compliance, and partnership professionals, who leave with an Open Banking Integration Blueprint. The course connects ecosystem roles, consent journeys, API specifications, security profiles, partner onboarding, data standards, sandbox testing, integration patterns, monitoring, incidents, versioning, resilience, and governance. Agile Leaders Training Center delivers practical open banking API integration training.

Who Should Attend

- Product functions responsible for open-banking services and customer journeys
- Integration and architecture functions responsible for interface patterns and dependencies
- Technology operations functions responsible for API service performance and change
- Risk and compliance functions responsible for consent, data, security, and third-party controls
- Partnership functions responsible for onboarding and managing external providers
- Assurance functions responsible for testing evidence and operational governance

The course assumes participants already support digital banking, interfaces, products, operations, risk, or partnerships and leaves out software coding labs, vendor certification, AI use-case design, and jurisdiction-specific legal advice.

Departments and Industries

The course supports departments that design, integrate, operate, control, or assure open-banking services across financial and technology ecosystems.

- Digital banking, payments, product, and customer-experience teams
- Integration architecture, technology operations, and service-management functions
- Risk, compliance, privacy, cybersecurity, and internal-audit departments
- Banks, payment institutions, financial-technology providers, and data platforms
- Accounting, retail, marketplace, and business-software partners
- Third-party provider, vendor-management, and ecosystem partnership functions

Learning Objectives

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



- Apply an open-banking ecosystem and accountability model
- Build consent, authorization, and data-flow journeys
- Evaluate API specifications, security profiles, and integration patterns
- Use sandbox, conformance, and service-acceptance controls
- Analyze monitoring, incident, versioning, and resilience evidence
- Build an Open Banking Integration Blueprint

Course Agenda

Day 1: Ecosystem, Consent and Accountability

- Open-Banking Participant and Value-Exchange Map
- Customer Consent and Authorization Journey
- Data Purpose and Permission Register
- Third-Party Role and Accountability Matrix
- Customer Experience and Transparency Checklist

Day 2: API Specifications and Security

- API Resource and Endpoint Inventory
- Request, Response, and Error Model
- Financial-Grade API Security Profile Map
- Identity, Certificate, and Access Control Flow
- Data Schema and Semantic Consistency Matrix

Day 3: Integration, Onboarding and Testing

- API Gateway and Integration Pattern Canvas
- Third-Party Onboarding and Registration Workflow
- Sandbox Test Scenario Catalogue
- Conformance and Acceptance Evidence Pack
- Dependency, Environment, and Release Readiness Checklist

Day 4: Operations, Change and Resilience

- API Service-Level and Performance Dashboard
- Monitoring, Logging, and Traceability Standard
- Incident, Escalation, and Customer Impact Playbook
- API Versioning and Change-Control Register
- Continuity, Recovery, and Dependency Scenario Map



Day 5: Open Banking Integration Practice

- Suggested Exercise: Ecosystem and Consent Journey Review
- Suggested Exercise: API and Security Profile Assessment
- Suggested Exercise: Onboarding and Sandbox Test Design
- Suggested Exercise: Incident and Version Change Decision
- Capstone Exercise: Open Banking Integration Blueprint

Practical Exercises

The course uses suggested activities to connect customer journeys, interface evidence, partner controls, and operating decisions.

- Suggested activity: map participants, consent, permissions, data flows, customer communication, and accountability.
- Suggested activity: review an API resource model, security flow, data schema, and error response against stated requirements.
- Suggested activity: design onboarding, sandbox, conformance, acceptance, and release-readiness evidence for a partner.
- Suggested activity: assemble monitoring, incidents, changes, resilience actions, owners, and measures into the capstone blueprint.

FAQs

Who suits open banking API integration training, and what does it assume?

Open banking API integration training suits professionals who already support digital banking, interfaces, products, operations, controls, or partnerships and need an end-to-end implementation method.

How does open banking API integration differ from open-banking AI training?

Open banking API integration focuses on interfaces, consent, security, onboarding, testing, operations, and resilience, while open-banking AI training applies transaction data to governed analytical and decision-support use cases.

What belongs in an open-banking consent journey?

An open-banking consent journey should define the customer purpose, requested data or service, authorization steps, duration, status, withdrawal, communication, records, exceptions, and accountable participants.



How should open-banking APIs be tested before release?

Open-banking APIs should be tested against specifications, security flows, schemas, validation rules, positive and negative scenarios, errors, performance, conformance expectations, customer journeys, and operational acceptance criteria.

How are open-banking API changes controlled?

Open-banking API changes are controlled through version policy, impact analysis, stakeholder notice, backward-compatibility decisions, sandbox availability, regression evidence, release approval, monitoring, and retirement planning.

Conclusion

Participants take back an Open Banking Integration Blueprint containing ecosystem maps, consent journeys, interface inventories, security flows, onboarding controls, test evidence, dashboards, incident playbooks, and change records. The blueprint changes disconnected technical and operational tasks into a traceable service lifecycle. It supports controlled integrations, accountable partners, reliable operations, and reviewable customer outcomes.