JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Open Banking Interface Integration and Partner Onboarding Training Course

9 – 13 May 2027
Kuala Lumpur

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Open Banking Interface Integration and Partner Onboarding Training Course

Ref: 2707_103342 **Date:** 9 – 13 May 2027 **Location:** Kuala Lumpur **Fees:** 4600 GBP

Open Banking Interface Integration and Partner Onboarding is a 1-week training course for bank product, technology and partnership staff who leave with a partner integration plan for one open banking use case. Banks now compete through the partners they admit, so consent, security and onboarding speed shape trust. Jupiter Prime Training delivers this course on Open Banking Interface Integration and Partner Onboarding.

Why Open Banking Interface Integration and Partner Onboarding Matters Now

Three forces shape open banking integration today. Customers expect to share account information and start payments inside the apps they already use. Third-party providers arrive in growing numbers, each needing credentials, testing and contract terms. Security teams expect every connection to prove who is calling and what the customer agreed to. A bank that onboards partners cleanly gains distribution; one that handles consent loosely invites fraud and outages. The course rests on token-based authorisation and structured partner due diligence.

Who Gains Most from Open Banking Interface Integration and Partner Onboarding

- Product owners who decide which journeys a bank opens to partners
- Integration engineers who build, document and version the interfaces third parties call
- Partnership leads who negotiate terms, screen providers and manage the onboarding pipeline
- Information security specialists who set authentication, certificate and token rules
- Operations and support staff who monitor live connections and handle partner incidents

The greatest gain comes when a product owner, an engineer and a partnership lead from one bank attend together.

Open Banking Interface Integration and Partner Onboarding Capabilities

Participants learn to steer a partner from first contact to live traffic.

- Assess which account information and payment initiation journeys suit partner access — product roadmap committee
- Design customer consent journeys with clear scope, duration and revocation — customer experience owners
- Specify interface contracts, versioning rules and error responses — integration engineers and partners
- Apply token, certificate and strong customer authentication controls to each connection — security approvers
- Build a third-party onboarding checklist with due diligence and go-live criteria — partnership board
- Test partner integrations against functional, security and performance scenarios — release decision makers

Key Open Banking Interface Integration and Partner Onboarding Terms

- Account information service — a permitted service that reads a customer's balances and transactions, with consent.
- Payment initiation service — a service that starts a payment from a customer's bank account on the customer's instruction.
- Consent object — the stored record of what a customer authorised, for which provider and until when.
- Access token — a short-lived credential that lets a partner call specific endpoints for one customer.
- Developer sandbox — an isolated test environment with sample accounts where partners build before reaching live data.
- Mutual certificate authentication — a check in which bank and partner each present digital certificates.

Open Banking Interface Integration and Partner Onboarding Day by Day

Day 1: The Open Banking Ecosystem and Its Roles

- Ecosystem Role Map — Positioning the Bank, Providers and Aggregators
- Account Information Versus Payment Initiation — Choosing the First Opened Journey
- Partner Business Models — Pricing Access and Sharing Revenue With Providers
- Customer Trust Drivers — Weighing Convenience Against Data Sharing Concerns
- Use Case Shortlist — Selecting One Journey for the Integration Plan

Day 2: Designing Consent and Customer Journeys

- Consent Scope and Duration Model — Limiting What Partners May Read or Initiate
- Redirect and Decoupled Authentication Flows — Balancing Friction and Fraud Exposure
- Consent Dashboard Design — Letting Customers Review and Revoke Permissions
- Payment Confirmation Screens — Reducing Disputed Transactions
- Journey Testing With Customer Panels — Refining Wording and Step Order

Day 3: Interface Design and Connection Security

- Resource and Endpoint Modelling — Structuring Accounts, Transactions and Payments Calls
- Versioning and Deprecation Policy — Protecting Partners From Breaking Changes
- Token Lifecycle and Scopes — Controlling Access Time and Permitted Actions
- Certificate Management and Key Rotation — Sustaining Trusted Partner Connections
- Rate Limiting and Anomaly Monitoring — Detecting Abuse Before Customers Notice

Day 4: Third-Party Onboarding and Integration Testing

- Provider Due Diligence Questionnaire — Screening Ownership, Security and Financial Standing
- Partner Agreement Clauses — Allocating Liability, Service Levels and Exit Terms
- Sandbox Access and Test Data — Accelerating Partner Build Without Live Exposure
- Conformance and Security Test Suites — Approving Partners for Production Traffic
- Go-Live Readiness Review — Confirming Monitoring, Support Routes and Rollback Steps

Day 5: Practising the Partner Integration Plan

- Applying the Role Map — Naming Owners for Each Integration Stage
- Applying the Consent Model — Fixing Scope and Expiry for the Chosen Journey
- Applying Security Controls — Matching Tokens and Certificates to Partner Risk
- Partner Incident Playbook — Coordinating Outages and Suspected Fraud With Providers
- Partner Integration Plan Presentation — Securing Sign-Off From Product and Security Leads

Applying Open Banking Interface Integration and Partner Onboarding After the Course

- Run a consent journey review of one partner flow against the consent model.
- Lead an onboarding retrospective that rebuilds the due diligence and go-live checklist.

Open Banking Interface Integration and Partner Onboarding Questions FAQ

What is Open Banking Interface Integration and Partner Onboarding and why does it matter now?

It is the work of opening bank accounts and payments to approved third parties through secure interfaces. It matters now because customers expect to use bank services inside partner applications, and each connection must protect consent and identity.

Which roles gain most from Open Banking Interface Integration and Partner Onboarding?

Product owners, integration engineers, partnership leads, security specialists and operations staff gain most. Each shapes a different stage, from choosing the journey to supporting live connections.

How does Open Banking Interface Integration and Partner Onboarding differ from a course on digital banking strategy?

This course covers building and securing partner connections, not setting the overall direction of a digital bank. You work on consent design, interface contracts, provider screening and testing.

What do you bring back from Open Banking Interface Integration and Partner Onboarding?

You bring back a partner integration plan for one use case. It sets out the journey, consent rules, security controls, onboarding checks and go-live criteria.

Open Banking Interface Integration and Partner Onboarding: The Way Forward

The partner integration plan first informs which journey the bank opens next. Product owners use it to set scope, engineers to schedule interface work and partnership leads to run onboarding. After the first partner goes live, revisit the consent and monitoring sections, as real partner traffic reveals gaps in the original design.