



Advanced Digital Identity and Biometric Risk in Finance Training Course

7 – 11 December 2026
Kuala Lumpur



Advanced Digital Identity and Biometric Risk in Finance Training Course

Ref: 1113_182157 **Date:** 7 – 11 December 2026 **Location:** Kuala Lumpur **Fees:** 5200 Euro

Overview

Advanced Digital Identity and Biometric Risk in Finance Training Course is a one-week course for digital banking, identity, fraud, risk, compliance, cybersecurity, product, audit and payment professionals, who leave with a Digital Identity Control Assurance Pack. Participants apply digital identity risk assessment, biometric authentication governance, identity proofing controls, presentation attack detection and financial identity fraud monitoring to practical service decisions. Agile Leaders Training Center develops digital identity and biometric risk capability.

Who Should Attend

- Teams responsible for digital banking identity journeys and customer access
- Teams responsible for identity and access architecture and authenticator management
- Teams responsible for fraud detection, financial crime controls and investigations
- Teams responsible for risk, compliance, privacy and control assurance
- Teams responsible for cybersecurity, product governance and third-party oversight
- Teams responsible for audit evidence and payment operations

The course assumes participants can assess financial-service processes and control evidence, and it leaves out biometric algorithm development, legal advice and jurisdiction-specific interpretation.

Departments and Industries

The course supports departments and industries that design, operate or assure digital identity services.



- Banking, payments and financial technology
- Insurance, lending and wealth services
- Telecommunications and digital platforms
- Identity, cybersecurity and fraud operations
- Risk, compliance, privacy and internal audit
- Product management and technology procurement

Learning Objectives

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

- Analyze identity lifecycles and assurance requirements
- Evaluate proofing, biometric and authenticator controls
- Diagnose liveness and presentation-attack weaknesses
- Apply privacy, consent and inclusion safeguards
- Build vendor, fraud-monitoring and incident controls
- Prioritize governance findings and remediation actions



Course Agenda

Day 1: Identity Assurance Architecture

- Digital Identity Lifecycle and Trust-Boundary Map
- NIST SP 800-63 Assurance-Level Decision Method
- Identity Proofing Evidence and Attribute Matrix
- Authenticator Binding and Recovery Control Model
- Financial Service Identity Risk Register

Day 2: Proofing and Biometric Controls

- Remote Proofing Journey and Evidence Validation Map
- Biometric Modality Selection Decision Matrix
- False Acceptance and False Rejection Analysis
- Document and Subject Liveness Control Checklist
- Presentation Attack Detection Test Plan



Day 3: Privacy, Inclusion and Fraud

- Biometric Data Flow and Consent Map
- Data Minimization and Retention Decision Record
- Accessibility and Demographic Performance Test
- Financial Identity Fraud Scenario Library
- Deepfake and Injection Attack Response Playbook

Day 4: Vendor Assurance and Operations

- Biometric Vendor Due-Diligence Scorecard
- FIDO Biometric Certification Evidence Review
- Authentication Telemetry and Fraud Indicator Matrix
- Identity Incident Triage and Escalation Workflow
- Digital Identity Governance and Accountability Model

Day 5: Control Assurance Practice

- Exercise: Map an Account-Opening Identity Journey
- Exercise: Diagnose a Presentation Attack Case
- Exercise: Evaluate a Biometric Vendor Submission
- Exercise: Prioritize a Fraud and Privacy Incident
- Capstone Exercise: Digital Identity Control Assurance Pack

Practical Exercises

The course uses suggested activities to convert identity evidence into financial-service control decisions.

- Suggested activity: assign assurance levels and controls to customer journeys
- Suggested activity: test biometric performance, liveness and fallback scenarios
- Suggested activity: score vendor evidence against risk and inclusion criteria
- Suggested activity: present a prioritized control-remediation decision

FAQs

Who suits digital identity and biometric risk training, and what does it assume?

Digital banking, identity, fraud, risk, compliance, cybersecurity, product, audit and payment professionals suit the training. It assumes experience assessing processes, risks or control evidence.

How does digital identity and biometric risk training differ from cybersecurity fundamentals training?

Digital identity and biometric risk training focuses on proofing, authenticators, biometric performance, fraud, privacy and governance; cybersecurity fundamentals training usually surveys a broader range of threats and safeguards.

What should biometric authentication governance evaluate?

Biometric authentication governance should evaluate purpose, assurance needs, performance, presentation attacks, fallback routes, consent, retention, accessibility, monitoring, vendor evidence and accountability.

How are presentation attacks controlled in financial identity services?

Presentation attacks are controlled through live capture, liveness checks, injection defenses, rate limits, device and transaction signals, human review, monitoring and tested escalation paths.

What evidence supports digital identity vendor assurance?

Vendor assurance uses architecture, test methods, performance results, attack-resistance evidence, data flows, subcontractor dependencies, change controls, incident history, accessibility results and operational monitoring commitments.



Conclusion

Participants take back a Digital Identity Control Assurance Pack containing journey maps, decision matrices, test plans, vendor scorecards and an incident playbook. The pack makes assurance, biometric, privacy and fraud decisions traceable. It supports consistent control reviews, vendor challenge and remediation reporting across financial services.