JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Biometric Authentication and Identity Verification Training Course

27 June – 1 July 2027
Kuala Lumpur

Biometric Authentication and Identity Verification Training Course

Ref: 2651_100917 **Date:** 27 June – 1 July 2027 **Location:** Kuala Lumpur **Fees:** 4600 GBP

Biometric Authentication and Identity Verification is a 1-week training course for finance operations, payments and fraud control staff who decide how customers prove who they are, from first onboarding to every later login and payment approval. Participants build a customer authentication control map. Impersonation attacks and synthetic identities now reach every finance function that releases money, and Jupiter Prime Training runs this course for the teams who own those controls.

Why Biometric Authentication and Identity Verification Matters Now

Customers expect to open accounts and approve payments by phone, so branch checks have moved into selfie capture and document scanning. Fraud groups answer with face-swap video, masks and synthetic identities. Auditors and data protection officers ask finance teams to show each control is proportionate to its risk. An organisation that balances friction, fraud loss and privacy keeps genuine customers moving; one that does not pays twice, in chargebacks and abandoned sign-ups. The course rests on risk-based assurance levels and layered authentication factors.

Who Gains Most from Biometric Authentication and Identity Verification

- Payments operations staff who release, hold or recall customer and supplier transfers
- Fraud control analysts who investigate account takeover and first-party fraud cases
- Customer onboarding specialists who approve, refer or decline new applications
- Finance controllers who own the cost and loss lines tied to authentication
- Internal control and audit staff who test identity checks against stated risk appetite

The greatest gain comes when onboarding, payments and fraud staff from one finance function attend together.

Biometric Authentication and Identity Verification Capabilities

Each identity check is judged by the evidence it collects, the attack it resists and the cost it adds.

- Assess document, face, fingerprint and voice checks against likely presentation attacks — the onboarding approval policy
- Specify liveness and matching thresholds for each customer journey — the balance between false rejects and fraud loss
- Design step-up authentication rules for high-value transfers and changes to payee details — payments release decisions
- Calculate the cost of an authentication method per customer, per payment and per prevented loss — the finance controller
- Test identity controls with sample attack cases and exception records — internal audit and risk owners
- Communicate privacy, consent and template storage choices in plain terms — customers and data protection officers

Key Biometric Authentication and Identity Verification Terms

- Identity proofing — collecting and checking evidence that an applicant is a real person matching the claimed identity.
- Liveness detection — a check that a biometric sample comes from a live person, not a photo, mask or recording.
- Presentation attack — an attempt to fool a biometric sensor with an artefact such as a printed face, replayed video or silicone fingerprint.
- False acceptance rate — the share of impostor attempts a biometric system wrongly accepts as a genuine match.
- Step-up authentication — an extra identity check triggered only when a transaction or account change carries higher risk.
- Synthetic identity — a fabricated identity mixing real and invented personal details to open accounts.

Biometric Authentication and Identity Verification Day by Day

Day 1: Identity Risk Across the Finance Journey

- Customer Journey Mapping — Where Identity Is Claimed, Checked and Trusted
- Identity Fraud Typology — Impersonation, Account Takeover and Synthetic Identities
- Assurance Levels — Matching Evidence Strength to Transaction Value
- Authentication Factor Types — Knowledge, Possession and Inherence Compared
- Loss Event Records — Reading Past Fraud Cases for Control Gaps

Day 2: Verifying Documents and Faces at Onboarding

- Identity Document Checks — Security Features, Chip Reading and Tamper Signs
- Face Matching — Comparing Selfie Captures Against Document Photos
- Active and Passive Liveness Checks — Resisting Masks, Replays and Deepfakes
- Data Source Corroboration — Address, Phone and Device Signals
- Referral Queues — Manual Review Rules for Borderline Applicants

Day 3: Authenticating Logins and Payments

- Fingerprint, Face and Voice Login — Choosing Methods by Channel and Customer Group
- Matching Thresholds — Trading False Rejects Against False Accepts
- Step-Up Rules — Payee Changes, Large Transfers and New Devices
- Behavioural Signals — Typing Rhythm, Device Handling and Session Anomalies
- Account Recovery Controls — Closing the Reset Route Fraudsters Prefer

Day 4: Cost, Privacy and Control Evidence

- Authentication Cost Model — Vendor Fees, Drop-Off and Prevented Losses
- Biometric Template Storage — On-Device Versus Central Matching Choices
- Consent and Data Minimisation Notes — Customer Trust and Privacy Duties
- Control Testing Packs — Sample Attacks, Exception Logs and Results
- Key Risk Indicators — Pass Rates, Referral Rates and Fraud Losses

Day 5: Practising the Customer Authentication Control Map

- Journey Risk Scoring — Applying Assurance Levels to Each Touchpoint
- Method Selection Matrix — Applying Liveness and Matching Choices
- Step-Up and Recovery Rules — Applying Payment and Reset Controls
- Cost and Indicator Summary — Applying the Cost Model to Each Control
- Customer Authentication Control Map — Owners, Evidence and Review Dates

Applying Biometric Authentication and Identity Verification After the Course

- Run a liveness and face matching test on twenty recent onboarding referrals.
- Review step-up rules for payee changes and large transfers and agree new thresholds backed by the cost model.

Biometric Authentication and Identity Verification Questions FAQ

What is Biometric Authentication and Identity Verification and why does it matter now?

It is the discipline of proving a customer is real and present before money moves. It matters now because face-swap video and synthetic identities defeat old document and password checks.

Which roles gain most from Biometric Authentication and Identity Verification?

Payments, fraud control, onboarding, finance control and internal audit staff gain most, because each approves, tests or pays for an identity check.

How does Biometric Authentication and Identity Verification differ from a general fraud investigation course?

It focuses on preventing impersonation at the point of onboarding, login and payment, rather than investigating losses afterwards.

What do you bring back from Biometric Authentication and Identity Verification?

You bring back a control map for your own customer journeys. It shows where identity is checked, which method applies, who owns it and what it costs.

Biometric Authentication and Identity Verification: The Way Forward

The customer authentication control map first informs where step-up checks sit on payee changes and large transfers. Payments, fraud and onboarding leads use it to agree owners and thresholds, and controllers use it to track cost against prevented loss. After its first quarterly review, revisit the balance between customer drop-off and fraud attempts stopped, since attack methods shift faster than policies.