Secure Payment Systems in Banking Training Course

Professional Development Training Course Outline

Category	Banking Institute	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s rapidly evolving digital banking ecosystem, secure payment systems have become a critical pillar for financial stability, fraud prevention, and customer trust. With the rise of real-time payments, mobile banking, fintech integration, blockchain technology, and open banking APIs, financial institutions must adopt robust cybersecurity frameworks, encryption standards, and regulatory compliance strategies to safeguard transactions. Secure Payment Systems in Banking Training Course is designed to equip banking professionals with cutting-edge knowledge in secure payment architectures, payment gateway security, fraud detection systems, and data protection mechanisms, ensuring resilience against emerging cyber threats.

As global payment infrastructures shift toward cashless economies, instant cross-border transactions, and digital wallets, banks face increasing risks from cyberattacks, phishing, identity theft, and payment fraud schemes. This comprehensive training provides deep insights into PCI DSS compliance, ISO 20022 standards, tokenization, biometric authentication, AI-driven fraud analytics, and risk management frameworks. Participants will gain practical expertise through real-world case studies, enabling them to design and implement secure, scalable, and compliant payment systems that enhance operational efficiency and customer confidence.

Programme Curriculum

Secure Payment Systems in Banking Training Course

Introduction

In today’s rapidly evolving digital banking ecosystem, secure payment systems have become a critical pillar for financial stability, fraud prevention, and customer trust. With the rise of real-time payments, mobile banking, fintech integration, blockchain technology, and open banking APIs, financial institutions must adopt robust

cybersecurity frameworks, encryption standards, and regulatory compliance strategies to safeguard transactions. Secure Payment Systems in Banking Training Course is designed to equip banking professionals with cutting-edge knowledge in secure payment architectures, payment gateway security, fraud detection systems, and data protection mechanisms, ensuring resilience against emerging cyber threats.

As global payment infrastructures shift toward cashless economies, instant cross-border transactions, and digital wallets, banks face increasing risks from cyberattacks, phishing, identity theft, and payment fraud schemes. This comprehensive training provides deep insights into PCI DSS compliance, ISO 20022 standards, tokenization, biometric authentication, AI-driven fraud analytics, and risk management frameworks. Participants will gain practical expertise through real-world case studies, enabling them to design and implement secure, scalable, and compliant payment systems that enhance operational efficiency and customer confidence.

Course Duration

10 days

Course Objectives

1. Understand secure payment system architecture and digital transaction flows
2. Analyze emerging cyber threats in banking payment systems
3. Implement advanced fraud detection and prevention strategies using AI/ML
4. Apply PCI DSS, ISO 20022, and global regulatory compliance frameworks
5. Design end-to-end encryption and tokenization solutions
6. Strengthen authentication mechanisms including biometrics and MFA
7. Evaluate real-time payment security and instant settlement risks
8. Develop risk management and incident response frameworks
9. Integrate secure APIs and open banking protocols
10. Enhance data privacy and protection using GDPR-aligned strategies
11. Leverage blockchain and distributed ledger technologies for secure payments
12. Optimize payment gateway security and transaction monitoring systems
13. Build cyber resilience and secure digital banking ecosystems

Target Audience

1. Banking and Financial Institution Professionals
2. Payment Systems Managers and Analysts
3. Cybersecurity and Information Security Officers
4. Risk and Compliance Managers
5. Fintech and Digital Banking Specialists
6. IT and Systems Architects in Banking
7. Fraud Detection and Prevention Teams
8. Regulators and Financial Consultants

Training Modules

Module 1: Overview of Payment Systems

- Evolution of digital payment systems
- Types of payment infrastructures
- Payment ecosystem stakeholders
- Transaction lifecycle and flows

- Case Study: Transition to real-time payments in retail banking

Module 2: Payment System Architecture

- Core banking integration
- Payment gateways and processors
- Switching systems
- Cloud-based payment systems
- Case Study: Scalable payment architecture implementation

Module 3: Cybersecurity in Payments

- Common payment system vulnerabilities
- Cyberattack vectors and threats
- Malware and phishing attacks
- Insider threats
- Case Study: Major banking cyberattack analysis

Module 4: Fraud Detection & Prevention

- Fraud typologies in banking
- AI/ML-based fraud analytics
- Transaction monitoring tools
- Behavioral analytics
- Case Study: Real-time fraud detection system success

Module 5: Regulatory Compliance

- PCI DSS standards
- ISO 20022 framework
- AML/KYC requirements
- Regulatory bodies and guidelines
- Case Study: Compliance failure and penalties

Module 6: Encryption & Tokenization

- Data encryption techniques
- Tokenization frameworks
- Key management systems
- Secure data transmission
- Case Study: Tokenization reducing fraud risk

Module 7: Authentication Mechanisms

- Multi-factor authentication (MFA)
- Biometric verification
- Digital identity management
- Authentication protocols
- Case Study: Biometric authentication in mobile banking

Module 8: Real-Time Payments Security

- Instant payment systems risks

- Settlement security
- Transaction validation
- Fraud in real-time payments
- Case Study: Secure RTP implementation

Module 9: API Security & Open Banking

- Open banking frameworks
- API vulnerabilities
- Secure API gateways
- Data sharing risks
- Case Study: Open banking breach incident

Module 10: Blockchain in Payments

- Blockchain fundamentals
- Smart contracts
- Distributed ledger security
- Cryptographic validation
- Case Study: Blockchain-based cross-border payments

Module 11: Risk Management

- Risk assessment models
- Payment risk indicators
- Mitigation strategies
- Risk monitoring tools
- Case Study: Enterprise risk management in payments

Module 12: Data Privacy & Protection

- GDPR and data protection
- Customer data security
- Data breach management
- Privacy frameworks
- Case Study: Data breach response strategy

Module 13: Payment Gateway Security

- Gateway vulnerabilities
- Secure transaction processing
- Payment routing
- Third-party risks
- Case Study: Payment gateway breach

Module 14: Incident Response & Recovery

- Incident response planning
- Cyberattack containment
- Disaster recovery strategies
- Business continuity planning
- Case Study: Banking system recovery after attack

Module 15: Future Trends in Secure Payments

- AI-driven security innovations
- Quantum cryptography
- Digital currencies (CBDCs)
- Embedded finance
- Case Study: Future-ready payment system design

Training Methodology

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price

23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com