

Payment Terminal Cybersecurity, FinTech & Digital Payments Training

4 – 8 January 2027
London

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Payment Terminal Cybersecurity, FinTech & Digital Payments Training

Ref: 103600689_109131 **Date:** 4 – 8 January 2027 **Location:** London **Fees:** 5700 Euro

Course Overview:

The Payment Terminal Cybersecurity, FinTech & Digital Payments Training course develops the technical and operational capabilities required to secure modern card, POS, mobile, and digital payment environments. Participants explore payment terminals, merchants, acquirers, issuers, payment networks, gateways, APIs, FinTech platforms, mobile wallets, and contactless technologies. The course combines Payment Terminal Cybersecurity Training, POS Cybersecurity Training, Digital Payment Security Training, and FinTech Cybersecurity Training with practical payment risk management. Key areas include terminal physical and logical security, POS integration, communications security, encryption, key management, mobile payment threats, digital fraud, endpoint protection, payment gateway security, payment API security, operational resilience, and third-party dependencies. Participants will develop practical capabilities for strengthening Payment Terminal Security, Card and POS Security, Electronic Payment Security, and secure digital payment operations.

Target Audience:

- Payment Systems Managers and Specialists
- Payment Terminal and POS Administrators
- Cybersecurity Professionals
- Information Security Analysts
- FinTech Professionals
- Digital Banking Specialists
- Card Operations Managers
- Payment Operations Specialists
- Fraud Risk and Fraud Prevention Professionals
- IT Risk and Technology Risk Officers
- Payment Security Engineers
- Network and Infrastructure Security Professionals
- Merchant Acquiring Specialists
- Payment Gateway and API Teams
- Digital Wallet and Mobile Payment Teams
- Compliance and Payment Risk Professionals
- Business Continuity and Operational Resilience Professionals

AGILE LEADERS
Training Center

Targeted Organizational Departments:

- Payment Systems and Digital Payments
- Card Operations and Merchant Acquiring
- Information Security and Cybersecurity
- FinTech and Digital Banking
- IT Infrastructure and Network Security
- Fraud Prevention and Financial Crime
- Technology Risk and Operational Risk
- POS and Payment Terminal Management
- Payment Processing and Switching
- Digital Channels and Mobile Banking
- Payment Gateway and API Management
- Business Continuity and Operational Resilience
- Compliance and Payment Security
- Merchant Services

Targeted Industries:

- Banks and Financial Institutions
- FinTech Companies
- Payment Service Providers
- Card Issuers and Acquirers
- Payment Processing Companies
- Electronic Money Institutions
- Digital Banks
- Retail and E-Commerce
- Telecommunications and Mobile Payment Providers
- Payment Gateway Providers
- Merchant Service Providers
- Technology and Cloud Service Providers
- Government Payment Platforms
- Transportation and Smart Payment Systems
- Hospitality and High-Volume Retail Operations

Course Offerings:

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

- Map card, POS, mobile, contactless, gateway, and digital payment transaction flows.
- Explain the roles of merchants, acquirers, issuers, processors, payment networks, gateways, and FinTech providers.
- Evaluate Payment Terminal Security across physical, logical, integration, communications, and lifecycle domains.
- Identify terminal tampering, malware, unauthorized modification, insecure interfaces, and payment data exposure.
- Apply POS Risk Management and Payment Terminal Risk Management principles.
- Assess threats against card-present, card-not-present, mobile, and contactless payments.
- Examine POS malware, man-in-the-middle, replay, phishing, social engineering, and device compromise scenarios.
- Understand encryption, cryptographic keys, tokenization, PIN protection, and secure payment data handling.
- Evaluate Payment Gateway Security and Payment API Security exposure.
- Assess mobile wallets, NFC, QR, token-based payments, device authentication, and contactless technologies.
- Differentiate card-present, card-not-present, counterfeit, lost-and-stolen, and digital payment fraud.
- Develop Payment Fraud Prevention and Card Fraud Prevention controls.
- Evaluate third-party, cloud, telecommunications, processor, and technology-provider dependencies.
- Strengthen endpoint security, incident response, continuity, redundancy, and payment-system resilience.
- Develop layered security strategies for Secure Payment Systems and modern FinTech environments.

Training Methodology:

The course uses instructor-led sessions, payment-flow analysis, cybersecurity case studies, group exercises, threat-mapping activities, fraud scenarios, incident-response discussions, and interactive workshops. Participants examine POS terminal vulnerabilities, Digital Payment Cybersecurity, Card Payment Security, mobile wallet risks, Payment Gateway Security, Payment API Security, payment fraud, and FinTech cyber threats. Practical activities include identifying payment-system attack surfaces, assessing security controls, evaluating terminal risks, analyzing transaction flows, reviewing cyber incidents, and developing mitigation strategies. Group work strengthens decision-making around POS Risk Management, Payment Terminal Risk Management, third-party dependencies, operational resilience, and secure payment architecture. Reflection and feedback sessions reinforce the application of Payment Systems Security Training concepts to banking, FinTech, merchant acquiring, digital payments, and payment processing environments.

AGILE LEADERS
Training Center

Course Toolbox:

- Payment ecosystem and transaction-flow maps
- POS and payment terminal security review checklists
- Payment-terminal attack-surface mapping
- Physical and logical security control examples
- POS integration security considerations
- Payment communications and interface security checklists
- Payment terminal lifecycle risk framework
- Digital payment threat-model examples
- Mobile wallet threat-model templates
- Payment API and gateway risk-review examples
- Card fraud analysis matrices
- Payment fraud scenario library
- Cyber incident classification examples
- Third-party and critical service provider risk matrix
- Payment-system resilience checklist
- Business continuity and outage scenario templates
- Secure payment architecture review framework
- Payment cybersecurity risk register examples

Note: Commercial software, POS devices, cybersecurity platforms, payment systems, or licensed tools are not provided. The course provides professional insights and examples of tools, frameworks, checklists, and technologies relevant to the course.

AGILE LEADERS
Training Center

Course Agenda:

Day 1: FinTech, Digital Payments & Modern Payment Ecosystems

- **Topic 1:** FinTech Landscape, Digital Finance and the Evolution of Payments
- **Topic 2:** Digital Payment Ecosystem: Merchants, PSPs, Acquirers, Issuers and Networks
- **Topic 3:** Card Payment Processing: Authorization, Clearing and Settlement Flows
- **Topic 4:** Digital Payment Technology: Cards, POS, Wallets, QR and Contactless Payments
- **Topic 5:** Payment Gateways, Payment APIs and FinTech Integration Models
- **Topic 6:** Cybersecurity, Operational Risk and Trust in Secure Payment Systems
- **Reflection & Review:** Mapping FinTech and Digital Payment Security Dependencies

Day 2: Payment Terminal, POS & Card Security Architecture

- **Topic 1:** Payment Terminal Architecture and Point-of-Interaction Security
- **Topic 2:** Physical Security: Tampering, Device Modification and Sensitive Data Exposure
- **Topic 3:** Logical Security: Firmware, Applications, Authentication and Access Controls
- **Topic 4:** POS Terminal Integration and Secure Payment Components
- **Topic 5:** Payment Communications, Interfaces, Protocols and Network Exposure
- **Topic 6:** Terminal Lifecycle Security, Deployment, Key Loading and Device Management
- **Reflection & Review:** Evaluating Payment Terminal Security Across the Device Lifecycle

Day 3: Payment Terminal Cybersecurity & POS Threat Management

- **Topic 1:** Payment Terminal Cybersecurity Threat Landscape and Attack Surfaces
- **Topic 2:** POS Malware, Device Compromise and Unauthorized Terminal Modification
- **Topic 3:** Man-in-the-Middle, Replay and Payment Communication Attacks
- **Topic 4:** Payment Terminal Risk Management and POS Risk Management
- **Topic 5:** Secure Configuration, Access Control and Payment Endpoint Protection
- **Topic 6:** Detection, Monitoring and Response to Payment Terminal Security Incidents
- **Reflection & Review:** Building a Layered POS Cybersecurity Defense Model

AGILE LEADERS
Training Center

Day 4: Mobile, Contactless, Card & Digital Payment Security

- **Topic 1:** Mobile Payment Security and Digital Wallet Architecture
- **Topic 2:** NFC, QR and Contactless Payment Security
- **Topic 3:** Tokenization, Cryptograms and Protection of Cardholder Data
- **Topic 4:** User Authentication, Device Authentication and Secure Elements
- **Topic 5:** Card-Present vs. Card-Not-Present Fraud and Attack Patterns
- **Topic 6:** Payment Fraud Prevention and Card Fraud Prevention Strategies
- **Reflection & Review:** Connecting Card, Mobile and Contactless Payment Security Controls

Day 5: Payment Security Strategy, Resilience & Emerging Cyber Risks

- **Topic 1:** Payment Systems Cybersecurity Governance and Security Strategy
- **Topic 2:** Payment Gateway Security and Payment API Security
- **Topic 3:** Third-Party, Cloud and Critical Service Provider Risks
- **Topic 4:** Cyber Incident Response, Payment Outages and Operational Resilience
- **Topic 5:** Redundancy, Business Continuity and Alternative Payment Arrangements
- **Topic 6:** Emerging FinTech Threats, Digital Fraud and Future Payment Security
- **Reflection & Review:** Designing a Secure and Resilient Digital Payment Environment

FAQ:

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

No formal cybersecurity or payment-industry certification is required. Participants should ideally have practical exposure to banking, payments, IT, cybersecurity, FinTech, card operations, POS systems, fraud management, technology risk, merchant acquiring, or digital channels. Basic familiarity with electronic payments, computer networks, payment processing, or information security terminology is beneficial. Advanced programming or cryptographic expertise is not required.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day's session is generally structured to last around 4–5 hours, with breaks and interactive activities included. The total course duration spans one week, approximately 20–25 hours of instruction.

Is payment terminal cybersecurity the same as PCI DSS compliance?

No. Payment terminal cybersecurity covers terminal physical and logical security, POS integration, communications, mobile and contactless payments, fraud, gateways, APIs, endpoint protection, third-party risks, cyber incidents, and operational resilience. PCI-related requirements form an important part of payment security but do not represent the entire payment cybersecurity environment.

How This Course is Different from Other Payment Terminal Cybersecurity Courses:

Payment Terminal Cybersecurity, FinTech & Digital Payments Training integrates terminal cybersecurity, FinTech, card security, POS security, mobile payments, contactless technologies, payment fraud, gateways, APIs, and operational resilience within one corporate training program. Rather than treating POS Security Training or Payment Terminal Security Training as isolated technical subjects, the course follows the complete payment transaction ecosystem from customers and terminals through merchants, gateways, processors, acquirers, payment networks, and issuers. Participants address physical and logical terminal security, secure communications, mobile wallets, tokenization, card fraud, Payment Gateway Security, Payment API Security, third-party risk, cyber incidents, continuity, and resilience. This integrated approach connects technical cybersecurity controls with Digital Payment Security Training, FinTech Cybersecurity Training, Payment Fraud Prevention Training, Card Fraud Prevention Training, and Payment Systems Security Training for practical application across modern payment environments.