



Finance Workflow Cybersecurity and Payment Fraud Defense Training Course

30 November – 4 December 2026
Kuala Lumpur

Finance Workflow Cybersecurity and Payment Fraud Defense Training Course

Ref: 765_158187 **Date:** 30 November – 4 December 2026 **Location:** Kuala Lumpur **Fees:** 5200 Euro

Overview

Finance Workflow Cybersecurity and Payment Fraud Defense Training Course is a five-day intermediate course for finance managers, accountants, treasury staff, controllers, auditors, and operations professionals who leave with a Finance Cyber Control Pack. Participants examine business email compromise, account takeover, altered payment instructions, data exposure, and third-party access through finance-process controls, verification, evidence, and escalation. The course connects finance decisions with security and fraud teams. Agile Leaders Training Center develops finance workflow cybersecurity practice.

Who Should Attend

- Accounting functions responsible for invoices, journals, and financial records
- Treasury functions responsible for payments, bank access, and liquidity operations
- Controllershship functions responsible for approvals and financial controls
- Internal audit functions responsible for testing control design and evidence
- Financial operations functions responsible for suppliers and shared services
- Risk functions responsible for coordinating cyber and fraud concerns

The course assumes participants can follow finance workflows and approval rules, and leaves out security engineering, payment-terminal configuration, forensic investigation, and certification preparation.

Departments and Industries

The course supports departments and industries that process payments and financial information.

- Finance, accounting, treasury, and internal audit
- Procurement, shared services, risk, and compliance
- Financial services and digital commerce
- Healthcare, education, and professional services
- Energy, manufacturing, logistics, and telecommunications

Learning Objectives

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



- Analyze cyber risk across finance workflows
- Diagnose business email compromise and account-takeover signals
- Apply independent payment and supplier-change verification
- Evaluate financial-data and third-party access controls
- Build control evidence and incident escalation records
- Build a Finance Cyber Control Pack

Course Agenda

Day 1: Map Finance Cyber Risk

- Finance Workflow and Trust Boundary Map
- Cyber-Fraud Scenario Classification Matrix
- Payment and Journal Control Point Register
- Role Access and Segregation Review Sheet
- Finance Cyber Risk Ownership Map

Day 2: Detect Email and Account Compromise

- Business Email Compromise Signal Checklist
- Invoice Thread and Sender Validation Method
- Account Takeover Indicator Card
- Urgency and Authority Manipulation Pattern Guide
- Mailbox Change and Session Concern Log

Day 3: Verify Payments and Third Parties

- Independent Payment Verification Protocol
- Supplier Bank Detail Change Control Form
- Out-of-Band Contact Validation Record
- Payment Exception and Override Decision Tree
- Third-Party Finance Access Review Matrix

Day 4: Protect Data and Coordinate Response

- Financial Data Handling and Transfer Checklist
- Finance Control Evidence Index
- Suspicious Payment Hold Decision Card
- Cyber-Fraud Escalation and Handover Map
- Security and Fraud Team Coordination Log



Day 5: Practice Finance Cyber Defense

- Exercise: Trace a Compromised Invoice Workflow
- Exercise: Validate a Supplier Detail Change
- Exercise: Diagnose Account Takeover Signals
- Exercise: Hold, Escalate, and Document a Payment Concern
- Capstone: Finance Cyber Control Pack

Practical Exercises

The course uses suggested activities based on financial services, healthcare, manufacturing, and shared-service operations.

- Suggested activity: map a payment workflow and identify trust boundaries, access points, and control evidence.
- Suggested activity: inspect an invoice conversation for sender, urgency, instruction-change, and account-compromise signals.
- Suggested activity: validate a supplier bank-detail request through an independent contact route.
- Suggested activity: document a payment hold, escalation, evidence handover, and recovery coordination decision.

FAQs

Who suits finance workflow cybersecurity training, and what does it assume?

Finance managers, accountants, treasury staff, controllers, auditors, and operations professionals suit the training; it assumes familiarity with finance workflows and approval rules.

How does finance workflow cybersecurity differ from general cyber awareness training?

Finance workflow cybersecurity applies verification, access, evidence, and escalation controls to payments and financial data, while general awareness training focuses on everyday safe behavior across the workforce.

How should finance teams verify changed payment instructions?

Finance teams should pause processing, use an independently maintained contact route, confirm the authorized requester and account details, apply the required approvals, record evidence, and treat urgency or secrecy as a risk signal.



What evidence should finance cybersecurity controls retain?

Finance controls should retain the request source, validation route, approvers, timestamps, account-change evidence, exception reasoning, system records, escalation details, hold or release decision, and follow-up actions.

How should finance professionals escalate suspected payment fraud?

Finance professionals should hold the transaction when authorized, preserve the communication and workflow evidence, use the approved escalation route, alert security and fraud functions, and document each handover and decision.

Conclusion

Participants take back a Finance Cyber Control Pack connecting workflow maps, compromise signals, verification protocols, access reviews, evidence indexes, and escalation records. It changes isolated caution into repeatable finance controls. The pack supports consistent payment decisions, clearer coordination, traceable exceptions, and faster handling of suspected cyber-enabled fraud.