CONCEPT

Cybersecurity in Financial Services: Payment Controls and Bank Cyber Resilience

8 – 12 March 2027
Dubai - Five-star CBD venue



Cybersecurity in Financial Services: Payment Controls and Bank Cyber Resilience

Ref: 974_21957 **Date:** 8 – 12 March 2027 **Location:** Dubai - Five-star CBD venue **Fees:** 21450 SAR

Introduction:

Cybersecurity in financial services is the focus of this one-week course for security, IT risk, operational risk and compliance staff in banks, insurers and payment firms, who finish with a Cyber Resilience Assessment and Board Report for a case bank. Institutions lose money when payment fraud, authentication and card channel controls are assessed in isolation and reported without a quantified view of exposure. Nominees already own or review security controls, and the course is taught through case study on payment flows and loss scenarios. CoreConcept Training Center designed this course for mixed cohorts.

Course Objectives:

- Map the cyber threats facing banks, insurers and payment firms to critical business services and their impact tolerances
- Assess card, payment and interbank messaging environments against PCI DSS objectives and customer security control sets
- Specify payment verification, strong customer authentication and account takeover controls for digital, ATM and card channels
- Quantify cyber loss exposure with the FAIR model and scope threat-led resilience tests and scenario exercises
- Classify and report cyber incidents that disrupt financial services within supervisory and customer notification expectations
- Produce a Cyber Resilience Assessment and Board Report with metrics, key risk indicators and a prioritised remediation roadmap

Target Audience:

- Information security teams responsible for protecting payment, card and digital banking platforms
- IT risk functions that assess technology and cyber risk across banking and insurance operations
- Operational risk functions accountable for resilience of critical financial services and loss event data
- Compliance functions that track supervisory cyber expectations and incident notification duties
- Payment operations and fraud control functions that own transaction verification and authentication rules
- Internal control and assurance functions that test cyber controls in financial institutions

Course Outline:

Day 1: Financial Sector Cyber Threat Landscape and Current State

- Threat Profile Matrix for Banks, Insurers and Payment Firms
- Critical Business Services and Cyber Impact Tolerance Mapping
- Cyber-Enabled Fraud Loss Taxonomy Across Retail and Wholesale Banking
- NIST Cybersecurity Framework Profile for a Financial Institution
- Cyber Resilience Maturity Baseline Using a Sector Scorecard

Day 2: Financial Sector Security Standards and Supervisory Expectations

- Operational Resilience Principles for Banks and Cyber Governance Roles
- ISO/IEC 27001 Controls Mapped to Core Banking Processes
- PCI DSS Six Control Objectives for Cardholder Data Environments
- Interbank Messaging Customer Security Controls and Independent Attestation
- Supervisory Cyber Expectations Gap Analysis Using a Requirements Register

Day 3: Payment, Channel and Customer Authentication Controls

- Payment Instruction Verification and Callback Controls for Treasury Transfers
- Strong Customer Authentication Factors and Dynamic Linking Design
- Account Takeover Prevention Using Device Binding and Behavioural Signals
- ATM and Card Channel Security Controls Checklist Review
- Fintech Partner and Cloud Provider Security Due Diligence Questionnaire

Day 4: Cyber Risk Quantification, Resilience Testing and Incident Reporting

- FAIR Model Loss Scenarios for Payment Fraud Events
- Threat-Led Resilience Testing Scope and Control Validation Plan
- Severe but Plausible Cyber Scenario Exercise Design
- ISO/IEC 27035 Incident Classification for Financial Service Disruption
- Supervisory Incident Notification Template and Customer Communication Log

Day 5: Case Study: Cyber Resilience Assessment for a Case Bank

- Case Bank Brief with Payment Flows and Channel Inventory
- Case Build Cyber Resilience Assessment Against Earlier Control Sets
- Key Risk Indicators and Security Metrics Dashboard for the Board
- Remediation Roadmap Prioritised by Quantified Loss Exposure
- Board Cyber Resilience Report Completion and Peer Challenge

Skills You Will Gain:

- Financial Sector Threat Profiling
- Impact Tolerance Setting
- Cardholder Data Environment Review
- Payment Fraud Control Design
- Customer Authentication Design
- Cyber Loss Quantification
- Resilience Scenario Testing
- Cyber Incident Notification

Why Attend This Course:

- Return with a Cyber Resilience Assessment and Board Report, built on a case bank, that the chief risk officer and board risk committee can review
- Decide which payment, authentication and card channel controls to strengthen first, based on quantified loss exposure rather than audit findings alone
- Avoid late or incomplete incident notifications and untested recovery assumptions that expose the institution to supervisory findings and customer harm
- Share the threat profile matrix, scenario exercise design and metrics dashboard with security, fraud and operational risk colleagues

Conclusion:

Once participants return, the chief risk officer and board risk committee can use the Cyber Resilience Assessment and Board Report to agree which payment, authentication and card channel weaknesses to fund first and which impact tolerances to accept. Security and fraud teams can reuse its metrics dashboard in regular reporting, and operational risk can feed its loss scenarios into the risk register. After the first board cycle, the institution should review whether the key risk indicators moved as expected and whether the scenario exercise exposed gaps the roadmap missed.