Banking Cyber Resilience Training Course

Professional Development Training Course Outline

Category	Banking Institute	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The Banking Cyber Resilience Training Course is designed to equip professionals, with the knowledge and practical skills required to protect modern financial institutions against evolving cyber threats. As banks rapidly adopt digital banking, cloud computing, artificial intelligence (AI), open banking, API banking, fintech integration, and real-time payment systems, cyber risks continue to grow in complexity. This training emphasizes cyber resilience, enabling organizations not only to prevent cyberattacks but also to detect, respond, recover, and continuously adapt while maintaining uninterrupted banking operations. Participants gain hands-on experience in implementing Zero Trust Architecture, Security Operations Center (SOC) practices, threat intelligence, incident response, business continuity, digital operational resilience, and regulatory compliance aligned with global banking standards.

The course combines internationally recognized cybersecurity frameworks with practical banking scenarios to help organizations strengthen their cyber defense capabilities against ransomware, phishing, insider threats, Advanced Persistent Threats (APTs), AI-powered cyberattacks, fraud, data breaches, and supply chain attacks. Through interactive workshops, real-world case studies, cyber simulations, and risk assessments, participants develop the expertise to build resilient banking ecosystems, improve governance, safeguard customer trust, ensure regulatory compliance, and enhance operational continuity. Upon completion, participants will be prepared to design and implement enterprise-wide cyber resilience strategies that support secure digital transformation and long-term business sustainability within the banking sector.

Programme Curriculum

Banking Cyber Resilience Training Course

Introduction

The Banking Cyber Resilience Training Course is designed to equip professionals, with the knowledge and practical skills required to protect modern financial institutions against evolving cyber threats. This training emphasizes cyber resilience, enabling organizations not only to prevent cyberattacks but also to detect, respond, recover, and continuously adapt while maintaining uninterrupted banking operations. Participants gain hands-on experience in implementing Zero Trust Architecture, Security Operations Center (SOC) practices, threat intelligence, incident response, business continuity, digital operational resilience, and regulatory compliance aligned with global banking standards.

The course combines internationally recognized cybersecurity frameworks with practical banking scenarios to help organizations strengthen their cyber defense capabilities against ransomware, phishing, insider threats, Advanced Persistent Threats (APTs), AI-powered cyberattacks, fraud, data breaches, and supply chain attacks. Through interactive workshops, real-world case studies, cyber simulations, and risk assessments, participants develop the expertise to build resilient banking ecosystems, improve governance, safeguard customer trust, ensure regulatory compliance, and enhance operational continuity. Upon completion, participants will be prepared to design and implement enterprise-wide cyber resilience strategies that support secure digital transformation and long-term business sustainability within the banking sector.

Course Duration

5 days

Course Objectives

1. Understand modern Banking Cyber Resilience Frameworks and cybersecurity governance.
2. Identify and mitigate Advanced Persistent Threats (APT) targeting financial institutions.
3. Implement Zero Trust Security Architecture for banking environments.
4. Strengthen Digital Banking Security and secure online financial services.
5. Secure Cloud Banking Infrastructure using modern cloud security controls.
6. Improve Cyber Risk Management and enterprise risk assessment practices.
7. Build effective Incident Response and Cyber Crisis Management capabilities.
8. Enhance Fraud Detection and Financial Crime Prevention using AI-driven analytics.
9. Implement Threat Intelligence and Security Operations Center (SOC) best practices.
10. Ensure compliance with Cybersecurity Regulations, Data Privacy, and banking standards.
11. Develop Business Continuity and Disaster Recovery strategies for cyber incidents.
12. Protect Payment Systems, SWIFT Infrastructure, APIs, and FinTech Ecosystems from cyber threats.
13. Build an enterprise-wide Cyber Resilience Strategy for sustainable digital transformation.

Target Audience

1. Banking Executives and Senior Management
2. Chief Information Security Officers (CISOs)
3. IT Managers and System Administrators
4. Cybersecurity Analysts and SOC Teams
5. Risk Management Professionals
6. Compliance, Audit, and Governance Officers
7. Digital Banking and FinTech Professionals
8. Business Continuity and Disaster Recovery Teams

Course Modules

Module 1: Banking Cybersecurity Fundamentals

- Cyber resilience principles in banking
- Banking threat landscape and cyber risks
- Cybersecurity governance and policies
- Regulatory requirements and compliance
- **Case Study:** Bangladesh Bank SWIFT Cyber Heist

Module 2: Cyber Risk Management & Governance

- Enterprise cyber risk assessment
- Third-party and supply chain security
- Risk mitigation strategies
- Governance frameworks
- **Case Study:** Capital One Cloud Security Incident

Module 3: Digital Banking & Payment Security

- Online banking security controls
- Payment gateway protection
- API security and Open Banking
- Mobile banking cybersecurity
- **Case Study:** Cosmos Bank Cyber Attack

Module 4: Threat Intelligence & Security Operations

- Threat intelligence lifecycle
- Security Operations Center (SOC)
- SIEM monitoring
- Threat hunting techniques
- **Case Study:** SolarWinds Supply Chain Attack

Module 5: Incident Response & Cyber Crisis Management

- Incident response lifecycle
- Cyber crisis communication
- Digital forensics fundamentals
- Ransomware response planning
- **Case Study:** Colonial Pipeline Ransomware Attack

Module 6: Cloud Security & Zero Trust Banking

- Cloud security architecture
- Zero Trust implementation
- Identity and Access Management (IAM)
- Multi-factor authentication (MFA)
- **Case Study:** Microsoft Exchange Server Exploitation

Module 7: Business Continuity & Operational Resilience

- Business Impact Analysis (BIA)
- Disaster Recovery Planning
- Cyber resilience testing
- Operational resilience frameworks

- **Case Study:** NotPetya Global Cyberattack

Module 8: Emerging Technologies & Future Banking Security

- Artificial Intelligence in cybersecurity
- Machine learning for fraud detection
- Blockchain security
- Quantum-safe cryptography
- **Case Study:** AI-Driven Deepfake Banking Fraud

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	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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