Banking Information Security 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

Banking Information Security Training Course is designed to strengthen cybersecurity resilience, protect financial ecosystems, and develop advanced skills in banking cybersecurity, information risk management, data protection, fraud prevention, and regulatory compliance. With the rapid growth of digital banking, mobile payments, cloud banking, artificial intelligence (AI), and fintech innovation, financial institutions face increasingly sophisticated cyber threats including ransomware, phishing, identity theft, insider threats, and advanced persistent threats (APTs). This training equips banking professionals with practical knowledge of cyber defense strategies, security governance, threat intelligence, and secure banking operations.

This comprehensive program focuses on building a security-first culture across banking organizations through real-world scenarios, industry best practices, security frameworks, and hands-on case studies. Participants learn how to implement zero trust security, security operations, incident response, data privacy controls, vulnerability management, and cyber risk mitigation strategies aligned with global banking standards. The course enables professionals to safeguard customer information, strengthen operational resilience, and support secure digital transformation initiatives.

Programme Curriculum

Banking Information Security Training Course

Introduction

Banking Information Security Training Course is designed to strengthen cybersecurity resilience, protect financial ecosystems, and develop advanced skills in banking cybersecurity, information risk management, data protection, fraud prevention, and regulatory compliance. With the rapid growth of digital banking, mobile payments, cloud banking, artificial intelligence (AI), and fintech innovation, financial institutions face increasingly sophisticated cyber threats including ransomware, phishing, identity theft, insider threats, and advanced persistent threats (APTs). This training equips banking professionals with practical knowledge of cyber defense

strategies, security governance, threat intelligence, and secure banking operations.

This comprehensive program focuses on building a security-first culture across banking organizations through real-world scenarios, industry best practices, security frameworks, and hands-on case studies. Participants learn how to implement zero trust security, security operations, incident response, data privacy controls, vulnerability management, and cyber risk mitigation strategies aligned with global banking standards. The course enables professionals to safeguard customer information, strengthen operational resilience, and support secure digital transformation initiatives.

Course Duration

5 days

Course Objectives

1. Understand advanced banking cybersecurity threats, attack vectors, and emerging cyber risks.
2. Develop skills in financial information security governance and risk management.
3. Learn implementation of data protection, encryption, and privacy security controls.
4. Master fraud detection, cyber fraud prevention, and digital payment security techniques.
5. Understand regulatory compliance frameworks for banking security environments.
6. Apply zero trust architecture and identity access management (IAM) principles.
7. Build expertise in security incident response and cyber crisis management.
8. Analyze threat intelligence and security monitoring technologies.
9. Learn secure practices for cloud banking and fintech cybersecurity.
10. Improve knowledge of network security and endpoint protection strategies.
11. Develop capabilities in security awareness and human risk management.
12. Understand business continuity, disaster recovery, and operational resilience.
13. Implement modern cybersecurity frameworks and defense-in-depth strategies.

Target Audience

1. Banking cybersecurity professionals
2. Information security officers and managers
3. IT administrators and network security teams
4. Risk management and compliance professionals
5. Digital banking and fintech professionals
6. Internal auditors and governance teams
7. Fraud prevention and investigation specialists
8. Banking executives and decision-makers

Course Modules

Module 1: Banking Cybersecurity Fundamentals

- Introduction to **financial sector cybersecurity landscape**
- Understanding banking cyber threats and attack methodologies
- Overview of information security principles and controls
- Banking security policies and governance structures
- Developing a cybersecurity mindset across banking teams
- **Case Study:** Analysis of a major banking cyberattack involving unauthorized access and customer data exposure.

Module 2: Banking Threat Intelligence and Risk Management

- Cyber threat intelligence lifecycle and intelligence platforms
- Financial cyber risk assessment methodologies
- Vulnerability identification and security risk scoring
- Advanced persistent threats (APT) targeting banks
- Risk-based security decision-making processes
- **Case Study:** Investigation of a targeted phishing campaign against banking employees using threat intelligence techniques.

Module 3: Data Protection and Privacy Security

- Customer data protection strategies
- Encryption technologies and key management
- Data loss prevention (DLP) solutions
- Privacy regulations and compliance requirements
- Secure handling of financial information
- **Case Study:** Review of a banking data breach and implementation of improved data protection controls.

Module 4: Digital Banking and Payment Security

- Mobile banking security challenges
- Online transaction protection methods
- Payment gateway security architecture
- API security for digital banking platforms
- Fraud prevention using AI and analytics
- **Case Study:** Assessment of digital payment fraud prevention strategies used by modern banks.

Module 5: Identity Security and Access Management

- Identity and access management (IAM) concepts
- Multi-factor authentication (MFA) implementation
- Privileged access management (PAM)
- Zero Trust security architecture
- User access monitoring and control
- **Case Study:** Implementation of zero trust controls to reduce unauthorized banking system access.

Module 6: Security Operations and Incident Response

- Security Operations Center (SOC) functions
- Security monitoring and SIEM technologies
- Incident detection and response procedures
- Cyber crisis communication management
- Digital forensic investigation techniques
- **Case Study:** Simulation of a ransomware incident response process within a banking environment.

Module 7: Cloud Banking and Emerging Technologies Security

- Cloud security challenges in financial services
- Secure cloud migration strategies
- Artificial intelligence (AI) cybersecurity applications
- Blockchain and fintech security considerations

- Emerging cyber threat management
- **Case Study:** Evaluation of cloud security controls during a banking digital transformation project.

Module 8: Compliance, Governance and Security Leadership

- Banking cybersecurity regulations and standards
- Information security governance frameworks
- Security audits and compliance management
- Business continuity and operational resilience
- Building a cybersecurity-driven banking culture
- **Case Study:** Creating a cybersecurity governance roadmap for a financial institution.

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