Cybersecurity for Banks 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

In today’s hyper-connected financial ecosystem, cybersecurity in banking has become a mission-critical priority driven by rapid digital transformation, fintech integration, cloud banking, and real-time payment systems. Banks are increasingly targeted by sophisticated cyber threats, including ransomware, phishing, insider attacks, and advanced persistent threats (APTs). Cybersecurity for Banks Training Course equips banking professionals with cutting-edge knowledge in cyber risk management, data protection, network security, and regulatory compliance, ensuring resilience against evolving cyber risks.

With the rise of AI-driven cyberattacks, open banking APIs, and cross-border digital transactions, financial institutions must adopt proactive and adaptive cybersecurity strategies. This course provides practical insights into threat intelligence, security operations (SOC), incident response, and cyber resilience frameworks aligned with global standards such as ISO 27001, NIST, and Basel guidelines. Participants will gain hands-on exposure to real-world case studies, empowering them to safeguard digital assets, customer data, and financial infrastructure.

Programme Curriculum

Cybersecurity for Banks Training Course

Introduction

In today’s hyper-connected financial ecosystem, cybersecurity in banking has become a mission-critical priority driven by rapid digital transformation, fintech integration, cloud banking, and real-time payment systems. Banks are increasingly targeted by sophisticated cyber threats, including ransomware, phishing, insider attacks, and advanced persistent threats (APTs). Cybersecurity for Banks Training Course equips banking professionals with cutting-edge knowledge in cyber risk management, data protection, network security, and regulatory compliance, ensuring resilience against evolving cyber risks.

With the rise of AI-driven cyberattacks, open banking APIs, and cross-border digital transactions, financial institutions must adopt proactive and adaptive cybersecurity strategies. This course provides practical insights into threat intelligence, security operations (SOC), incident response, and cyber resilience frameworks aligned with global standards such as ISO 27001, NIST, and Basel guidelines. Participants will gain hands-on exposure to real-world case studies, empowering them to safeguard digital assets, customer data, and financial infrastructure.

Course Duration

5 days

Course Objectives

1. Understand cybersecurity fundamentals in banking ecosystems
2. Identify emerging cyber threats and attack vectors in financial services
3. Implement advanced threat detection and prevention strategies
4. Strengthen data privacy and encryption frameworks
5. Enhance cyber risk assessment and mitigation techniques
6. Develop incident response and cyber crisis management plans
7. Apply regulatory compliance
8. Secure digital banking channels and mobile platforms
9. Manage third-party and vendor cybersecurity risks
10. Utilize AI and machine learning in cybersecurity defense
11. Protect cloud infrastructure and banking systems
12. Build cyber resilience and business continuity strategies
13. Promote cybersecurity awareness and culture in banks

Target Audience

1. Bank IT and Cybersecurity Professionals
2. Risk and Compliance Officers
3. Information Security Managers (CISOs)
4. Digital Banking and Fintech Teams
5. Internal and External Auditors
6. Operations and Infrastructure Managers
7. Fraud Prevention and AML Specialists
8. Senior Banking Executives and Decision Makers

Course Modules

Module 1: Cybersecurity Fundamentals in Banking

- Overview of banking cyber ecosystem
- Key cybersecurity concepts and frameworks
- Types of cyber threats in financial institutions
- Security architecture in banks
- Case Study: Global bank phishing attack and response

Module 2: Threat Landscape and Risk Management

- Advanced persistent threats (APTs)
- Cyber risk assessment methodologies

- Vulnerability management tools
- Risk mitigation strategies
- Case Study: Ransomware attack on financial institutions

Module 3: Network and Infrastructure Security

- Secure network design and firewalls
- Intrusion detection and prevention systems (IDS/IPS)
- Endpoint security strategies
- Secure data centers and infrastructure
- Case Study: Data breach due to network misconfiguration

Module 4: Data Protection and Privacy

- Data classification and protection policies
- Encryption and tokenization techniques
- Regulatory compliance (GDPR, PCI-DSS)
- Data loss prevention (DLP) tools
- Case Study: Customer data leak and compliance penalties

Module 5: Digital Banking and Application Security

- Secure mobile and internet banking
- API security in open banking
- Secure software development lifecycle (SSDLC)
- Authentication and access controls
- Case Study: API vulnerability exploitation

Module 6: Cloud Security in Banking

- Cloud risk management strategies
- Securing SaaS, PaaS, and IaaS platforms
- Identity and access management (IAM)
- Cloud compliance frameworks
- Case Study: Cloud misconfiguration breach

Module 7: Incident Response and Cyber Resilience

- Incident detection and response planning
- Cyber crisis management frameworks
- Business continuity and disaster recovery
- Security Operations Center (SOC) functions
- Case Study: Bank recovery after cyberattack

Module 8: Emerging Technologies and Cybersecurity Trends

- AI and machine learning in cybersecurity
- Blockchain security in banking
- Zero Trust Architecture (ZTA)
- Cybersecurity automation tools
- Case Study: AI-driven fraud detection implementation

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

Start Date	End Date	Location	Price
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