Cyber Risk Management in Banking 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 rapidly evolving digital banking ecosystem, cyber threats have become more sophisticated, persistent, and financially damaging. Banks are prime targets for cybercrime, ransomware attacks, phishing schemes, data breaches, and advanced persistent threats (APTs). Cyber Risk Management in Banking Training Course is designed to equip banking professionals with cutting-edge knowledge and practical tools to identify, assess, mitigate, and monitor cyber risks. The course integrates cybersecurity frameworks, regulatory compliance, threat intelligence, and digital resilience strategies aligned with global standards such as ISO 27001, NIST, and Basel guidelines.

With the rise of fintech innovation, cloud banking, open banking APIs, and digital payments, financial institutions must adopt proactive and intelligence-driven cyber risk management approaches. This training emphasizes real-world case studies, incident response planning, cyber risk governance, and emerging technologies such as AI-driven security and blockchain risk mitigation. Participants will gain actionable insights into strengthening cyber resilience, protecting customer data, ensuring regulatory compliance, and maintaining operational continuity in an increasingly complex threat landscape.

Programme Curriculum

Cyber Risk Management in Banking Training Course

Introduction
In today’s rapidly evolving digital banking ecosystem, cyber threats have become more sophisticated, persistent, and financially damaging. Banks are prime targets for cybercrime, ransomware attacks, phishing schemes, data breaches, and advanced persistent threats (APTs). Cyber Risk Management in Banking Training Course is designed to equip banking professionals with cutting-edge knowledge and practical tools to identify, assess, mitigate, and monitor cyber risks. The course integrates cybersecurity frameworks, regulatory compliance, threat intelligence, and digital resilience strategies aligned with global standards such as ISO

27001, NIST, and Basel guidelines.

With the rise of fintech innovation, cloud banking, open banking APIs, and digital payments, financial institutions must adopt proactive and intelligence-driven cyber risk management approaches. This training emphasizes real-world case studies, incident response planning, cyber risk governance, and emerging technologies such as AI-driven security and blockchain risk mitigation. Participants will gain actionable insights into strengthening cyber resilience, protecting customer data, ensuring regulatory compliance, and maintaining operational continuity in an increasingly complex threat landscape.

Course Duration

5 days

Course Objectives

1. Understand Cyber Risk Management Frameworks
2. Identify emerging cyber threats in digital banking and fintech ecosystems
3. Analyze cyber attack vectors, vulnerabilities, and threat intelligence models
4. Implement risk assessment methodologies and cyber risk scoring techniques
5. Strengthen cybersecurity governance and enterprise risk management (ERM)
6. Develop incident response and cyber crisis management strategies
7. Ensure regulatory compliance
8. Enhance data protection, privacy, and encryption standards
9. Apply cloud security and third-party risk management practices
10. Leverage AI and machine learning in fraud detection and cybersecurity
11. Build cyber resilience and business continuity planning (BCP)
12. Conduct penetration testing and vulnerability assessments
13. Promote cybersecurity awareness and culture within banks

Target Audience

1. Risk Management Professionals
2. Cybersecurity and IT Security Officers
3. Compliance and Audit Managers
4. Banking Operations Managers
5. Digital Banking and Fintech Teams
6. Internal and External Auditors
7. Chief Risk Officers (CROs) and Executives
8. IT Governance and Data Protection Officers

Course Modules

Module 1: Introduction to Cyber Risk in Banking

- Overview of cyber risk landscape in financial services
- Key cyber threats and vulnerabilities in banks
- Cyber risk vs traditional operational risk
- Global cybersecurity standards and frameworks
- Role of cyber risk in enterprise risk management

  Case Study: Analysis of a major global bank data breach incident

Module 2: Cyber Threat Intelligence & Attack Vectors

- Understanding threat intelligence lifecycle
- Common attack vectors: phishing, malware, ransomware
- Insider threats and social engineering risks
- Dark web monitoring and intelligence gathering
- Threat detection tools and technologies

  Case Study: Phishing attack leading to financial fraud in a bank

Module 3: Cyber Risk Assessment & Measurement

- Risk identification and classification
- Quantitative and qualitative risk assessment methods
- Cyber risk scoring and heat maps
- Risk appetite and tolerance in banking
- Key risk indicators (KRIs) and reporting

  Case Study: Cyber risk assessment for a digital banking platform

Module 4: Cybersecurity Governance & Compliance

- Governance structures and roles
- Regulatory frameworks
- Policies, procedures, and controls
- Third-party and vendor risk management
- Audit and compliance monitoring

  Case Study: Regulatory penalties due to weak cybersecurity controls

Module 5: Data Protection & Privacy Management

- Data classification and lifecycle management
- Encryption, tokenization, and access controls
- Privacy laws and data protection regulations
- Managing customer data security
- Data breach prevention strategies

  Case Study: Customer data leak and reputational damage

Module 6: Incident Response & Cyber Crisis Management

- Incident detection and response lifecycle
- Cyber crisis management frameworks
- Communication and stakeholder management
- Digital forensics and investigation
- Post-incident review and lessons learned

  Case Study: Ransomware attack response in a financial institution

Module 7: Emerging Technologies & Cyber Risks

- Risks in **cloud computing and SaaS banking**
- Cyber risks in **AI, blockchain, and APIs**
- Open banking security challenges
- Fintech partnerships and risk exposure
- Future trends in cyber risk management

  Case Study: API vulnerability exploitation in open banking

Module 8: Cyber Resilience & Business Continuity

- Building cyber resilience frameworks
- Business continuity and disaster recovery (BCP/DR)
- Stress testing and scenario analysis
- Cyber insurance and financial impact mitigation
- Continuous monitoring and improvement
  Case Study: Maintaining operations during a cyber disruption

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