Cyber Incident Response 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 rapidly evolving digital banking ecosystem, financial institutions face an unprecedented surge in cyber threats, including ransomware attacks, phishing campaigns, insider threats, data breaches, and advanced persistent threats (APTs). Banks operate within a highly interconnected environment driven by cloud computing, fintech integrations, open banking APIs, and real-time payment systems, making them prime targets for sophisticated cybercriminals. A robust Cyber Incident Response Framework is no longer optional it is a strategic necessity to ensure business continuity, regulatory compliance, operational resilience, and customer trust.

Cyber Incident Response for Banks Training Course equips banking professionals with cutting-edge skills in cybersecurity incident detection, response, containment, eradication, and recovery aligned with global standards such as NIST, ISO 27035, and FFIEC guidelines. Participants will gain hands-on expertise in threat intelligence, digital forensics, Security Operations Center (SOC) operations, incident handling playbooks, and crisis communication strategies, enabling them to proactively mitigate risks and strengthen cyber resilience in banking environments.

Programme Curriculum

Cyber Incident Response for Banks Training Course

Introduction

In today’s rapidly evolving digital banking ecosystem, financial institutions face an unprecedented surge in cyber threats, including ransomware attacks, phishing campaigns, insider threats, data breaches, and advanced persistent threats (APTs). Banks operate within a highly interconnected environment driven by cloud computing, fintech integrations, open banking APIs, and real-time payment systems, making them prime targets for sophisticated cybercriminals. A robust Cyber Incident Response Framework is no longer optional it is a

strategic necessity to ensure business continuity, regulatory compliance, operational resilience, and customer trust.

Cyber Incident Response for Banks Training Course equips banking professionals with cutting-edge skills in cybersecurity incident detection, response, containment, eradication, and recovery aligned with global standards such as NIST, ISO 27035, and FFIEC guidelines. Participants will gain hands-on expertise in threat intelligence, digital forensics, Security Operations Center (SOC) operations, incident handling playbooks, and crisis communication strategies, enabling them to proactively mitigate risks and strengthen cyber resilience in banking environments.

Course Duration

5 days

Training Objectives

By the end of this course, participants will be able to:

1. Master Cyber Incident Response Lifecycle Management
2. Implement Real-Time Threat Detection and Monitoring
3. Apply Advanced Digital Forensics Techniques
4. Strengthen Security Operations Center (SOC) Efficiency
5. Develop Incident Response Playbooks and Runbooks
6. Enhance Cyber Threat Intelligence Utilization
7. Execute Ransomware Containment and Recovery Strategies
8. Ensure Regulatory Compliance and Cyber Governance
9. Improve Cloud Security Incident Handling
10. Conduct Cyber Crisis Management and Communication
11. Implement Zero Trust Security Frameworks
12. Perform Post-Incident Analysis and Reporting
13. Build Cyber Resilience and Business Continuity Plans

Target Audience

1. Cybersecurity Analysts and SOC Teams
2. IT Security Managers and Risk Officers
3. Bank Compliance and Audit Professionals
4. Digital Banking and IT Operations Teams
5. Chief Information Security Officers (CISOs)
6. Incident Response and Forensics Specialists
7. Fraud Risk and Anti-Money Laundering Teams
8. Fintech and Payment Security Professionals

Training Modules

Module 1: Cyber Threat Landscape in Banking

- Overview of modern cyber threats in financial services
- Understanding attack vectors and threat actors
- Banking-specific vulnerabilities and risks
- Impact of fintech and open banking risks
- Case Study: Global bank ransomware breach analysis

Module 2: Cyber Incident Response Frameworks

- Introduction to NIST and ISO 27035 frameworks
- Incident classification and prioritization
- Roles and responsibilities in response teams
- Building incident response policies
- Case Study: Implementing NIST in a commercial bank

Module 3: Threat Detection and Monitoring

- Security Information and Event Management (SIEM)
- Real-time monitoring and alerting systems
- Behavioral analytics and anomaly detection
- Threat intelligence integration
- **Case Study:** Detecting insider fraud using SIEM

Module 4: Incident Containment and Eradication

- Containment strategies for cyber incidents
- Malware analysis and removal techniques
- Network isolation and endpoint protection
- Preventing lateral movement
- **Case Study:** Containing a phishing-based breach

Module 5: Digital Forensics and Investigation

- Fundamentals of **cyber forensics in banking**
- Evidence collection and preservation
- Log analysis and timeline reconstruction
- Legal considerations in investigations
- **Case Study:** Investigating unauthorized transactions

Module 6: Cyber Crisis Management

- Crisis communication strategies
- Stakeholder and regulatory reporting
- Reputation risk management
- Incident escalation procedures
- **Case Study:** Managing public response to data breach

Module 7: Recovery and Business Continuity

- Disaster recovery planning
- Data backup and restoration strategies
- Ensuring operational resilience
- Post-incident recovery frameworks
- **Case Study:** Restoring services after ransomware attack

Module 8: Post-Incident Review and Cyber Resilience

- Root cause analysis and lessons learned
- Improving incident response processes

- Cyber resilience and continuous improvement
- Training and simulation exercises
- **Case Study:** Strengthening defenses after repeated attacks

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
07 Sep 2026	11 Sep 2026	Online	$1,000
07 Sep 2026	11 Sep 2026	Physical	$1,500

Start Date	End Date	Location	Price
14 Sep 2026	18 Sep 2026	Online	$1,000
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Online	$1,000
28 Sep 2026	02 Oct 2026	Physical	$1,500

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

Register Online Now

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