Banking Data Protection 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 Data Protection Training Course is designed to strengthen cybersecurity resilience, regulatory compliance, data privacy governance, and digital risk management within the banking and financial services sector. As banks accelerate digital transformation through cloud banking, open banking, artificial intelligence (AI), blockchain, mobile banking, and fintech ecosystems, protecting sensitive customer information has become a strategic priority. This course equips banking professionals with advanced knowledge of data protection frameworks, information security controls, privacy regulations, threat intelligence, and secure data handling practices to prevent data breaches and enhance customer trust.

The course focuses on emerging challenges such as ransomware attacks, insider threats, third-party risks, identity theft, payment fraud, and regulatory enforcement. Participants learn practical approaches to implementing Data Loss Prevention (DLP), Zero Trust Architecture, encryption strategies, privacy-by-design principles, cyber risk assessment, and incident response management. Through real-world banking case studies, interactive exercises, and scenario-based learning, this training enables organizations to build a strong data protection culture, operational resilience framework, and future-ready cybersecurity strategy.

Programme Curriculum

Banking Data Protection Training Course

Introduction

Banking Data Protection Training Course is designed to strengthen cybersecurity resilience, regulatory compliance, data privacy governance, and digital risk management within the banking and financial services sector. As banks accelerate digital transformation through cloud banking, open banking, artificial intelligence (AI), blockchain, mobile banking, and fintech ecosystems, protecting sensitive customer information has become a strategic priority. This course equips banking professionals with advanced knowledge of data protection frameworks, information security controls, privacy regulations, threat intelligence, and secure data

handling practices to prevent data breaches and enhance customer trust.

The course focuses on emerging challenges such as ransomware attacks, insider threats, third-party risks, identity theft, payment fraud, and regulatory enforcement. Participants learn practical approaches to implementing Data Loss Prevention (DLP), Zero Trust Architecture, encryption strategies, privacy-by-design principles, cyber risk assessment, and incident response management. Through real-world banking case studies, interactive exercises, and scenario-based learning, this training enables organizations to build a strong data protection culture, operational resilience framework, and future-ready cybersecurity strategy.

Course Duration

5 days

Course Objectives

By completing this Banking Data Protection Training Course, participants will be able to:

1. Understand the principles of banking data protection, privacy governance, and cybersecurity risk management.
2. Implement effective data privacy frameworks aligned with global regulatory standards.
3. Develop skills in GDPR compliance, financial data governance, and regulatory reporting.
4. Identify and mitigate cyber threats, phishing attacks, ransomware, and financial fraud risks.
5. Apply Zero Trust Security models for protecting banking information systems.
6. Design effective Data Loss Prevention (DLP) and information classification strategies.
7. Improve knowledge of cloud security, SaaS protection, and secure digital banking environments.
8. Strengthen capabilities in identity and access management (IAM) and privileged access security.
9. Apply encryption, tokenization, and secure data lifecycle management techniques.
10. Conduct banking-focused cyber risk assessments and vulnerability analysis.
11. Develop effective incident response, breach management, and crisis communication plans.
12. Enhance third-party and vendor risk management through secure supply chain practices.
13. Build a sustainable cybersecurity awareness and data protection culture across banking organizations.

Target Audience

1. Bank executives and senior management leaders
2. Chief Information Security Officers (CISOs) and cybersecurity managers
3. Data Protection Officers (DPOs) and privacy professionals
4. Banking IT administrators and infrastructure teams
5. Risk management and compliance officers
6. Digital banking and fintech professionals
7. Internal auditors and governance specialists
8. Financial services cybersecurity consultants

Course Modules

Module 1: Banking Data Protection Fundamentals and Cybersecurity Landscape

- Principles of financial data protection and information security
- Evolution of banking cyber threats and digital transformation risks
- Data classification, ownership, and governance models
- Banking security frameworks and best practices
- Building a data protection culture

- Case Study: Digital Banking Data Exposure Incident

Module 2: Data Privacy Regulations and Compliance Frameworks

- Understanding GDPR, privacy laws, and financial regulations
- Data Protection Impact Assessments (DPIA)
- Regulatory compliance monitoring
- Privacy-by-design and privacy engineering
- Audit preparation and compliance reporting
- Case Study: Global Bank Regulatory Compliance Challenge

Module 3: Banking Cyber Threats and Data Breach Prevention

- Modern banking cyber attack techniques
- Ransomware and malware defense strategies
- Phishing and social engineering prevention
- Insider threat detection
- Threat intelligence and security monitoring
- Case Study: Ransomware Attack on Financial Infrastructure.

Module 4: Data Security Technologies and Protection Controls

- Encryption and cryptographic security
- Tokenization and masking techniques
- Data Loss Prevention (DLP)
- Secure databases and application protection
- Endpoint and network security controls
- Case Study: Payment Data Protection Program

Module 5: Identity Security, Access Management, and Zero Trust Banking

- Identity and Access Management (IAM)
- Multi-Factor Authentication (MFA)
- Privileged Access Management (PAM)
- Zero Trust Architecture implementation
- Access governance and authentication controls
- Case Study: Unauthorized Account Access Prevention

Module 6: Cloud Banking Security and Digital Transformation Risks

- Cloud security governance
- Secure migration strategies
- API security and open banking protection
- Third-party cloud risk management
- Secure software development practices
- Case Study: Cloud Banking Migration Security

Module 7: Data Breach Response, Incident Management, and Recovery

- Incident response lifecycle
- Cyber crisis management
- Breach notification procedures

- Digital forensics fundamentals
- Business continuity and disaster recovery
- Case Study: Customer Data Breach Response Simulation

Module 8: Future Trends in Banking Data Protection and Cyber Resilience

- Artificial Intelligence (AI) in cybersecurity
- Machine learning threat detection
- Blockchain security applications
- Quantum-safe encryption concepts
- Future-ready cyber resilience strategies
- Case Study: AI-Powered Banking Security Transformation

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