Cyber Resilience for Financial Inclusion Providers Training Course

Professional Development Training Course Outline

Category	Microfinance & Financial Inclusion	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

As digital financial services expand rapidly, financial inclusion providers face increasing cyber threats, ranging from data breaches to operational disruptions. Ensuring cyber resilience is critical for protecting customers, maintaining trust, and sustaining business operations. Cyber Resilience for Financial Inclusion Providers Training Course equips participants with practical knowledge of cyber risk management, regulatory compliance, and resilience-building strategies tailored to financial inclusion contexts. Participants will explore cybersecurity frameworks, incident response planning, risk assessments, and governance approaches essential for digital finance providers. Real-world case studies will highlight the impact of cyber threats on financial inclusion and demonstrate effective mitigation strategies.

The course further focuses on proactive monitoring, prevention, and recovery strategies to enhance operational resilience. Participants will learn to develop organizational policies, incident response plans, and business continuity frameworks that safeguard both institutions and clients. Emphasis is placed on integrating cybersecurity with financial inclusion goals, ensuring that vulnerable populations are protected while digital financial services scale responsibly. By the end of the training, participants will be capable of implementing comprehensive cyber resilience measures across digital financial service providers.

Programme Curriculum

Cyber Resilience for Financial Inclusion Providers Training Course

Introduction

As digital financial services expand rapidly, financial inclusion providers face increasing cyber threats, ranging from data breaches to operational disruptions. Ensuring cyber resilience is critical for protecting customers, maintaining trust, and sustaining business operations. Cyber Resilience for Financial Inclusion Providers

Training Course equips participants with practical knowledge of cyber risk management, regulatory compliance, and resilience-building strategies tailored to financial inclusion contexts. Participants will explore cybersecurity frameworks, incident response planning, risk assessments, and governance approaches essential for digital finance providers. Real-world case studies will highlight the impact of cyber threats on financial inclusion and demonstrate effective mitigation strategies.

The course further focuses on proactive monitoring, prevention, and recovery strategies to enhance operational resilience. Participants will learn to develop organizational policies, incident response plans, and business continuity frameworks that safeguard both institutions and clients. Emphasis is placed on integrating cybersecurity with financial inclusion goals, ensuring that vulnerable populations are protected while digital financial services scale responsibly. By the end of the training, participants will be capable of implementing comprehensive cyber resilience measures across digital financial service providers.

Course Objectives

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

- Understand cyber threats and vulnerabilities in digital financial services
- Develop organizational cybersecurity policies and governance frameworks
- Apply risk assessment techniques to identify and mitigate threats
- Implement incident response and business continuity plans
- Ensure compliance with national and international cybersecurity regulations
- Integrate cybersecurity strategies with financial inclusion objectives
- Monitor and evaluate cyber risks continuously
- Design secure digital platforms and infrastructure
- Enhance stakeholder awareness and capacity for cyber resilience
- Strengthen data protection and privacy mechanisms
- Apply threat detection and prevention technologies effectively
- Evaluate third-party vendors and partnerships for cyber risk
- Build a culture of cyber awareness across organizations
- Develop proactive crisis management and recovery strategies
- Align cyber resilience measures with operational, financial, and reputational goals

Organizational Benefits

- Strengthened protection against cyber threats and data breaches
- Improved operational resilience and business continuity
- Enhanced trust among customers and stakeholders
- Compliance with cybersecurity regulations and standards
- Reduced financial and reputational risks
- Improved incident response and recovery capabilities
- Better governance and internal control frameworks
- Increased awareness and preparedness across teams
- Enhanced security of digital financial platforms
- Support for scaling financial inclusion responsibly

Target Audience

- Financial inclusion providers and microfinance institutions (MFIs)
- Banks and digital financial service providers
- Fintech startups and mobile money operators
- Compliance, IT security, and risk management teams
- Regulatory authorities overseeing digital finance
- Development finance institutions (DFIs)
- Policy makers and program managers in financial inclusion
- NGOs supporting digital financial literacy and inclusion

Course Duration: 10 days

Course Modules

Module 1: Introduction to Cyber Resilience

- Overview of cyber threats and trends in digital finance
- Importance of resilience for financial inclusion
- Key stakeholders in cyber governance
- Operational and reputational risks
- Global and national regulatory landscape
- *Case study: Cyber resilience implementation in Kenyan fintechs*

Module 2: Cybersecurity Frameworks

- Cybersecurity standards and frameworks
- Risk-based approach to cyber resilience
- Policies, procedures, and governance
- Role of regulators and industry bodies
- Monitoring and enforcement mechanisms
- *Case study: NIST cybersecurity framework adoption in financial services*

Module 3: Risk Assessment and Threat Management

- Identifying vulnerabilities and threats
- Cyber risk assessment methodologies
- Prioritization of risks and controls
- Scenario planning and threat modeling
- Risk mitigation strategies
- *Case study: Threat management in Nigerian mobile money platforms*

Module 4: Data Protection and Privacy

- Legal and regulatory requirements for data protection
- Privacy-by-design principles
- Data classification, storage, and encryption
- Managing third-party data processors
- Monitoring and auditing data handling
- *Case study: GDPR compliance in fintech services*

Module 5: Incident Response Planning

- Components of an incident response plan
- Detection, reporting, and escalation procedures
- Containment and recovery strategies
- Communication with stakeholders
- Post-incident analysis and lessons learned
- *Case study: Incident response during a cyberattack in an African bank*

Module 6: Business Continuity and Recovery

- Developing business continuity plans
- Integration with operational and IT systems
- Backup and recovery procedures
- Continuity testing and drills
- Maintaining services during disruptions
- *Case study: Business continuity planning for digital lenders*

Module 7: Secure Digital Platforms and Infrastructure

- Network and system security measures
- Application security and mobile platforms
- Authentication and access management
- Secure payment and transaction processing
- Security monitoring and alert systems
- *Case study: Securing mobile money platforms in India*

Module 8: Cyber Risk Monitoring and Reporting

- Key performance indicators for cyber resilience
- Dashboards and reporting frameworks
- Compliance monitoring and audit trails
- Continuous risk evaluation
- Regulatory submission and stakeholder reporting
- *Case study: Cyber risk monitoring in Philippine fintechs*

Module 9: Vendor and Third-Party Risk Management

- Assessing third-party cybersecurity risks
- Vendor due diligence and contracts
- Monitoring and managing outsourcing risks
- Integration with internal security policies
- Mitigation of supply chain vulnerabilities
- *Case study: Vendor risk management in Latin American fintechs*

Module 10: Governance and Policy Development

- Cybersecurity policy formulation
- Board and management oversight
- Roles and responsibilities in cyber governance
- Regulatory compliance integration
- Policy communication and enforcement
- *Case study: Governance structures in South African MFIs*

Module 11: Employee Awareness and Training

- Building a cyber-aware culture
- Training programs and awareness campaigns
- Behavioral practices for secure operations
- Role-based access and responsibilities
- Monitoring effectiveness of training
- *Case study: Employee cybersecurity awareness program in Kenya*

Module 12: Threat Detection and Prevention Technologies

- Tools for threat monitoring and detection
- Firewalls, antivirus, and intrusion detection
- Secure communication and encryption technologies
- Proactive threat hunting strategies
- Integrating AI and analytics for threat prevention
- *Case study: Threat detection in Nigerian mobile money services*

Module 13: Crisis Management and Communication

- Crisis management planning
- Stakeholder communication strategies
- Media and public relations during incidents

- Coordination with regulators and law enforcement
- Learning and adapting post-crisis
- *Case study: Managing a cyber crisis in a fintech startup*

Module 14: Integrating Cyber Resilience with Financial Inclusion

- Protecting vulnerable populations' data
- Aligning cyber strategies with inclusion goals
- Ensuring access while maintaining security
- Scaling secure digital financial services
- Policy recommendations for regulators and institutions
- *Case study: Inclusive finance and cyber resilience in India*

Module 15: Future Trends and Strategic Planning

- Emerging cyber threats in digital finance
- Advanced cybersecurity technologies and trends
- Strategic planning for long-term resilience
- Aligning organizational strategy with regulatory developments
- Sustainability and continuous improvement
- *Case study: Strategic cyber resilience roadmap for African fintechs*

Training Methodology

- Expert-led presentations and discussions
- Case study analysis from global financial inclusion providers
- Hands-on exercises in risk assessment and incident response
- Peer-to-peer learning and problem-solving sessions
- Cyber simulation and scenario-based exercises
- Practical tools and templates for monitoring, reporting, and governance
- Strategic planning workshops for cyber resilience

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
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

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

Register Online Now

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