Training Course on Cyber Resilience in the Financial Ecosystem

Professional Development Training Course Outline

Category	Banking Institute	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In an era of rapid digital transformation, central banks must be fortified against evolving cyber threats. As custodians of monetary stability and national financial infrastructure, central banks face unique vulnerabilities in their digital ecosystems. Train Course on Cyber Resilience in Financial Ecosystem is designed to equip central bank professionals with the critical skills, tools, and strategic frameworks to mitigate, respond to, and recover from sophisticated cyber incidents.

This course provides an in-depth understanding of cyber risk management, threat intelligence, regulatory compliance, data privacy, and incident response strategies tailored for the central banking ecosystem. Through practical modules, real-world case studies, and expert-led discussions, participants will gain insights into building resilient systems that align with international standards such as ISO 22301, NIST, and the CPMI-IOSCO guidelines.

Programme Curriculum

Training Course on Cyber Resilience in the Financial Ecosystem

Introduction

In an era of rapid digital transformation, central banks must be fortified against evolving cyber threats. As custodians of monetary stability and national financial infrastructure, central banks face unique vulnerabilities in their digital ecosystems. Train Course on Cyber Resilience in Financial Ecosystem is designed to equip central bank professionals with the critical skills, tools, and strategic frameworks to mitigate, respond to, and recover from sophisticated cyber incidents.

This course provides an in-depth understanding of cyber risk management, threat intelligence, regulatory compliance, data privacy, and incident response strategies tailored for the central banking ecosystem. Through practical modules, real-world

case studies, and expert-led discussions, participants will gain insights into building resilient systems that align with international standards such as ISO 22301, NIST, and the CPMI-IOSCO guidelines.

Course Objectives

1. Understand the foundations of cyber resilience in central banking operations.
2. Identify and evaluate emerging cyber threats and vulnerabilities in financial systems.
3. Develop effective incident response plans and disaster recovery frameworks.
4. Integrate AI and automation in cyber risk monitoring.
5. Implement regulatory compliance in line with global frameworks (GDPR, PSD2, DORA).
6. Design a comprehensive cybersecurity governance model.
7. Leverage threat intelligence platforms (TIPs) for proactive defense.
8. Establish resilient digital infrastructure for core banking operations.
9. Apply zero-trust architecture and network segmentation.
10. Foster an organizational cyber risk culture.
11. Utilize penetration testing and vulnerability assessment tools.
12. Coordinate with cross-border stakeholders for synchronized resilience.
13. Prepare cyber simulation exercises to enhance institutional readiness.

Target Audience

1. Cybersecurity officers in central banks
2. Risk management professionals
3. IT and network administrators
4. Financial regulators
5. Digital transformation leaders
6. Compliance and legal teams
7. Executive decision-makers
8. Monetary policy and operational staff

Course Duration: 10 days

Course Modules

Module 1: Introduction to Cyber Resilience in Central Banking

- Definition and scope of cyber resilience
- Importance of cyber resilience for financial stability
- Overview of global standards (NIST, ISO, CPMI-IOSCO)
- Cyber resilience vs cybersecurity
- Common vulnerabilities in central banks
- **Case Study**: The Bangladesh Bank cyber heist

Module 2: Cyber Threat Landscape for Financial Institutions

- Understanding advanced persistent threats (APTs)
- Ransomware and phishing attack vectors
- Insider threats and supply chain vulnerabilities
- Cybercrime trends in global banking
- Identifying red flags and threat indicators
- **Case Study**: The SWIFT network attack

Module 3: Risk Management Frameworks

- Cyber risk identification and assessment

- ISO 31000 and COSO ERM application
- Risk appetite and tolerance
- Mapping critical financial assets
- Cyber risk heatmaps and dashboards
- **Case Study**: European Central Bank risk mitigation strategy

Module 4: Incident Response and Recovery Planning

- Building an incident response team
- Steps in the cyber incident lifecycle
- Business continuity vs disaster recovery
- Post-incident analysis and learning
- Coordination with law enforcement
- **Case Study**: The Fedwire outage response

Module 5: Regulatory and Legal Compliance

- Overview of GDPR, PSD2, DORA
- Data protection and privacy laws
- Compliance challenges for central banks
- National and cross-border legal obligations
- Cyber insurance and liability management
- **Case Study**: GDPR enforcement on a European central bank

Module 6: Threat Intelligence and Information Sharing

- Building a threat intelligence program
- Using Threat Intelligence Platforms (TIPs)
- Cyber threat indicators (IOCs, TTPs)
- Intelligence sharing protocols (FS-ISAC, ENISA)
- Privacy and ethics in intelligence collection
- **Case Study**: UK’s NCSC threat-sharing model

Module 7: Security Operations Center (SOC) for Central Banks

- Role of SOC in continuous monitoring
- Key technologies: SIEM, SOAR, IDS
- SOC staffing and skillsets
- Metrics and KPIs for SOC effectiveness
- Tiered escalation and alert triage
- **Case Study**: Bank of England’s SOC setup

Module 8: AI and Automation in Cybersecurity

- AI-powered threat detection
- Machine learning in anomaly identification
- Automated incident response tools
- Risk of adversarial AI
- Benefits and limitations of automation
- **Case Study**: AI-driven SOC pilot in the Reserve Bank of India

Module 9: Identity and Access Management (IAM)

- Role-based access control (RBAC)
- Multi-factor authentication (MFA)
- Privileged access management

- IAM tools and integrations
- IAM audit and governance
- **Case Study**: Unauthorized access breach at a national bank

Module 10: Cloud Security in Financial Ecosystems

- Cloud deployment models and risks
- Secure cloud architecture for central banks
- Shared responsibility model
- Encryption and key management
- Compliance in cloud environments
- **Case Study**: Cloud migration by the Bank of Canada

Module 11: Zero Trust Architecture for Central Banks

- Principles of zero trust
- Micro-segmentation and least privilege
- Implementing continuous verification
- Security challenges in legacy systems
- Policy enforcement points (PEPs)
- **Case Study**: U.S. Federal Reserve's transition to zero trust

Module 12: Penetration Testing and Vulnerability Management

- Types of penetration testing
- Selecting penetration testing tools
- Continuous vulnerability scanning
- Interpreting test results
- Patch management strategies
- **Case Study**: Penetration test on a central clearing system

Module 13: Cyber Resilience Governance and Culture

- Governance frameworks and roles
- Embedding cyber into enterprise strategy
- Cyber hygiene training for employees
- Top-down vs bottom-up approaches
- Developing a cyber-resilient culture
- **Case Study**: Dutch Central Bank's cyber governance reforms

Module 14: International Cooperation and Cross-Border Resilience

- Role of BIS, IMF, and World Bank
- International cyber policy alignment
- Crisis coordination among nations
- Global standards harmonization
- Legal challenges in cross-border incidents
- **Case Study**: SWIFT's international response coordination

Module 15: Simulation Exercises and Red Teaming

- Purpose of cyber drills
- Designing tabletop exercises
- Simulated ransomware attack scenarios
- Evaluating red team effectiveness
- Lessons from exercise reports

- **Case Study**: ECB’s cyber drill with EU central banks

Training Methodology

- Interactive expert-led sessions
- Real-world case study discussions
- Group simulations and scenario-based drills
- Hands-on cybersecurity lab environments
- Quizzes and assessments after each module
- Final project presentation and feedback

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

Start Date	End Date	Location	Price
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