6550-1

In-Class

16 hours

Course Description:

This course is designed to equip bank employees with the knowledge and skills to navigate the rapidly evolving landscape of digital banking, including emerging trends, risks, and opportunities. Participants will gain a deep understanding of the latest developments in fraud, digital currency, e-payment, online banking, mobile wallets, artificial intelligence, and other innovative areas, enabling them to provide exceptional customer service and stay ahead of the competition.

Target Audience:

- Bank employees, including customer service representatives, branch managers, Tellers, risks, and fraud management professionals.
- Financial institution employees, including compliance officers, IT, and non-IT.
- Anyone interested in staying up to date with the latest trends and innovations in digital banking.

Course Objectives:

- Understand the latest trends and innovations in digital banking, including online banking, mobile wallets, and emerging payment technologies.
- Develop knowledge about different types of fraud in digital banking, such as phishing, smishing, vishing, and deepfake fraud, as well as strategies for fraud detection and prevention.
- Learn about digital currencies, including Bitcoin and Ethereum, and understand blockchain technology and its applications in the banking industry.
- Gain insights into various e-payment systems, including online banking, mobile payments, credit cards, and ATMs, as well as their security features, risks, and emerging trends.
- Develop skills in using online banking and mobile wallet applications, understanding their evolution, security features, risks, and best practices for secure usage.
- Understand the role of artificial intelligence (AI) and machine learning (ML) in banking, including their applications in fraud detection, customer service, and risk management, as well as ethical considerations.
- Acquire knowledge about cybersecurity threats in digital banking and strategies for mitigating risks, such as encryption, two-factor authentication, incident response, and disaster recovery planning.
- Learn about regulatory frameworks and compliance requirements for digital banking services, such as PSD2, GDPR, and PCI-DSS, as well as best practices for regulatory compliance.
- Understand the importance of customer experience in digital banking and strategies for designing effective digital channels, enhancing customer engagement, and building loyalty.
- Explore the future of banking and emerging technologies, such as quantum computing and 5G networks, and develop strategies for staying ahead of the curve in a rapidly evolving industry.

Course Outline:

Module 1: Introduction to Digital Banking

- Overview of digital banking and its impact on the financial industry.
- Key drivers of digital transformation in banking.
- Benefits and challenges of digital banking.

Module 2: Emerging Trends in Fraud

- Types of fraud in digital banking (e.g., phishing, smishing, vishing).
- Advanced fraud techniques (e.g., deepfake, AI-powered fraud).
- Fraud detection and prevention strategies.

Module 3: Digital Currencies and Blockchain

- Introduction to digital currencies (e.g., Bitcoin, Ethereum).
- Blockchain technology and its applications in banking.
- Regulatory frameworks for digital currencies.

Module 4: E-Payment Systems

- Overview of e-payment systems (e.g., online banking, mobile payments, credit cards and ATMs).
- Security features and risks associated with e-payment systems.
- Emerging trends in e-payment systems (e.g., electronic checks, contactless payments, wearables).

6550-1

In-Class

16 hours

Module 5: Online Banking and Mobile Wallets
- Evolution of online banking and mobile wallets.
- Security features and risks associated with online banking and mobile wallets.
- Best practices for online banking and mobile wallet security.

Module 6: Artificial Intelligence and Machine Learning in Banking.
- Introduction to AI and ML in banking.
- Applications of AI and ML in fraud detection, customer service, and risk management.
- Ethical considerations and challenges of AI and ML in banking.

Module 7: Cybersecurity in Digital Banking.
- Overview of cybersecurity threats in digital banking.
- Strategies for mitigating cybersecurity risks (e.g., encryption, two-factor authentication).
- Incident response and disaster recovery planning.
- Module 8: Regulatory Frameworks and Compliance.
- Overview of regulatory frameworks for digital banking (e.g., PSD2, GDPR, PCI-DSS).
- Compliance requirements for digital banking services.
- Best practices for regulatory compliance in digital banking.

Module 8: Regulatory Frameworks and Compliance.
- Overview of regulatory frameworks for digital banking (e.g., PSD2, GDPR, PCI-DSS).
- Compliance requirements for digital banking services.
- Best practices for regulatory compliance in digital banking.

Module 9: Customer Experience and Digital Channels.
- Importance of customer experience in digital banking.
- Designing effective digital channels (e.g., mobile apps, online platforms).
- Strategies for enhancing customer engagement and loyalty.

Module 10: Future of Banking and Emerging Technologies.
- Emerging technologies in banking (e.g., quantum computing, 5G networks).
- Potential impact of emerging technologies on the banking industry.
- Strategies for staying ahead of the curve in a rapidly evolving industry.

Assessment Strategy:
Participants will be informally assessed on their interaction during sessions and their participation in exercises.

Course Language:
English.

Prerequisites:
Intermediate level of English.

6550-1

In-Class

16 hours

Trainer BIO

Dr. Zakaria Abokabera:

Instructor Biography: I am Zakaria Abokabera, a renowned expert in document examination and digital forensics. With experience in the fields of signatures and currency verification, cybercrime, E-payment, Artificial intelligence, and digital fraud prevention, I am a certified instructor dedicated to educating individuals and institutions on advanced techniques in these areas. As a recognized researcher and innovator, I have developed multiple patented technologies and AI applications for documents for forensic analysis.

Education:

Bachelor of Science in Pharmacy (Honors) - Al-Azhar University, 2004 - Master in Document Fraud Detection using Spectral Chemical Analysis - Cairo University, 2020 - Ongoing PhD in Digital and Physical Document Security - Cairo University.

Certifications:

- EMRTD (Electronic Machine-Readable Travel Document)- IOM-UN.
- TOT MTRDs (Training of Trainers in Electronic Machine-Readable Travel Document)- IOM-UN IDL (Instructional Design for Learning) – EBI.
- Blending Learning Techniques – EBI.
- Advanced Instructional Strategies in the Virtual Classroom - University of California Irvine, USA - New Frontiers in Document Examination – Foster + Freeman.
- IACRB Certified Computer Forensics Examiner (CCFE) - InfoSec Institute, USA.
- IACRB Certified Mobile Forensics Examiner (CMFE) - InfoSec Institute, USA.
- AI Prompt Engineering - Google, USA.
- Online Payment Security Privacy - Newcastle University, UK.
- Introduction to Cyber Security - Open University, UK.
- Understanding Transitional Organized Crime – UNODC.
- Blockchain Business Foundations - BTA, USA.
- Fundamentals of Artificial Intelligence (AI) – Google.
- Generative AI from Google.
- Forensic 2030 Foster + Freeman.
- Crime Scene Laser Application – Foster + Freeman.
- Other specialized learning certificates.

Years of Experience at EBI:

From 2010 till present.