CENTRAL BANK OF EGYPT
Egyptian Banking Institute

Digital Banking, Payments and Financial Crime

ACCREDITED BY ACCET A Partnership for Quality®

Compliance and Governance

493-P26-VE

Virtual

32 hours

EGP 9,250

Course Description:

This course is explaining what is happening in digital banking markets as well as the implications for new and existing market participants. Focusing on the control and risk environments it also reviews the strategy and goals that will be impacted. The course considers the model for digital banking as well as the control environment. Main regulations are also considered as well as the change that is now impacting strategy and approaches. Bitcoin and other cybercurrencies as well as Blockchain and its role are also addressed. The attendees will have gained a general introduction to the structure, controls and challenges of operating in this fast-changing sector.

Target Audience:

- Internal control dept.
- risk management dept.
- Internal audit dept.
- Branch manager.
- Senior level.

Course Objectives

By the end of the program, participants will be able to:

- Define Digital Banking.
- Explain Systems of Payment and Its Risk.
- Identify Financial Crime.
- Define the AML Frameworks in Practice in Digital Banking.
- Describe the Policies and The Strategies of Cyber Security Risk Management.
- Explain Information and Systems Security Models.
- Define Financial Crime in Digital Banking.
- Identify the Change and Future (Cyber Currencies and Blockchain).

Course Outline

Module 1: Digital Banking

Session 1: Digital Banking

- Mobile banking v digital banking.
- Structure and governance of a digital bank.
- E-Banking Innovation, Trends & Directions.
- Mobile Payments and Mobile Payments Technology.
- Risk Management in E-Banking.
- Risk management principles for electronic banking.
- Operating Strategies & Management Models.
- ECB Paper – Present and future of money in the digital age (2021).
- Quiz.

Module 2: Payment Systems and Risk

Session 1: Payment Systems and Risk

- How payment systems are changing.
- The changing regulatory environment.
- Payment Services Regulations 2017.
- PSD2.
- The impact on the infrastructure.
- Bitcoin, blockchain, Ethereum and other developments.
- SWIFT and new products.
- Visa, Mastercard and other existing product providers.
- Impact on security and systems.
- Quiz.

Module 3: Financial Crime

Session 1: Financial Crime

- The importance of KYC.
- The “All Crimes” Money Laundering Offences.
- Consent and Tipping Off.
- The terrorism dimensions.
- Ongoing monitoring.
- EU 5th and 6th AML Directive.

493-P26-VE

Virtual

32 hours

EGP 9,250

- FATF on internet-based payments (June 2013).
- BIS Sound management of risks related to money laundering and financing of terrorism (July 2020).
- BIS General guidance to account opening & Wolfsberg Group SWIFT guidance (2016).
- Quiz.

Module 4: The AML Frameworks in Practice in Digital Banking

Session 1: The AML Frameworks

- Key elements of an AML framework.
- Key roles and responsibilities including the first line of defense.
- The design and implementation of a risk-based approach.
- Risk acceptance policies.
- Quiz.

Session 2: The AML Frameworks in Practice in Digital Banking

- CDD and EDD and what this will mean in practice?
- What does a PEP really mean to us?
- KYB – what are we really responsible for?
- Record keeping.
- The importance of the sanction's regime globally.
- Solutions and data mining.
- Quiz.

Module 5: Cyber Security Risk Management Policies and Strategies

Session 1: Cyber Security Risk Management Policies and Strategies

- What is a cyber security risk management strategy?
- Cyber-resilience: Range of practice (BCBS d454 2018).
- The benefits of a cybersecurity strategy.
- Building an Enterprise Security Architecture (ESA).
- The approaches for developing an effective strategy.
- The meaning of security policy.
- Cyber security policy.
- Security policy principles.
- Quiz.

Module 6: Information and Systems Security Models

Session 1: Information and Systems Security Models

- Conceptual and Logical security models.
- Cyber security challenges and solutions.
- Business data model and file security mechanisms.
- Database security mechanisms.
- Cryptographic mechanisms and their uses.
- Access Control and authentication.
- Network and application security.
- Systems security.
- Penetration testing and dealing with incidents.
- Quiz.

Module 7: Financial Crime in Digital Banking

Session 1: Financial Crime in Digital Banking

- Detecting and combating money laundering activities:
  - Building profiles & "fingerprints".
  - Clustering.
  - Link analysis.
- Data mining and fraud detection:
  - Text mining.
  - Neural data mining.

Session 2: Data mining

- Data mining and other types of financial crime:
  - Tax evasion.
  - Corruption.
  - Insider dealing, market abuses.
  - Others.
- Quiz.

Module 8: The Change and The Future

Session 1: The Change and The Future

- The impact of faster banking.
- Cryptocurrency.

493-P26-VE

Virtual

32 hours

EGP 9,250

- Blockchain.
- RTP and other solutions.
- The future.
- Quiz.

Module 9: Impact Session

- Gathering feedback from participants to recap the key topics covered in the training.
- Group activity (split the participants into groups to share experience, by discussing challenges faced and successes achieved, then share the top challenges and solutions to the whole group for more effective outcomes).
- Encouraging the participants to solve a case study by sharing one takeaway to apply what they learned.

Assessment Strategy:

- 80% quizzes between sessions.
- 20% Participation.
- 60% cut-off-score.

Upon Successful Completion of this Course, Participants will obtain:

2.9 CEUs

Course Language:

English.

Perquisites:

None.

Certificate requirements:

Participants must attend an impact session, which will take place 3–4 weeks after the last day of the course, in order to receive the certificate. This session will last two hours, and its duration will be included in the total program hours. In addition to completing all the required assignments and attending at least 80% of the course duration.