QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1417

AML for Digital Banking & FinTech Training Course

COMPLIANCE, AML & FINANCIAL CRIME
FINANCE, INVESTMENT & BANKING

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The rapid growth of Digital Banking and Financial Technology (FinTech) has transformed the global financial services landscape, enabling organizations to deliver faster, more accessible, and highly innovative financial products and services. However, this digital transformation has also introduced new Anti-Money Laundering (AML) challenges, creating increased exposure to money laundering, terrorist financing, cyber-enabled financial crime, and regulatory compliance risks.

AML for Digital Banking & FinTech Training Course is designed to equip professionals with the knowledge, skills, and practical tools required to identify, assess, monitor, and mitigate money laundering risks within digital financial ecosystems. The course provides a comprehensive understanding of how AML frameworks must evolve to address emerging technologies, digital customer onboarding, electronic payments, virtual assets, digital wallets, and innovative FinTech business models.

Participants will gain valuable insights into international AML regulations, risk-based compliance strategies, customer due diligence requirements, transaction monitoring practices, and financial crime prevention mechanisms applicable to digital banking environments. The course also explores the impact of regulatory expectations on digital financial institutions and how organizations can establish effective AML controls while maintaining innovation and operational efficiency.

In an increasingly regulated and technology-driven environment, financial institutions, FinTech companies, regulators, and compliance professionals must ensure that digital transformation initiatives are supported by robust AML governance, risk management, and monitoring frameworks. Effective AML programs not only support regulatory compliance but also protect organizational reputation, customer trust, and long-term business sustainability.

Through practical case studies, real-world examples, interactive discussions, and implementation-focused exercises, this course enables participants to strengthen their institution’s AML capabilities and develop proactive strategies for combating financial crime in modern digital banking and FinTech operations.

Objectives

- Analyze money laundering and financial crime risks associated with digital banking platforms and FinTech services during the course.
- Evaluate international AML regulations, standards, and regulatory expectations applicable to digital financial institutions.
- Apply risk-based approaches to identify, assess, and manage AML risks across digital products, services, and customer segments.
- Develop effective customer due diligence and digital identity verification procedures.
- Design transaction monitoring frameworks capable of detecting suspicious activities in digital environments.
- Implement AML controls for digital payments, e-wallets, virtual assets, and FinTech platforms.
- Assess emerging threats and vulnerabilities associated with digital financial services and technologies.
- Improve compliance effectiveness through advanced monitoring, analytics, and automation tools.
- Strengthen organizational capabilities in suspicious activity investigation and reporting processes.
- Align AML governance structures with regulatory requirements and business objectives.
- Develop practical strategies for managing AML risks across digital banking and FinTech operations.
- Evaluate organizational readiness for evolving financial crime and compliance challenges.

Who Should Attend

This course is designed for AML professionals, compliance officers, financial crime specialists, risk managers, internal auditors, governance professionals, and regulatory compliance personnel working within banks, financial institutions, and FinTech organizations.

It is particularly beneficial for professionals involved in digital banking operations, electronic payments, mobile banking, digital transformation initiatives, customer onboarding, financial technology solutions, fraud prevention, information security, and transaction monitoring functions. Individuals responsible for implementing compliance programs and managing regulatory relationships will also gain significant value from the program.

The course is equally relevant for executives, department heads, decision makers, regulatory authorities, financial investigators, consultants, and professionals responsible for managing financial crime risks, ensuring compliance, and supporting innovation within digital financial ecosystems.

Learning Outcomes

- By the end of this course, participants will be able to:
- Identify key money laundering risks within digital banking and FinTech environments.
- Interpret AML regulatory requirements applicable to digital financial services.
- Conduct risk assessments for digital products, customers, and delivery channels.
- Apply customer due diligence and enhanced due diligence procedures effectively.
- Design and enhance transaction monitoring systems for digital financial activities.
- Detect suspicious transaction patterns and financial crime indicators.
- Evaluate risks associated with digital payments, virtual assets, and emerging technologies.
- Implement practical AML controls across digital banking and FinTech operations.
- Strengthen investigation processes and suspicious activity reporting practices.
- Utilize data analytics and technology solutions to improve AML effectiveness.
- Support organizational compliance objectives through risk-based AML frameworks.
- Develop actionable plans to enhance AML governance and compliance performance.

Course Outline

DAY 01

AML Fundamentals for Digital Banking and FinTech

- Evolution of digital banking and financial technology ecosystems
- Fundamentals of money laundering and terrorist financing
- Financial crime risks in digital financial services
- International AML standards, regulations, and compliance requirements

> PRACTICAL DISCUSSION
>
> Emerging AML challenges in digital banking and FinTech

DAY 02

Risk Assessment and Digital Customer Due Diligence

- Risk-based AML frameworks for digital financial institutions
- Customer risk assessment methodologies
- Digital onboarding and identity verification processes
- Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)

> **PRACTICAL APPLICATION**
>
> Conducting AML risk assessments for digital customers

DAY 03

Transaction Monitoring and Suspicious Activity Detection

- Transaction monitoring principles and methodologies
- Monitoring digital payments and electronic transactions
- Identifying suspicious activity indicators and red flags
- Case management, alert investigation, and escalation procedures

> **PRACTICAL WORKSHOP**
>
> Analyzing suspicious transaction scenarios

DAY 04

AML Controls for FinTech and Digital Financial Services

- AML governance and compliance program design
- Managing risks in e-wallets, mobile payments, and digital platforms
- AML considerations for virtual assets and emerging technologies
- Roles and responsibilities across compliance, risk, and business functions

> **PRACTICAL EXERCISE**
>
> Evaluating and strengthening AML control frameworks

DAY 05

Advanced Technologies and Future AML Strategies

- Artificial intelligence and machine learning in AML compliance
- Data analytics and automation for financial crime detection
- Regulatory technology (RegTech) solutions for AML programs
- Building a future-ready AML strategy for digital banking and FinTech

> **FINAL WORKSHOP**
> Developing an AML improvement roadmap and implementation action plan

Register or Request More Information

Course page: https://quest-training.com/courses/aml-for-digital-banking-fintech-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440