Financial Crime Compliance for Banks Training Course

Professional Development Training Course Outline

Category	Banking Institute	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The modern financial landscape is increasingly defined by the rapid evolution of digital assets, artificial intelligence (AI), and sophisticated cross-border financial crime typologies. Banks today face an unprecedented surge in regulatory scrutiny, where the integration of RegTech and proactive risk-based approaches is no longer optional but a critical pillar of institutional integrity. Financial Crime Compliance for Banks Training Course is engineered to equip banking professionals with the advanced technical acumen required to navigate the complex interplay between innovation and security, ensuring robust defenses against money laundering, terrorist financing, and cyber-enabled fraud.

By bridging the gap between theoretical regulatory frameworks and operational realities, this program fosters a culture of compliance excellence and organizational accountability. Through immersive, high-stakes learning environments, participants will move beyond standard procedural knowledge to develop the critical thinking skills necessary for real-time anomaly detection and strategic risk mitigation. This initiative is dedicated to transforming compliance from a reactive necessity into a competitive advantage, safeguarding your institution's reputation and financial health in an era of hyper-connected threats.

Programme Curriculum

Financial Crime Compliance for Banks Training Course

Introduction

The modern financial landscape is increasingly defined by the rapid evolution of digital assets, artificial intelligence (AI), and sophisticated cross-border financial crime typologies. Banks today face an unprecedented surge in regulatory scrutiny, where the integration of RegTech and proactive risk-based approaches is no longer optional but a critical pillar of institutional integrity. Financial Crime Compliance for Banks Training Course is engineered to equip banking professionals with the advanced technical acumen required to navigate

the complex interplay between innovation and security, ensuring robust defenses against money laundering, terrorist financing, and cyber-enabled fraud.

By bridging the gap between theoretical regulatory frameworks and operational realities, this program fosters a culture of compliance excellence and organizational accountability. Through immersive, high-stakes learning environments, participants will move beyond standard procedural knowledge to develop the critical thinking skills necessary for real-time anomaly detection and strategic risk mitigation. This initiative is dedicated to transforming compliance from a reactive necessity into a competitive advantage, safeguarding your institution's reputation and financial health in an era of hyper-connected threats.

Course Duration

5 days

Course Objectives

1. Master the application of risk-based approaches (RBA) in identifying emerging threats.
2. Implement advanced Customer Due Diligence (CDD) and KYC protocols for high-risk entities.
3. Analyze the impact of generative AI on both financial crime and detection capabilities.
4. Navigate the evolving landscape of digital asset and DeFi (Decentralized Finance) regulations.
5. Develop expertise in transaction monitoring and reducing alert fatigue through automation.
6. Understand the legal requirements and operational nuances of Sanctions Screening.
7. Enhance proficiency in preparing and submitting high-quality Suspicious Activity Reports (SARs).
8. Identify and mitigate Trade-Based Money Laundering (TBML) red flags.
9. Strengthen governance surrounding Politically Exposed Persons (PEPs) and Beneficial Ownership.
10. Integrate RegTech solutions for more efficient regulatory reporting and data management.
11. Combat Cyber-enabled financial fraud and identity theft through enhanced security measures.
12. Establish effective internal controls and audit readiness for regulatory examinations.
13. Promote an ethical culture of compliance to foster organizational resilience.

Target Audience

- Compliance Officers & AML Specialists
- Risk Managers & Internal Auditors
- Front-Office Relationship Managers
- Banking Operations & Transaction Monitoring Teams
- Legal Counsel & Regulatory Liaison Officers
- Senior Management & Board Members
- FinTech Strategy & Innovation Leaders
- Cybersecurity & IT Security Analysts

Training Modules

Module 1: Foundations of Financial Crime Governance

- Understanding the global AML/CTF regulatory landscape.
- Defining the roles of the MLRO and the board in risk oversight.
- Establishing a robust institutional compliance framework.
- Aligning internal policies with international legal obligations.
- **Case Study:** Analysis of a global bank's failure in governance leading to multi-billion dollar regulatory fines.

Module 2: Advanced Customer Due Diligence (CDD) & KYC

- Implementing tiered risk-profiling for diverse customer segments.
- Mastering Beneficial Ownership identification in complex legal structures.
- Conducting Enhanced Due Diligence (EDD) for high-risk jurisdictions.
- Leveraging biometric and digital verification technologies.
- **Case Study:** Investigating the use of shell companies to obscure beneficial ownership in high-profile corruption scandals.

Module 3: Digital Assets & The DeFi Threat Landscape

- Regulatory challenges in crypto-asset and blockchain-based transactions.
- Identifying red flags unique to virtual asset service providers (VASPs).
- Applying the "Travel Rule" to ensure regulatory transparency.
- Managing the intersection of Decentralized Finance (DeFi) and AML.
- **Case Study:** Deconstructing a "pig-butchering" scam involving cryptocurrency laundering through decentralized exchanges.

Module 4: Transaction Monitoring & AI Integration

- Transitioning from rule-based systems to AI-powered predictive analytics.
- Strategies to optimize detection rates while minimizing "alert fatigue."
- Identifying patterns in structuring, smurfing, and rapid fund movement.
- Collaborating with IT to calibrate monitoring thresholds effectively.
- **Case Study:** How AI-driven anomaly detection successfully identified an automated money-mule network.

Module 5: Sanctions & Trade-Based Money Laundering (TBML)

- Navigating complex, overlapping US, EU, and UK sanctions regimes.
- Detecting irregularities in trade finance documentation and invoicing.
- Monitoring high-risk correspondent banking relationships.
- Strategies for responding to rapid shifts in global geopolitical sanctions.
- **Case Study:** Tracking illicit dual-use goods through a series of "phantom" trade shipments and front companies.

Module 6: Cyber-Fraud & Digital Financial Crime

- Recognizing the evolution of phishing, ransomware, and identity theft.
- Protecting client data and ensuring secure digital authentication.
- The role of generative AI in synthetic identity fraud creation.
- Coordinated incident response protocols for financial institutions.
- **Case Study:** Managing the aftermath of a sophisticated Business Email Compromise (BEC) attack on a corporate client.

Module 7: Reporting, Investigations & Intelligence

- Writing impactful, actionable Suspicious Activity Reports (SARs).
- Techniques for conducting thorough internal financial investigations.
- Collaborating with Financial Intelligence Units (FIUs) and law enforcement.
- Maintaining strict confidentiality and chain-of-custody in evidence.

- **Case Study:** A successful inter-agency investigation triggered by a high-quality internal SAR submission.

Module 8: Building a Proactive Culture of Compliance

- Implementing "Courageous Conversations" and internal whistleblowing channels.
- Linking compliance metrics to individual performance and accountability.
- Continuous professional development and maintaining industry certification.
- Adapting training modules to address emerging threats in real-time.
- **Case Study:** A deep dive into an organization that transformed its compliance culture from "checkbox" to "proactive risk management."

Training Methodology

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

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	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 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