€TRAINING

Mitigating Financial Crime Risks in Banking

13 - 17 October 2025
Barcelona (Spain)

Mitigating Financial Crime Risks in Banking

REF: F1752 DATE: 13 - 17 October 2025 Venue: Barcelona (Spain) - Fee: 5565 Euro

Introduction:

This training program explores the risks of financial crime in the banking sector, covering the key practices and strategies to mitigate these risks. It empowers them to strengthen their understanding of financial crime, including fraud, money laundering, and cybercrime, to protect their institutions and ensure compliance with regulatory standards.

Program Objectives:

At the end of this program, participants will be able to:

- Explore the various types of financial crimes affecting banks.

- Identify and assess risks related to fraud, money laundering, and cybercrime.

- Implement strategies to mitigate financial crime risks.

- Ensure compliance with anti-money laundering AML and counter-terrorism financing CTF regulations.

- Leverage technology to detect and prevent financial crimes.

Targeted Audience:

- Risk Managers.

- Compliance Officers.

- Fraud Prevention Specialists.

- Bank Managers.

- Financial Crime Analysts.

Program Outline:

Unit 1:

Understanding Financial Crime in Banking:

- Overview of financial crime in the banking sector.

- Types of financial crimes: fraud, money laundering, cybercrime, and bribery.

- Impact of financial crime on banks and financial stability.

- Key regulatory frameworks governing financial crime.

- The role of financial institutions in combating financial crime.

Unit 2:

Fraud Detection and Prevention:

- Common types of fraud in the banking industry.

- Techniques for detecting and preventing fraud.

- Developing an effective fraud risk management framework.

- Internal controls and anti-fraud policies.

Unit 3:

Anti-Money Laundering AML and Counter-Terrorism Financing CTF:

- Understanding money laundering and terrorism financing.

- Key components of AML and CTF regulations.

- Customer due diligence CDD and Know Your Customer KYC procedures.

- Transaction monitoring and suspicious activity reporting.

- Compliance challenges and best practices for AML/CTF.

Unit 4:

Cybercrime and Financial Institutions:

- Overview of cybercrime risks in the banking sector.

- Key types of cyber attacks targeting financial institutions.

- Implementing cybersecurity measures to protect against financial crimes.

- Incident response and recovery plans for cybercrime.

- Regulatory requirements related to cybersecurity in banking.

Unit 5:

Leveraging Technology for Financial Crime Prevention:

- The role of artificial intelligence AI and machine learning in detecting financial crime.

- Automating compliance processes with regtech solutions.

- Data analytics for risk assessment and monitoring.

- Blockchain and its potential in preventing financial crime.

- Future trends in technology and financial crime prevention.