



# Syllabus

# STEP Certificate in Anti-Money Laundering



[www.step.org/qualifications](http://www.step.org/qualifications)

# Anti-Money Laundering

## Introduction

This document contains the detailed syllabus for the STEP Certificate in Anti-Money Laundering .

For more information about the course and how to apply, please visit the [course page](#) on the CLTI website.



Our education partner



# Anti-Money Laundering

## Module 1

### WHAT ARE THE MONEY LAUNDERING, TERRORIST FINANCING AND SANCTIONS RISKS THAT MUST BE MANAGED?

#### **This module covers:**

- What is money laundering?
  - How is money laundered?
  - A modern assessment of money laundering
  - Predicate offences
  - Money laundering and corruption
  - Money laundering and tax evasion
  - Why is money laundering prevention important?
- Terrorist Financing
  - What is terrorist financing?
  - The threat of terrorism
  - How is terrorism financed?
  - Movement of terrorist funds
- Proliferation finance
  - What is proliferation financing
  - Dual-use items
  - The risks arising from proliferation financing
- Financial and economic sanctions
  - What are sanctions?
  - Why are sanctions important?
  - United Nations Sanctions Framework
  - Regional sanctions
  - National Sanctions framework: UK, US and China



Our education partner



# Anti-Money Laundering

## **By the end of this module you should be able to:**

- understand what money laundering is and appreciate the range of underlying predicate offences
- recognise how and why criminal proceeds are laundered, including the three-stage module and its limitations
- define terrorist financing and how it resembles, and differs from, money laundering
- understand the variety of methods used to finance terrorism and how it can involve both legitimately earned and criminally sourced money
- understand what is meant by proliferation financing and the risks associate with it
- explain what sanctions are, know the bodies that impose them and understand the role of sanctions in international relations and law, and
- describe a variety of different types of sanction and explain how they are implemented in a variety of sanctions regimes.



Our education partner



# Anti-Money Laundering

## Module 2

### THE INTERNATIONAL BODIES AND STANDARD SETTERS

#### **This module covers:**

- The role of the international bodies
- Key international organisations
  - The International Monetary Fund
  - The United Nations
  - The World Bank
  - The Financial Action Task Force
  - Transparency International
  - The European Union
  - The Basel Committee on Banking Supervision
  - The Egmont Group
  - The Wolfsberg Group
- The work of the international bodies and its relevance for AML practitioners
  - Understanding the nature of the threat
  - Use in risk assessments

#### **By the end of this module you should be able to:**

- demonstrate a broad understanding of the roles of the IMF, the UN and the World Bank as international standard-setters in combating money laundering and terrorist financing
- appreciate the roles of the Basel Committee, the European Commission, the Egmont Group and the Wolfsberg Group, which regulate and/or provide guidance to the financial services sector

# Anti-Money Laundering

- explain the key international initiatives of the above organisations, designed to counter money laundering and terrorist financing
- describe the role of FATF and FSRBs in setting and assuring standards
- explain how FATF Mutual Evaluations of countries against the international standards are conducted, and
- outline how the work of international bodies can benefit an AML professional.



Our education partner



# Anti-Money Laundering

## Module 3

### NATIONAL LEGAL AND REGULATORY FRAMEWORKS

#### This module covers:

- The impact of the FATF standards and recommendations on domestic frameworks
- US primary legislation and regulation
  - Bank Secrecy Act 1970
  - The PATRIOT Act
  - The US Anti-Money Laundering Act 2020
  - Key US regulatory and law enforcement authorities
- United Kingdom
  - Primary legislation: The Proceeds of Crime Act 2002
  - Secondary legislation: The Money Laundering Regulations 2017
  - Industry and professional guidance
  - Financial Conduct Authority supervisory rules and enforcement
  - Key UK law enforcement authorities
- Jersey strategy on money laundering and terrorist financing
  - Legislative framework
  - Secondary legislation
  - Compliance with international AML/CFT standards
- Singapore
  - CDSA
  - TSOFA
  - Monetary Authority of Singapore (MAS)
- People's Republic of China

# Anti-Money Laundering

- India
  - The Reserve Bank of India (RBI)
  - Indian FIU
- United Arab Emirates (UAE)
  - Supervisory authority
  - FATF Mutual Evaluation of the UAE

## **By the end of this module you should be able to:**

- appreciate the differences between primary and secondary legislation and the various kinds of guidance published in major financial centres
- be able to outline the general legal and regulatory requirements within domestic legislation in a range of countries, namely the US, the UK, Singapore, China, India and the UAE
- appreciate the impact that extraterritorial legislation, such as the US BSA and the Patriot Act, can have in other jurisdictions, and
- understand how knowledge of different national AML frameworks, enforcement actions and FATF Mutual Evaluations are valuable to an AML practitioner.

# Anti-Money Laundering

## Module 4

### TAKING AN AML/CFT RISK-BASED APPROACH AND MANAGING THE RISKS

#### **This module covers:**

- What is an AML/CFT risk-based approach?
  - FATF guidance on the risk-based approach
  - National risk assessments
- Determining the risks
  - Business risk assessments: organisations and operational risks
  - Assessing sector risk
  - Assessing product and service risk
  - Delivery channel risk
  - Geographical risk
  - Customer risk
- Management of AML/CFT risks
  - Implementing a risk-based approach
- AML roles and responsibilities
  - The role of senior management
  - The role of the money laundering reporting officer
  - The MLCO/MLRO's role in money laundering risk assessment
  - Managing relationships with law enforcement agencies and regulators
- Escalation to senior management
- Exiting relationships



Our education partner



# Anti-Money Laundering

## **By the end of this module you should be able to:**

- appreciate the types of risk a firm may face and be able to outline the principles and benefits of an RBA
- be able to explain how the risks facing a particular business are determined
- understand how a risk-based approach is implemented
- recognise the responsibilities of the board and senior management
- be able to explain the role and duties of the MLCO/MLRO, and
- understand matters to be taken into consideration when escalating or exiting relationships.

# Anti-Money Laundering

## Module 5

### INITIAL AND 'ONGOING' CUSTOMER DUE DILIGENCE (CDD)

#### **This module covers:**

- What is customer due diligence (CDD)?
  - The basic international standard
  - The basic European and UK domestic standard
  - Who is the customer and what is meant by the identification of beneficial owners?
- The risk-based approach to CDD
  - The requirements of the international standards
  - Practical application of the risk-based approach to CDD
  - Risk-based CDD requirements for existing customers
- The practical application of CDD
  - Interpretation of the key CDD terminology
  - CDD for specific risk situations
- Simplified due diligence and lower risk situations
  - What is SDD?
  - Lower risk situations
  - Exceptions made to guard against financial exclusion
- Higher-risk situations and enhanced due diligence
  - What is EDD?
  - When is enhanced due diligence required?
  - High risk: non-face-to-face
  - Mandatory high-risk customers: PEPs
  - The need of a PEP policy
  - De-classification of a customer as a PEP

# Anti-Money Laundering

- EDD: establishing source of wealth
- Mandatory high-risk relationships: correspondent banking
- Other examples of high-risk situations
- Unacceptable relationships
- Identifying and verifying identity
  - Who must be identified and why?
  - Digital verification of identity
  - Identifying and verifying the identity of corporate entities
  - Relying on third parties and accepting introduced business
- The extent of additional information to be collected
- 'Ongoing CDD' and monitoring relationships
  - Trigger event monitoring
  - The challenges to be overcome
- Testing the CDD process

## **By the end of this module you should be able to:**

- understand the definitions of CDD in FATF Recommendation 10 and its Interpretive Note
- be able to explain what is meant by regulatory terminology on CDD
- recognise the practical ways of applying a risk-based approach to CDD, including assessment of high-risk and low-risk situations for both new and existing customers
- appreciate what is involved in EDD and when it should be applied, especially in the case of PEPs
- understand how CDD is applied in correspondent banking relationships and other higher-risk corporate relationships, and
- recognise the various methods of identifying and verifying customers' identities, the identification requirements, and the application of electronic methods of identity verification.



Our education partner



# Anti-Money Laundering

## Module 6

### MONITORING ACTIVITY AND TRANSACTIONS

#### **This module covers:**

- The developing standards for monitoring transactions and activity
  - Customer profiling and using CDD information for monitoring purposes
  - Transaction records
  - Monitoring processes adding value to the AML/CTF regime
- Risk-based transaction monitoring and filtering framework
  - Transaction monitoring programmes
  - Automated transaction monitoring systems
  - Escalation processes
  - MI and exception reporting
- International Standards and wire transfer requirements
  - The EU Wire Transfer Regulation
- Sanctions lists and screening
  - Who should be screened?
  - Screening systems and controls

#### **By the end of this module you should be able to:**

- understand how FATF Recommendation 10 is applied in practice in the financial services sector and the developing risks that monitoring must address
- be able to use CDD information as part of monitoring processes and appreciate its importance in combating money laundering and terrorist financing
- be able to outline key risks relating to transaction monitoring and filtering activities

# Anti-Money Laundering

- understand international wire transfer requirements and be able to apply them
- be able to describe measures necessary for an effective transaction monitoring framework, and
- understand who should be subject to sanctions screening and control requirements, the sort of screening systems that can be used, and the advantages of applying robust systems.



Our education partner



# Anti-Money Laundering

## Module 7

### RECOGNISING AND REPORTING SUSPICIONS

#### **This module covers:**

- The international requirements
- Currency transaction reporting
  - The US dual reporting requirements
- National requirements (EU and UK)
- What is meant by suspicion and reasonable grounds to suspect?
  - The subjective test of suspicion
  - Reasonable grounds to suspect; the objective test of suspicion
- Setting reporting rules and parameters
  - The issues for consideration
  - Cross-border reporting obligations
  - What constitutes suspicious activity?
- The SAR/STR process and its documentation
  - Acknowledging an SAR/STR
  - Reasons for reporting
  - Making enquiries
  - The MLCO/MLRO evaluation process
  - Avoiding tipping off
- Balancing the needs of law enforcement with breach of customer confidentiality
  - The interface with data protection

# Anti-Money Laundering

## **By the end of this module you should be able to:**

- understand and be able to give examples of what is meant by suspicion and reasonable grounds to know or suspect, and the difference between the subjective and objective tests of suspicion
- understand how suspicions are generally formulated and appreciate the sort of behaviours ('red flags') by a customer that should generate suspicions
- be able to design a system for staff to use in reporting suspicions to the MLRO and the procedures to be followed by the MLRO on receipt of such reports
- know when and how to make a valuable and accurate SAR to law enforcement agencies once a suspicion has formed
- appreciate the problems that can arise from conflicts between legal obligations to report and the need to maintain customer confidentiality, and
- understand the risks of tipping off and the MLCO's/MLRO's duty to help staff avoid this.

# Anti-Money Laundering

## Module 8

### THE VULNERABILITIES OF SPECIFIC SERVICES AND PRODUCTS

#### This module covers:

- Introduction
- Retail banking services
  - Basic current/checking accounts and savings/ deposit accounts
- Private banking
- Correspondent banking
- Lending and credit
  - Credit/charge cards and stored-value cards
  - Consumer finance
  - Mortgage lending
- International trade and trade finance
- Foreign exchange and money transfer services
  - Foreign exchange bureaux
  - Money services businesses including alternative remittance systems
- Trust and corporate service providers
  - Corporate service providers
  - Trustee services
  - Tax evasion through offshore trusts and companies
- Insurance
  - Life insurance
  - General insurance
- The gaming industry
- Internet payment systems
- Virtual assets and virtual asset service providers



Our education partner



# Anti-Money Laundering

## **By the end of this module you should be able to:**

- be familiar with the money laundering vulnerabilities of specific financial services and products, such as bank accounts and wire transfers and any others to which you are exposed in your employment
- be aware of how various service providers, such as banks, trusts and CSPs, may be vulnerable to exploitation by money launderers and terrorist financing activities
- be able to recognise how financial systems outside the mainstream, such as ARS, may interact with conventional financial services and expose them to risk
- appreciate the sorts of suspicious activity that may be encountered in the gaming sector
- have an awareness of internet payments and virtual currencies and their potential for criminal use, and
- have an awareness of money laundering typologies for the sectors discussed in this unit.