STEP CERTIFICATE IN ANTI-MONEY LAUNDERING

Syllabus

In collaboration with

ICA INTERNATIONAL COMPLIANCE ASSOCIATION

Delivered by

CLTI

30 YEARS OF STEP

INTRODUCTION

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

This syllabus should be read in conjunction with the course brochure, which explains the method of delivery and assessment, entry requirements and personal and business benefits of completing the programme. The brochure, course dates and enrolment application form can also be found on the programme's website **www.cltint.com/course/step-aml**

MODULE 1: WHAT ARE THE MONEY LAUNDERING AND TERRORIST FINANCING RISKS THAT MUST BE MANAGED?

This module covers:

- What is money laundering?
  - What role can the financial sector play?
  - How is money laundered?
  - A modern assessment of money laundering
  - The money laundering offences
  - The links between money laundering and corruption
  - Money laundering and tax evasion
  - Why is money laundering prevention important?
- Terrorist financing
  - What is terrorist financing?
  - How is terrorism financed?
  - What is an alternative remittance system?
- Financial and economic sanctions
  - What are sanctions?
  - Why are sanctions important?
  - United Nations Sanctions Framework
  - Regional sanctions
  - The UK sanctions regime
  - US (OFAC) regime
  - Country restrictions
  - Local sanctions laws
  - The cost of getting it wrong
- Proliferation finance
  - Dual-use items
  - The risks arising from proliferation financing

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 model and its limitations
- Be able to 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
- Explain what sanctions are, know the bodies that impose them and understand their role in international relations and law
- Describe a variety of different types of sanction and explain how they are implemented in a variety of sanctions regimes
- Understand what is meant by proliferation finance and the risks that involvement with it poses for financial institutions

MODULE 2: THE INTERNATIONAL BODIES AND STANDARD SETTERS

This module covers:

- The International Monetary Fund
- The role of the international bodies
- Key international organisations
  - United Nations Global Programme against Money Laundering
  - The World Bank
  - The Financial Action Task Force
  - The Basel Committee on Banking Supervision
  - The European Commission and Council
  - The Egmont Group
  - The Wolfsberg Group
  - Transparency International
- The work of the international bodies and its relevance for AML practitioners
- FATF mutual evaluations
- Typologies and guidance
- The focus of transparency

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

- Have a broad understanding of the roles of the IMF, UN and 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
- Be familiar with the key international initiatives of the above organisations, designed to counter money laundering and terrorist financing
- Be able to describe the role of the Financial Action Task Force and the FATF Style Regional Bodies in setting and assuring standards
- Understand how FATF mutual evaluations of countries against the international standards are conducted
- Recognise the link between the international AML/CFT standards and the transparency of beneficial ownerships of corporate vehicles, and be able to explain the work of Transparency International

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
  - Other related AML/CFT legislation
- Key US regulatory and law enforcement authorities
  - Lessons from enforcement actions
- United Kingdom
  - Primary legislation: The Proceeds of Crime Act 2002
  - Secondary legislation: The Money Laundering Regulations 2007
  - Industry and professional guidance
  - Financial Conduct Authority supervisory rules and enforcement
  - Key UK law enforcement authorities
  - The UK as a high-risk jurisdiction
- Examples of other jurisdictions
  - Singapore
  - Hong Kong India
  - United Arab Emirates

By the end of this module you should:

- Understand the basic requirements of the FATF standards and 40 Recommendations, and how and why these have developed as they have
- 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, Hong Kong, India and the UAE
- Appreciate the impact that US legislation such as the BSA and the Patriot Act can have in other jurisdictions, i.e. US extraterritoriality
- Understand how knowledge of enforcement actions is valuable to MLROs and be able to cite examples

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
  - Customer risk
  - Geographical risk - delivery channel risk
- Management of AML/CFT risks - implementing a risk-based approach
- Anti-money laundering roles and responsibilities within a financial services business
  - 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

By the end of this module you should:

- Appreciate the types of risk a firm may face and be able to outline the principles and benefits of a risk-based approach
- Be able to explain how the risks facing a particular business are determined and know the official guidance available to help do this
- Understand how a risk-based approach is implemented
- Understand the importance of a robust governance structure for money laundering prevention, the responsibilities of the board/senior management and the clear allocation of roles and responsibilities throughout the organisation
- Be able to explain the role and duties of the MLCO/MLRO and list the key skills required to discharge these duties
- Understand matters to be taking into consideration when escalating or exiting relationships

MODULE 5: INITIAL AND 'ONGOING' CUSTOMER DUE DILIGENCE (CDD)

This module covers:

- What is CDD?
  - The basic European and 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
- Lower-risk situations and simplified due diligence
  - What does simplified due diligence mean?
  - Exceptions made to guard against financial exclusion
- Higher-risk situations and enhanced due diligence
  - When is enhanced due diligence required?
  - What is enhanced due diligence?
  - Mandatory high-risk customers: PEPs
  - Mandatory high-risk relationships: correspondent banking
  - Other examples of high-risk situations
  - Unacceptable relationships
- The practical application of CDD
  - Interpretation of the key CDD terminology
  - CDD for specific risk situations
- Identifying and verifying identity
  - Who must be identified and why?
  - Electronic verification of identity
  - Identifying and verifying the identity of corporate entities
  - Beneficial ownership and complex structures
  - 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:

- Understand the definitions of Customer Due Diligence in FATF Recommendation 10 and its Interpretive Note
- Understand 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 enhanced due diligence 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
- Be able to explain what is meant by regulatory terminology on CDD and know some practical methods of CDD that can be applied in relation to specific types of customer or transaction
- Understand the various methods of identifying and verifying customers' identities, the identification requirements in the US and EU, and the application or electronic methods of identity verification
- Know what you need to do to discover the beneficial owners of corporate structures
- Understand what is meant by 'ongoing CDD' and the importance of regular reviews of customers' accounts and activity
- Understand the importance of assuring the effectiveness of an organisation's CDD processes and the related responsibilities of senior management

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/CFT regime
- Risk-based transaction monitoring and filtering framework
  - Transaction monitoring programmes
  - Automated transaction monitoring systems
  - Escalation processes
  - MI and exception reporting
- Wire transfer requirements of the International Standards
  - 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:

- 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 the monitoring processes and appreciate the importance of the latter in combating money laundering and terrorist financing
- Be able to outline key risks relating to transaction monitoring and filtering activities and know how to use this knowledge in creating a risk-based transaction monitoring and filtering framework
- Appreciate the strengths and weaknesses of automated transaction monitoring systems
- Understand international wire transfer requirements and be able to apply them
- Be able to describe measures necessary for establishing control standards for an effective transaction monitoring framework
- 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

MODULE 7: RECOGNISING AND REPORTING SUSPICIONS

This module covers:

- The international requirements
- Currency transaction reporting
  - The US dual reporting requirements
- EU and UK requirements
  - UK-specific requirements: a summary reminder
- 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 requirements

By the end of this module you should:

- 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 behaviour ('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
- Understand the risks of tipping off and the MLCO/MLRO's duty to help staff avoid this

MODULE 8: THE VULNERABILITIES OF SPECIFIC SERVICES AND PRODUCTS

This module covers:

- Banking services
  - Retail banking services
  - Private banking
- Correspondent banking
- Lending and Credit
  - Credit/charge cards and stored-value cards
  - Consumer finance
  - Mortgage lending
- International trade and trade finance
  - Letters of credit
- 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 sector
- Internet payment systems and virtual currencies
  - Risk factors within internet service providers
  - Digital virtual currencies

By the end of this module you should:

- 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, trust and CSPs, may be vulnerable to exploitation by money launderers and terrorist-financing activities
- Be aware of 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 the rapidly developing sectors of internet payments and virtual currencies and their potential for criminal use
- Have an awareness of money laundering typologies for the sectors discussed in this module

CONTACT US

For full details of the programme visit:

www.cltint.com/course/step-aml

If you have any queries please contact us:

Email: cltinternational@centlaw.com

Phone: +44 (0) 121 362 7733

CLT International Ltd, Wilmington plc

Fort Dunlop | 6th Floor | Fort Parkway

Birmingham | B24 9FD | United Kingdom