

ICA Certification in Anti Money Laundering and Counter Financing of Terrorism (Malaysia)

Syllabus

Learning Level: Intermediate

Introduction

This certification is designed for those who wish to possess an understanding of the complexities surrounding anti money laundering (AML) and counter financing of terrorism (CFT) today.

You will develop a practical understanding of AML principles and equip yourself with all of the knowledge required to begin or further a career in AML. You will learn how to manage the risks of money laundering, terrorist financing, sanctions, and gain an understanding of international initiatives to counter money laundering and terrorist financing. In addition, you will examine the importance and purpose of a robust governance structure in money laundering prevention and learn to identify the different money laundering typologies associated with different sectors such as money services business and insurance.

Using an immersive scenario to bring knowledge to life, you will practice your skills in AML risk management and under the guidance of the



facilitator, enhance your ability to better manage compliance issues relating to your firm. You will be asked to review and assess information relating to the scenario and make judgement-based decisions during the workshop. There will be group discussions and activities to explore the rationale behind decisions made, discussions on best practices, and the chance to learn from other participants.

Learning objectives

This programme is designed to equip you to demonstrate knowledge, understanding and skills regarding:

- what are the money laundering and terrorist risks that must be managed?
- the international bodies and standard setter
- national (Malaysia) legal and regulatory framework
- taking an anti money laundering risk-based approach and managing the risk
- initial and ongoing customer due diligence (CDD)
- monitoring activity and transactions
- recognising and reporting suspicious activities
- the vulnerability of specific products and services.

Training methodology

Virtual workshops and online learning:

- 1 x 1-hour welcome & getting started session
- 3 x 3-hour virtual classrooms
- 1 x 3-hour immersive learning scenario (putting you at the centre of a story) and tutorial
- 1 x 1-hour assessment preparation virtual classroom

Participant profile

- New/recently appointed money laundering reporting officers (MLROs) and deputies
- New/recently appointed financial crime and risk officers
- Compliance officers
- Internal auditors assuming responsibilities for money laundering/financial crime issues
- All individuals engaged in financial services and who aspire to a career in anti money laundering

Programme fee RM 6,000 per pax

Assessment structure

The course is assessed through:

- a timed, online scenario-based assessment, and
- 2,000–2,500 word assignment.

Unit
1

What are the Money Laundering, Terrorist Financing and Sanctions Risks that must be Managed?

- 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

Unit
2

The International Bodies and Standard Setters

- 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

Unit
3

National legal and regulatory frameworks

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

Unit
4

Taking an AML/CFT Risk-based Approach and Managing the Risks

- 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

Unit
5

Initial and 'Ongoing' Customer Due Diligence (CDD)

- 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
 - 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

Unit
6

Monitoring activity and transactions

- 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

Unit
7

Recognising and Reporting Suspicions

- 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

Unit
8

The Vulnerabilities of Specific Services and Products

- 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

Supplementary material

- Malaysia regulatory requirements and examples

