

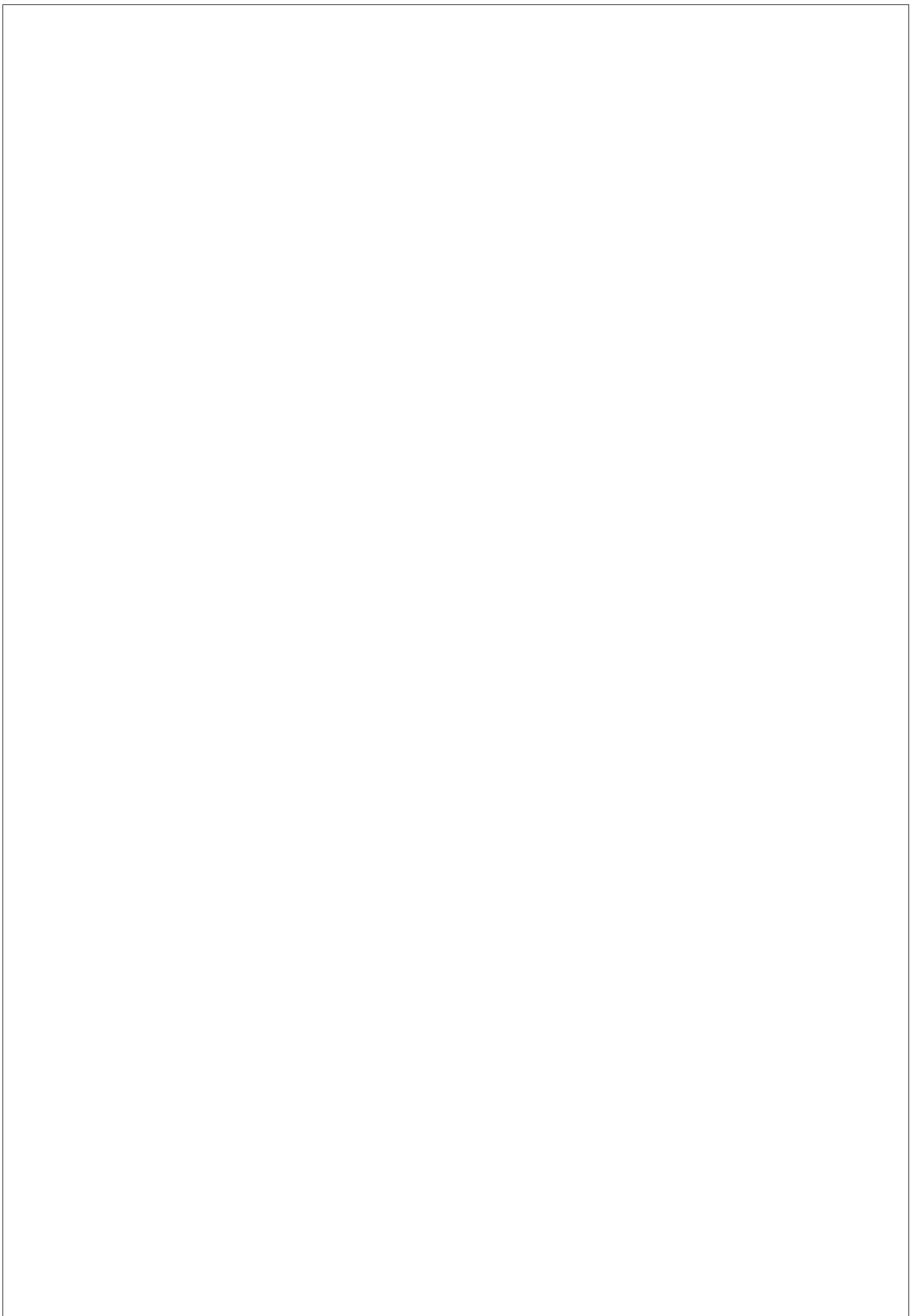


CHARTERED INSTITUTE FOR  
SECURITIES & INVESTMENT

# Combating Financial Crime

Effective from 11 January 2023

© Chartered Institute for Securities & Investment



## Objective of the Examination

The objective of the examination is to ensure that candidates have a basic knowledge of the regulations and practices related to combating financial crime.

The examination will test candidates' knowledge and understanding of the following elements:

- The Background and Nature of Financial Crime
- Money Laundering
- Terrorist Financing
- Bribery and Corruption
- Fraud and Market Abuse
- Tax Evasion
- Financial Sanctions
- Financial Crime Risk Management
- The Role of the Financial Services Sector

## Syllabus Structure

The unit is divided into **elements**. These are broken down into a series of **learning objectives**.

Each learning objective begins with one of the following prefixes: **know** or **understand**. These words indicate the different levels of skill to be tested. Learning objectives prefixed:

- **know** requires the candidate to recall information such as facts, rules and principles
- **understand** requires the candidate to demonstrate comprehension of an issue, fact, rule or principle

## Candidate Update

Candidates are reminded to check the 'Candidate Update' area of the Institute's website ([cisi.org/candidateupdate](http://cisi.org/candidateupdate)) on a regular basis for updates that could affect their examination as a result of sector change.

## Examination Specification

Each examination paper is constructed from a specification that determines the weightings that will be given to each element. The specification is given below.

It is important to note that the numbers quoted may vary slightly from examination to examination as there is some flexibility to ensure that each examination has a consistent level of difficulty. However, the number of questions tested in each element and / or case study should not change by more than two.

<b>50 multiple choice questions</b>		
Element 1	The Background and Nature of Financial Crime	5
Element 2	Money Laundering	8
Element 3	Terrorist Financing	4
Element 4	Bribery and Corruption	6
Element 5	Fraud and Market Abuse	4
Element 6	Tax Evasion	4
Element 7	Financial Sanctions	4
Element 8	Financial Crime Risk Management	8
Element 9	The Role of the Financial Services Sector	7
<b>TOTAL</b>		<b>50 Questions</b>

## Assessment Structure

The unit will be assessed by a 1 hour examination of 50 multiple choice questions drawn from across the syllabus.

Candidates sitting the exam by Computer Based Testing may have, in addition, up to 10% additional questions as trial questions that are not separately identified and do not contribute to the result. Candidates who are asked to answer these additional questions will be given proportionately more time to complete the test.

## Summary Syllabus

### **Element 1 The Background and Nature of Financial Crime**

- 1.1 Definitions
- 1.2 Governmental and quasi-governmental approaches to Combating Financial Crime (CFC)
- 1.3 Best practice
- 1.4 Asset recovery

### **Element 2 Money Laundering**

- 2.1 Background
- 2.2 International Anti-money laundering (AML) standards
- 2.3 Financial Action Task Force (FATF)
- 2.4 The role of other international bodies

### **Element 3 Terrorist Financing**

- 3.1 Background
- 3.2 Measures to combat the financing of terrorism
- 3.3 Standards for combating the financing of terrorism

### **Element 4 Bribery and Corruption**

- 4.1 Bribery and corruption
- 4.2 UK Bribery Act (2010)
- 4.3 Foreign Corrupt Practices Act (FCPA) (1977)
- 4.4 Corrupt practice
- 4.5 Combating Corruption

### **Element 5 Fraud and Market Abuse**

- 5.1 Fraud
- 5.2 Types of fraud
- 5.3 Market abuse
- 5.4 Sarbanes-Oxley Act (2002)

**Element 6 Tax Evasion**

- 6.1 Tax evasion
- 6.2 Criminal Finances Act (2017)

**Element 7 Financial Sanctions**

- 7.1 Financial Sanctions

**Element 8 Financial Crime Risk Management**

- 8.1 Considerations for the financial services sector
- 8.2 Risks
- 8.3 Practical business safeguards

**Element 9 The Role of the Financial Services Sector**

- 9.1 Relations with regulators
- 9.2 Specific responsibilities
- 9.3 Compliance
- 9.4 Fintech
- 9.5 Customer Due Diligence (CDD)
- 9.6 Reporting obligations
- 9.7 Consent regimes
- 9.8 Record keeping obligations

## **Element 1 The Background and Nature of Financial Crime**

### **1.1 Definitions**

On completion, the candidate should:

1.1.1 know the following terms:

- financial crime
- money laundering
- predicate offences
- terrorist financing
- proliferation financing
- fraud
- market abuse
- bribery and corruption
- international financial sanctions
- trade and investment sanctions
- tax evasion
- data protection

### **1.2 Governmental and quasi-governmental approaches to Combating Financial Crime (CFC)**

On completion, the candidate should:

1.2.1 know the role and objectives of FATF, its limitations and the legal context of its recommendations

1.2.2 know the role of financial regulators, commissions, and institutions in combating financial crime

- European Commission and Supervisory Authorities
- Office of Foreign Assets Control (OFAC)
- Financial Conduct Authority (FCA)



- Office for Financial Sanctions Implementation (OFSI)
- Other domestic regulators

1.2.3 know how regulators implement international standards and facilitate cross border cooperation

1.2.4 understand the role and scope of:

- intelligence gathering and analysis
- investigating financial crime
- asset recovery and repatriation

### **1.3 Best practice**

On completion, the candidate should:

1.3.1 know the role, evolution, and practical application of best practice in CFC and establishing international standards

1.3.2 understand the role of the FCA's financial crime guidance

1.3.3 understand the importance of the Joint Money Laundering Steering Group Guidance to UK financial services firms

### **1.4 Asset recovery**

On completion, the candidate should:

1.4.1 know the importance of recovery for prevention, deterrence, and justice

### 1.4.2 know civil and criminal remedies to recovering assets and the implications of freezing orders

- criminal confiscation
- civil recovery
- freezing orders
- search orders
- disclosure of information orders
- tracing
- monitoring
- unexplained wealth orders

## **Element 2 Money Laundering**

### **2.1 Background**

On completion, the candidate should:

#### 2.1.1 understand the models of the money laundering process:

- Placement, Layering, Integration model (PLI)
- the 'enable, distance, and disguise' model

#### 2.1.2 know these associated activities as defined by the Proceeds of Crime Act (POCA) (2002):

- concealment
- arrangements
- acquisition, use and possession
- failure to disclose
- tipping off
- consent regime
- criminal property
- criminal conduct

- 2.1.3 know the role, purpose and scope of The Money Laundering, Terrorist Financing and Transfer of Funds (information on the payer) Regulations (MLR 2017) as amended
- 2.1.4 understand how the stages of the money laundering process are detected by financial services firms in the regulated sectors

### **2.2 International Anti-money laundering (AML) standards**

On completion, the candidate should:

- 2.2.1 know the role, purpose and scope of international instruments and conventions
  - UN conventions
  - Directives/Regulations of the European Union - 2015/849/EC (4th Money Laundering Directive) 2018/843/EC (5th Money Laundering Directive) 2018/1673/EC (6th Money Laundering Directive) 2015/847/EC (Fund Transfer Regulations)

### **2.3 Financial Action Task Force (FATF)**

On completion, the candidate should:

- 2.3.1 know FATF's risk-based approach to AML and combating the financing of terrorism (CFT)
- 2.3.2 know the broad categories of what the recommendations cover
- 2.3.3 know the categorisation of jurisdictions which FATF considers to have strategic deficiencies
- 2.3.4 understand the role, activities, and coverage of FATF Style Regional Bodies (FSRBs)

## **2.4 The role of other international bodies**

On completion, the candidate should:

2.4.1 know the role other bodies play in combating money laundering and establishing best practice

- Basel Committee on Banking Supervision
- International Organization of Securities Commissions (IOSCO)
- International Association of Insurance Supervisors (IAIS)
- Egmont Group of Financial Intelligence Units
- Wolfsberg Group
- Regulatory and supervisory bodies
- Professional bodies

2.4.2 understand the importance of the guidance issued by the European Supervisory Authorities and the role played by the European Central Bank (ECB)

2.4.3 understand each jurisdictions list of high-risk countries

## **Element 3 Terrorist Financing**

### **3.1 Background**

On completion, the candidate should:

3.1.1 understand the similarities and differences between:

- money laundering and financing terrorism
- proliferation finance and terrorist financing

### **3.2 Measures to combat the financing of terrorism**

On completion, the candidate should:

3.2.1 know the main provisions of the United Nations International Convention for the Suppression of the Financing of Terrorism

3.2.2 know the work of the United Nations Security Council in relation to the financing of Terrorism

### **3.3 Standards for combating the financing of terrorism**

On completion, the candidate should:

3.3.1 know EU and UK CFT initiatives

- money laundering directives
- regulations of fund transfers
- Payment Services Regulation

## **Element 4 Bribery and Corruption**

### **4.1 Bribery and corruption**

On completion, the candidate should:

4.1.1 know the difference between bribery and corruption

### **4.2 UK Bribery Act (2010)**

On completion, the candidate should:

4.2.1 know the extra-territorial reach of the Act

4.2.2 know the global reach of the UK Bribery Act (2010) and the offences:

- bribing another person
- receiving bribes
- bribery of a Foreign Public Official (FPO)
- failure of commercial organisations to prevent bribery

4.2.3 know the definition of an FPO

4.2.4 understand the liabilities corporate entities face from “Associated Persons”

- 4.2.5 understand strict liability and the meaning of "adequate procedures"
- 4.2.6 understand the six principles for bribery prevention and their legal context
- 4.2.7 know the maximum penalties applicable to individuals found guilty under the Act
- 4.2.8 understand the circumstances under which Directors and senior officers of a corporation may be found liable under the Act
  - consent or connivance
  - passive acquiescence
  - failure to implement adequate procedures and potential civil liability

### **4.3 Foreign Corrupt Practices Act (FCPA) (1977)**

On completion, the candidate should:

- 4.3.1 understand the objectives and scope of the FCPA (1977)
- 4.3.2 know the key differences between the UK Bribery Act (2010) and the FCPA (1977)

### **4.4 Corrupt practice**

On completion, the candidate should:

- 4.4.1 understand the main components and differences between types of corrupt practice
  - active and passive bribery
  - embezzlement
  - trading in influence
  - abuse of office
  - illicit enrichment
  - concealment

#### **4.5 Combating Corruption**

On completion, the candidate should:

4.5.1 know the role that international bodies play in combating corruption

4.5.2 understand the practical application and limitations of quantitative indicators in combating corruption

### **Element 5 Fraud and Market Abuse**

#### **5.1 Fraud**

On completion, the candidate should:

5.1.1 know the three classes of fraud defined in the UK Fraud Act (2006)

- false representation
- failing to disclose information
- abuse of position

#### **5.2 Types of fraud**

On completion, the candidate should:

5.2.1 know common examples of types of fraudulent activity:

- Identity fraud and identity theft
- Cyber attacks and computer hacks
- Phishing
- Malware
- Application fraud
- 419 fraud
- Account takeover
- Money mules
- Authorised payment fraud

- Smurfing

5.2.2 know the difference between internal and external fraud

### **5.3 Market abuse**

On completion, the candidate should:

5.3.1 know international and UK legislation for combating market abuse

- The EU Market Abuse Regulation (2014) (MAR)
- The Dodd Frank Wall Street Reform and Consumer Protection Act (Dodd Frank) and the Volcker Rule
- FATF Risk-based Approach Guidance for the Securities Sector (2018)
- ESMA guidance
- Market Abuse (Amendment) (EU Exit) Regulations 2019

5.3.2 know behaviours that constitute market abuse

5.3.3 know the insider dealing provisions of the UK's Criminal Justice Act 1993 (part 5, s.52)

5.3.4 know the offences relating to financial services provisions of the UK's Financial Services Act 2012 (part 7, sections 89, 90 & 91)

5.3.5 know how market abuse is detected

### **5.4 Sarbanes-Oxley Act (2002)**

On completion, the candidate should:

5.4.1 know the main provisions of the Sarbanes-Oxley Act (2002)



## **Element 6 Tax Evasion**

### **6.1 Tax evasion**

On completion, the candidate should:

- 6.1.1 know the difference between tax evasion and tax avoidance
- 6.1.2 know international EU and US approaches to improving tax compliance
  - Foreign Account Tax Compliance Act (FATCA)
  - Crown Dependencies and Overseas Territories (CDOT) regulation
  - OECD's Common Reporting Standard for Automatic Exchange of Financial Information (CRS)
  - EU's list of non-cooperative tax jurisdictions
- 6.1.3 understand the difference between individual and corporate liability
- 6.1.4 know how tax evasion is detected

### **6.2 Criminal Finances Act (2017)**

On completion, the candidate should:

- 6.2.1 know the extra-territorial reach of the Act
- 6.2.2 know the offences introduced by the Criminal Finances Act (2017)
- 6.2.3 understand the liabilities corporate entities face from "Associated Persons"
- 6.2.4 understand strict liability and the meaning of "reasonable procedures"
- 6.2.5 understand the six principles for tax evasion prevention and their legal context
- 6.2.6 know the maximum penalties under the Act

**Element 7 Financial Sanctions**

**7.1 Financial Sanctions**

On completion, the candidate should:

7.1.1 know the purpose and application of financial sanctions screening in relation to

- terrorist financing
- proliferation finance
- other foreign policy objectives

7.1.2 understand the impact of the financial sanctions listing process of the:

- United Nations
- European Union
- United Kingdom, including the role of OFSI
- OFAC
- other states

7.1.3 know the range of legal financial sanctions related to "designation"

- asset freezes
- prohibitions
- targeted sanctions

7.1.4 know the potential penalties of dealing with designated persons and entities

## **Element 8 Financial Crime Risk Management**

### **8.1 Considerations for the financial services sector**

On completion, the candidate should:

8.1.1 understand how financial crime can directly impact on firms

- embezzlement
- asset misappropriation
- fraudulent customer activity
- defrauded by organised criminals
- limiting access to data
- data compromise

8.1.2 understand how firms can be exploited as a vehicle for financial crime

- criminals using the firm's services to launder the proceeds of crime
- customer payments to terrorists
- theft of customer data to facilitate identity fraud
- trade-based money laundering

8.1.3 understand how a firm or its representatives may collude in the propagation of financial crime

- misstatement of financial circumstances
- corporate malfeasance

8.1.4 understand the relevant implications of business strategies

- corporate structure
- outsourcing and oversight
- use of middlemen
- Fintech
- Green Finance

## 8.2 Risks

On completion, the candidate should:

- 8.2.1 know the role, significance, and utilisation of national risk assessments
- 8.2.2 understand how to identify, assess, and manage the risks posed on a firm's business activities by the following:
  - products and services
  - customers
  - sector
  - countries
  - delivery channels
- 8.2.3 understand the risks associated with non-compliance for regulated firms
  - financial
  - reputational
  - legal including civil liability
  - operational
  - systemic
  - regulatory
  - criminal
  - prudential

## 8.3 Practical business safeguards

On completion, the candidate should:

- 8.3.1 know the relevant risk factors firms may consider before commencing business relationships
  - nature and purpose of the relationship
  - source of introduction

## Combating Financial Crime

- company structure
- political connections
- country risk
- establishing beneficial ownership
- the customer's or beneficial owner's reputation
- source of funds/ source of wealth
- expected account activity
- sector risk
- involvement in public contracts
- charities, voluntary and not-for-profit bodies

8.3.2 understand the risks from counterparties with opaque corporate and ownership structures

8.3.3 understand what measures can be adopted to minimise financial crime opportunities within a firm

- conflicts of interest policies
- compliance monitoring
- information barriers
- restricting physical access
- limiting access to data
- effective sign off protocols
- gifts and entertainment policies
- remuneration policies
- objective audit processes
- I.T. security
- whistleblowing
- employee vetting
- penetration testing and vulnerability assessment
- secure disposal

- staff training
- segregation of duties

8.3.4 understand how internal policies and procedures on CFC are formulated:

- laws and regulations
- regulators' handbooks
- relevant codes of conduct
- sector and regulatory guidance

8.3.5 know effective techniques for conducting due diligence on:

- directors
- employees
- contractors
- service providers

8.3.6 know the additional measures financial services firms can take to manage the risk of financial crime originated or enabled by an employee

- raising awareness
- improving the management of I.T. privileges for joiners, movers and leavers
- classifying and segmenting data
- embedding ethical practice in relation to data security
- implementing whistleblowing procedures

8.3.7 know the role industry groups and guidance bodies play in facilitating practical solutions for business

8.3.8 understand how auditing contributes to corporate governance, accounting and reporting requirements

- audit committees
- internal audit
- external auditors

## **Element 9 The Role of the Financial Services Sector**

### **9.1 Relations with regulators**

On completion, the candidate should:

9.1.1 know financial services firms' responsibilities for dealing with regulatory and other relevant authorities

- protection of customer confidentiality
- responses to information requests
- responses to investigation orders
- civil recovery, forfeiture and confiscation
- global investigation, prosecution and confiscation
- presentation of evidence in court
- transparency with regulator

### **9.2 Specific responsibilities**

On completion, the candidate should:

9.2.1 know the role of the Money Laundering Reporting Officer (MLRO) and the Nominated Officer (NO) or equivalents

9.2.2 understand the responsibilities of Directors and senior management in relation to CFC under the Senior Managers and Certification Regime (SM&CR) or equivalent individual accountability regimes

9.2.3 know regulators expectations from firms with respect to adequate management systems and controls to combat financial crime

### **9.3 Compliance**

On completion, the candidate should:

9.3.1 know the Basel Committee on Banking Supervision's (BCBS) definition of "Compliance risk"

9.3.2 understand how a compliance culture may be created and maintained, including:

- tone from within
- performance management processes
- appointment of Compliance/Anti Money-Laundering Reporting Officers
- information gathering and analysis
- application in routine operations
- raising awareness
- training
- updates

### **9.4 Fintech**

On completion, the candidate should:

- 9.4.1 know the benefits of utilising technology to support a compliance culture and the limitations of over reliance on systems
- 9.4.2 know how distributed ledger technology and advanced/objective blockchain ID can be utilised for CDD
- 9.4.3 know how the following technological solutions can be utilised for CDD:
  - digital recognition
  - face recognition
- 9.4.4 know how artificial intelligence (AI) can be utilised for detecting financial crime
- 9.4.5 know how data sources can be utilised by firms to detect financial crime
  - customer complaints
  - trade and transactions monitoring
  - suspicious transaction reports
  - Internet and website usage patterns
  - customer device profiles



- employee turnover statistics

9.4.6 know the role of fast-paced electronic markets (FPM)

9.4.7 know the role of the Global Financial Innovation Network (GFIN)

### **9.5 Customer Due Diligence (CDD)**

On completion, the candidate should:

9.5.1 know how regulated financial institutions implement CDD procedures

- Know Your Customer (KYC)
- ongoing monitoring
- non-face-to-face
- correspondent banking
- Politically Exposed Persons (PEPs)
- reliance on others

9.5.2 understand how firms implement a risk-based approach

9.5.3 know Enhanced Due Diligence (EDD) requirements for higher risk situations

9.5.4 know how financial institutions implement sanctions screening procedures

9.5.5 know examples of Politically Exposed Peoples (PEPs)

9.5.6 know standards for dealing with PEPs

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations (MLR 2017) and the FCA's Finalised Guidance G17/6: the treatment of PEPs for anti-money laundering purposes

**9.6 Reporting obligations**

On completion, the candidate should:

- 9.6.1 know how and why regulated financial institutions report suspicious transactions, trading activity and order reports
- 9.6.2 know the circumstances in which financial services firms are obliged to report currency transactions and those circumstances that are exempt

**9.7 Consent regimes**

On completion, the candidate should:

- 9.7.1 know what is meant by a “consent regime”
- 9.7.2 know the legal basis on which the consent of a Financial Intelligence Unit (FIU) must be obtained

**9.8 Record keeping obligations**

On completion, the candidate should:

- 9.8.1 understand the reasons why financial institutions have record-keeping requirements and the circumstances in which they are required to comply