

Certificate in Global
Financial Compliance

Global Financial Compliance

Edition 12, July 2026

Your journey to success starts here!

Flexible, accessible learning options tailored to your needs
– wherever you are.

Looking for extra support? We've got you covered!

MyStudy

View sample exam papers, study tips and key exam information.

Accredited Training Partners (ATP)

Get expert-led classroom tuition or virtual support from one of our trusted ATPs.

Reasonable Adjustments

Need exam accommodations? Request extra time, larger fonts or other support.



Stay ahead of the game with CISI membership

Passing your exam is just the beginning – your next step is to become a CISI member.

Gain access to thousands of online resources, exclusive events and powerful networking opportunities that give your career a competitive edge.

Become a member today

Supercharge your expertise with the **CISI Learning Platform**



Discover curated content collections, get personalised recommendations and stay ahead with the latest industry insights – all at your fingertips, anytime, anywhere.

Get started now – access videos, articles, modules and more on the Learning Platform today.

[Learn more](#)

[Access via the CISI App](#)





Welcome to the Chartered Institute for Securities & Investment's Global Financial Compliance study material which has been written to prepare you for the Chartered Institute for Securities & Investment's Global Financial Compliance examination.

Published by

Chartered Institute for Securities & Investment

© Chartered Institute for Securities & Investment 2026

20 Fenchurch Street, London EC3M 3BY, United Kingdom

Tel: +44 20 7645 0600 Fax: +44 20 7645 0601

Email: customersupport@cisi.org www.cisi.org/qualifications

Author

Dr Natalie Schoon ACSI

Reviewers

Martin Mitchell FCSI

Karl Micallef

This is for educational purposes only and the Chartered Institute for Securities & Investment accepts no responsibility for persons undertaking trading or investments in whatever form.

While every effort has been made to ensure its accuracy, no responsibility for loss occasioned to any person acting or refraining

from action as a result of any material in this publication can be accepted by the publisher or authors.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior permission of the copyright owner.

Warning: any unauthorised act in relation to all or any part of the material in this publication may result in both a civil claim for damages and criminal prosecution.

Candidates should be aware that the laws mentioned in this study material may not always apply to Scotland.

A learning map, which contains the full syllabus, appears at the end of this study material. The syllabus can also be viewed on cisi.org and is also available by contacting the Customer Support Centre on +44 20 7645 0777.

Please note that the examination is based upon the syllabus. Candidates are reminded to check the Candidate Update area details (cisi.org/candidateupdate) on a regular basis for updates as a result of industry change(s) that could affect their examination.

The questions contained within the study material are designed to aid revision of different areas of the syllabus and to help you consolidate your learning chapter by chapter.

Please note that, as part of exam security, hand-held calculators are not allowed in CISI exam venues. Candidates must use the onscreen calculator for all CISI CBT exams in all languages in the UK and internationally.

Version: 12.1 (July 2026)



Important – Keep Informed of Amendments or Changes to Examination Dates

Changes in industry practice, economic conditions, legislation/regulations, technology and various other factors mean that practitioners must ensure that their knowledge is up to date. At the time of publication, the content is approved as suitable for examinations taken during the period specified. However, changes affecting the industry may either prompt or postpone the publication of an updated version.

It should be noted that the current version will always supersede the content of those issued previously. Keep informed on the publication of new versions and any changes to examination dates by regularly checking the CISI's website: cisi.org/candidateupdate

Learning and Professional Development with the CISI

The Chartered Institute for Securities & Investment is the leading professional body for those who work in, or aspire to work in, the investment sector, and we are passionately committed to enhancing knowledge, skills and integrity – the three pillars of professionalism at the heart of our Chartered body.

CISI examinations are used extensively by firms to meet the requirements of government regulators. Besides the regulators in the UK, where the CISI head office is based, CISI examinations are recognised by a wide range of governments and their regulators, from Singapore to Dubai and the US.

Around 50,000 examinations are taken each year, and it is compulsory for candidates to use CISI study materials to prepare for CISI examinations so that they have the best chance of success. Titles are normally revised every year by experts who themselves work in the industry and also by our Accredited Training Partners,

who offer training and elearning to help prepare candidates for the examinations. Information for candidates is also posted on a special area of our website: cisi.org/candidateupdate.

This edition not only provides a thorough preparation for the examination it refers to, but it is also a valuable reference for practitioners, and studying from it counts towards your Continuing Professional Development (CPD). Mock examination papers, for most of our titles, will be made available on our website, as an additional revision tool.

CISI examination candidates are automatically registered, without additional charge, as student members for one year (should they not be members of the CISI already), and this enables you to use a vast range of online resources, including CISI TV, free of any additional charge. The CISI has more than 40,000 members, and nearly half of them have already completed relevant qualifications and transferred to a core membership grade. Please click here to find out more information on becoming a member.

If you wish leave feedback, please email your comments to learningresources@cisi.org



Chapter One

The International Regulatory Environment

Section 1

Models of Regulation

Section 2

The International Approach to Regulation

This syllabus area will provide approximately 20 of the 100 examinations questions



1. Models of Regulation

This workbook reflects global financial compliance practices. The examples used draw heavily on United Kingdom (UK) and European Union (EU) regulations, both to provide insight and highlight the innovative approach adopted in these jurisdictions.



1.1.1 Understand the objectives and benefits of regulation

Effective capital and financial markets are an essential part of the economy. They fuel economic development and aid wealth creation. Confidence and trust in these markets are vital. Loss of confidence and trust can result in the failure of financial companies and have an adverse impact on the economy. This can, among others, result in recession, loss of jobs and income, reduction of the value of investments, reduction in market capitalisation of companies, and defaults on loans. The near collapse of large financial institutions during the 2007–08 global financial crisis had a global impact and the subsequent bailout of the banks; reduction in government spending and increase in taxes has had a far-reaching impact on individuals and corporations.

As the Basel Committee for Banking Supervision (BCBS) notes in their corporate governance principles, banks and, by extension, financial markets play a crucial role in the economy by intermediating funds from savers and depositors to activities that support enterprises and help drive economic growth. Their safety and soundness are critical to financial stability. Therefore, rules and codes of conduct are of the utmost importance to protect investors and the general public. Although the development of such rules and the extent to which they are enforced varies from country to country, the development of global financial markets depends on an agreement on standards of behaviour and mechanisms for dispute resolution. These standards, rules and codes of conduct can be established through self-regulation of the industry, or by means of a statutory approach where governments provide enabling legislation and establish statutory-based regulatory authorities. Integrity and ethical behaviour are a key part of any code of conduct. As financial markets have become increasingly global in nature and interdependence has grown, the financial sector has moved from self-regulation to a statutory approach. This has facilitated international cooperation and the development of improved and common standards. Furthermore, after the 2007–08 financial crisis, integrity and ethical behaviour has experienced renewed focus from professional bodies, governments, and regulators.

Regulation has also been used to restrict the ability of criminals and terrorists to use the financial system to their advantage, and to aid enforcement and intelligence agencies to identify criminal activity. Again, this has developed from purely domestic initiatives to major international efforts to reduce crime related to financial services. These crimes include **money laundering (ML)**, terrorist financing (TF), fraud and tax evasion.

The objectives and benefits of regulation can be summarised as:

- increase in confidence and trust in financial markets, systems and products

- establish an environment to encourage economic development and wealth creation
- reduce the risk of market and system failures, including their economic consequences
- enhance consumer protection, giving them the reassurance they need to save and invest, and
- reduce financial crime by ensuring financial systems cannot easily be exploited.

1.2 Law and Regulation



1.1.2 Know the interaction between law and regulation

The objectives and benefits of regulation are typically achieved through a combination of laws and regulations.

- **Law** – the principles and regulations established in a community by an authority, such as the government, and applicable to the people. Laws can be a combination of legislation, custom, and policies recognised and enforced by judicial decision. When a person is found guilty of breaking the law, they are typically punished with a reprimand, a prison sentence and/or a penalty. Financial services legislation provides the structural framework for the sector itself, as well as the products it offers. In the UK, for example, key legislation includes the Financial Services and Markets Act 2000 (FSMA), which sets out the UK's regulatory structure, and multiple Finance Acts which contain provisions related to taxes, duties, exemptions and reliefs. National and international laws regarding the prevention of money laundering and terrorist financing (ML/TF), tax and other financial services-related crimes will be incorporated into the appropriate regulations

relevant to the structuring of banking or other financial products or customer advice.

- **Regulation** – detailed rules that expand on and implement the overarching laws laid down in the legislation. It is a combination of rules and standards generally covering matters such as observing proper standards of market conduct, managing conflicts of interest, treating customers fairly, ensuring the suitability of customer advice, and ensuring stability of the financial system.

Compliance laws, rules and standards have various sources, including:

- primary legislation
- rules and standards issued by legislators and supervisors
- market conventions
- codes of practice promoted by industry associations or professional bodies, and
- internal codes of conduct applicable to the staff members of financial institutions.

Industry and internal codes are likely to go beyond what is legally binding and embrace broader standards of integrity and ethical conduct.

1.3 Rules-Based and Principles-Based Approaches



1.1.3 Understand the main differences between rules-based and principles-based approaches to financial regulation

When drafting regulation, regulators make a choice between rules-based and principles-based approaches.

- **Rules-based** – regulations are mainly prescriptive procedures including very detailed rules. These rules specify exactly what individuals and firms must do to ensure they comply. A rules-based approach requires strict adherence to precise rules with little allowance for interpretation. It is typically inflexible and may result in a tick-box exercise.
- **Principles-based** – regulations focus on the spirit of the rules and, therefore, the types of behaviour and outcomes. Unlike the rules-based approach, it is not about blindly following the rules. A principles-based approach acts as a fundamental source of guidance on how firms and individuals are expected to act. How individuals and firms ensure they comply with the regulations, and to what extent the principles are met, is their own responsibility.

A rules-based approach must be sufficiently detailed in order to provide a reliable distinction between right and wrong. Maintaining a comprehensive rules-based model is challenging, particularly in evolving markets with an increase in the use of technology, and a wider range of products and assets. A broader and more complicated market requires a larger body of rules which take into account evolving business activities.

The challenge faced by regulators with a principles-based approach is ensuring that firms apply consistent interpretations to their implementation of the principles.

Some firms and compliance officers prefer a rules-based approach because they know exactly what is expected of them, and they cannot be challenged or criticised as long as they strictly follow the rules.

Others prefer a principles-based approach because it provides scope for innovation and the freedom to develop services and business models within the framework of the principles.

Although regulators predominantly follow one approach, they tend to also incorporate elements of the other approach.

The success of a principles-based approach depends on firms and individuals making the right decisions. Strong ethical standards, often set by professional bodies like the Chartered Institute for Securities & Investment (CISI), play a key role in a principles-based regulatory environment (see chapter 4).

From 2001 until the 2007–08 financial crisis, the UK's financial regulators were moving towards a light-touch principles-based approach. The global financial crisis showed this approach to be flawed and resulted in an increase in demand for rules. The UK regulators, in particular the Financial Conduct Authority (FCA), has retained both principles and rules, while introducing a greater focus on the outcomes for the consumers of financial services.

1.4 Models of Self-Regulation



1.1.4 Understand models of self-regulation

1.1.5 Understand the regulation of faith- and ethical-based finance and the attendant regulatory implications

Self-regulation is where groups or industries mutually agree the rules that will govern their own collective behaviours. It exists in addition to laws or regulations established by governments or regulatory bodies. In some cases, self-regulation develops because there is no regulation in place. While self-regulation measures must operate within the parameters of national laws, strong self-regulation can reduce the need for, or extent of, state regulation.

In the financial sector, self-regulation is typically a unique combination of private interests with government oversight, which

has delivered an effective and efficient form of regulation for the complex and dynamic environment. As stated in the Model for Effective Regulation report by the International Organization of Securities Commissions (IOSCO) on Objectives and Principles of Securities Regulation:

'Self-regulatory organisations (SROs) can be a valuable component to the regulator in achieving the objectives of securities regulation.' ♦

The adoption of self-regulation differs from country to country, across market sectors and across developed and emerging markets. Where its role is significant, it is almost always the result of a long track record of responsible behaviour under the oversight of statutory regulators. That relationship with statutory regulators has permitted SROs to contribute to the quality of regulation and to the content of policy in the public interest.

The broad objectives of self-regulation in financial markets are the same as those identified for government regulation in the IOSCO Objectives and Principles of Securities Regulation to:

- preserve market integrity (fair, efficient and transparent markets)
- preserve financial integrity (reduce systemic risk), and
- protect investors.

Many different forms of self-regulation currently exist for financial markets to achieve these objectives such as:

- industry SROs
- exchange self-regulatory frameworks, and
- private associations.

All of these define and encourage adherence to standards of best practice among their participants.

Self-regulation typically focuses on oversight of the market itself, qualification standards for market intermediation and oversight of the business conduct of intermediaries. Business conduct of intermediaries include their relationship with their **client** market users. A single SRO may be responsible for all of these tasks, or they may be divided or shared among SROs within a given country or market sector.

Some approaches may be applied purely within the organisation, such as ethical-based finance. A firm may hold strong principles that guide its investment policies (eg, avoidance of sectors such as weaponry or tobacco). A firm might also choose to market itself according to ethical positions because it meets their values, or to attract certain customers. While there may be no specific independent party overseeing such practices, a firm that publicly takes a moral position must ensure its reputation is secure.

1.4.1 Key Elements of an Effective Self-Regulatory Model

The elements which contribute to an effective self-regulatory model include the following:

- **Industry-specific knowledge** – important given the complexity of markets and products.
- **Industry motivation** – business incentive to operate a fair, financially sound and competitive marketplace. Reputation and competition are powerful motivating forces for sustaining behaviour.
- **Contractual relationship** – this can go beyond national boundaries and require ethical standards that go beyond government regulations.
- **Transparency and accountability** – an SRO's compliance programme should be transparent and accountable to ensure that SROs follow professional standards of behaviour on

matters including confidentiality and procedural fairness. Such transparency can occur in different ways, including making SRO rules accessible to the public in printed or digital form, and by publicising significant disciplinary actions taken by an SRO and through educational outreach programmes. The inclusion of both public representatives and industry professionals on an SRO's governing body and public participation in deliberations pertaining to regulatory policy and rulemaking can also provide the foundation for an open organisation. In some jurisdictions, SROs prepare regulatory plans that are submitted to their statutory regulator and made available to the public. These regulatory plans describe the SRO's regulatory objectives, activities for the year, and a cost forecast.

- **Flexible SRO compliance programmes** – SROs are generally able to modify their rules quicker than government agencies. This is due to their experience and expertise in the industry, their size, and because they are not subject to the more rigid requirements typically imposed on the rulemaking process of statutory regulators.
- **Coordination and sharing information** – coordination and information sharing between markets is important to address cross-market issues. A coordinated approach is necessary to address potential **market abuse** or systemic risk concerns that may impact more than one market.

In 2000, a report by IOSCO's SRO Consultative Committee (Model for Effective Regulation) indicated that an SRO's common regulatory practices and objectives should include:

- enforcing rules and regulations through investigations and disciplinary action
- conducting financial/operations and sales practice examinations
- conducting fitness screening for access to marketplace

- handling customer complaints
- having surveillance programmes to detect improper conduct
- sharing information and cooperating with other SROs, and
- providing a dispute resolution forum.

An integral component of many SRO compliance programmes is the development of guidebooks and other educational materials to help their members meet their regulatory responsibilities.

An example of self-regulation is the use of the International Swaps and Derivatives Association (ISDA) Master Agreement. ISDA is a membership association established in 1985 with the aim of fostering a safe and efficient derivatives market to facilitate effective risk management for all users of derivatives products.

Members of ISDA agree to use the ISDA Master Agreement and associated documentation as a basis for derivative transactions. Members benefit from the netting provisions, which enable firms to net their exposures with each other. As a result, the transactions are legally treated as a single transaction with a single net value.

1.4.2 Islamic Finance Adoption of Self-Regulation

Some forms of self-regulation are established to reflect wider principles originating from ethics, society, and faith. An example of faith- and ethical-based regulation is the Islamic finance industry, which is regulated by a combination of SROs and statutory regulation in the countries in which they operate. Islamic commercial and financial ethics stem from the principles of Shariah (also referred to as Islamic law) which includes the major prohibitions of *riba* (interest), *gharar* (unnecessary uncertainty) and *maysir* (gambling). All values, standards and rules structuring Islamic commercial and financial ethics are outlined in Shariah, which is best characterised as a framework providing legal, moral and spiritual guidance aimed at achieving the goals of Islam. It is

worth noting that these principles are not unique to Islamic financial institutions. Credit unions, for example, generally follow the same principles as Islamic financial institutions when it comes to behaviour, leverage, industries to avoid, and speculative transactions.

Similar to other financial institutions, Islamic financial institutions are authorised and supervised by the regulatory authority in their country of incorporation.

In addition, the following two self-regulating bodies have been established:

- The **Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI)** – an autonomous body responsible for the formulation and issuance of accountancy, auditing ethics, governance and Shariah standards for the international Islamic banking and finance industry. The standards have been developed to encourage the harmonisation of Islamic banking and finance practices, and to ensure transparency and uniformity of financial reporting by Islamic banks and financial institutions.
- The **Islamic Financial Services Board (IFSB)** – an international standard-setting organisation with a mission to promote and enhance the soundness and stability of the Islamic financial sector by issuing global prudential standards and guiding principles for the industry, broadly defined to include banking, capital markets and insurance sectors. The IFSB standards are mainly based on the identification, management and disclosure of risks relevant to Islamic products and operations. Full members of the IFSB are typically **central banks** in countries where Islamic financial institutions are incorporated. These countries are invited to apply the (optional) IFSB standards in order to provide a comparable regulated environment for the Islamic financial sector. The standards are mandatory in some countries, such as Bahrain and Sudan, and are used as guidelines in others.

From the perspective of financial institutions, Shariah compliance can be achieved in various ways including by adopting national regulation, or by the voluntary adoption of Shariah-compliant standards through the directives and resolutions of the firms' internal Shariah boards.

1.5 Extra-Territorial Reach of Legislation



- 1.1.6 Understand the purpose of the following: Data Protection, eg, GDPR; Tax Reporting, eg, CRS, FATCA; Market Integrity, eg, MiFID II, MiFIR, MAR, EMIR, PSD2, Sarbanes Oxley, CSDR; Financial Crime, eg, UK Bribery Act, FCPA, AMLD

As the financial sector is international, many regulations and laws have application beyond national borders. Compliance officers need to be aware of such legislation, and understand the potential impact. The regulations outlined in the remainder of this section are EU regulations which are implemented across the EU by individual member states. These also form the basis for the implementation of similar rules in countries outside the EU, amended to cater for specific local circumstances. The UK, for example, has adopted the main provisions of EU financial laws into UK legislation since its withdrawal from the EU on 1 January 2021. However, the UK has also made changes, such as the lowering of the age of consent in the UK General Data Protection Regulation (GDPR) from 16 to 13 years, and the exemption from the MiFID inducement rules for research on SME issuers. Other deviations may happen over time. Similarly, the data protection regulations in Hong Kong have substantially changed in recent years and are largely aligned with the EU GDPR. Because the EU GDPR serves as a blue print for the implementation of data protection in a large number of

jurisdictions, the remainder of this section will focus on the EU GDPR.

1.5.1 Data Protection (GDPR)

The EU GDPR came into force on 25 May 2018 and replaced the Data Protection Directive. It is designed to harmonise data privacy laws across Europe to protect EU citizens from privacy and data breaches in an increasingly data-driven world. The key points of the GDPR as it is in force at the time the workbook is published are summarised in the table below. Note that there are currently consultations in progress to simplify the regulations, particularly for small and medium sized enterprises, which include:

- data legislation including rules on cookies and other tracking technologies
- cybersecurity incident reporting, and
- targeted adjustments to the Artificial Intelligence Act to ensure optimal application for the rules.

Area	Description
Scope	GDPR applies to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location. It applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor who is not based in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required), and the monitoring of behaviour that takes place within the EU. Non-EU businesses processing the data

	of EU citizens have to appoint a representative in the EU.
Penalties	Breaches of the GDPR are subject to a tiered structure and subject to a maximum penalty of 4% of the annual global turnover of the previous financial year or €20 million (or equivalent), whichever is greater.
Consent	The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. It must be clear and separate from other matters using clear and plain language. It must be as easy to withdraw consent as it is to give it.
Data Subject Rights	- Any data breach that is likely to <i>'result in a risk for the rights and freedoms of individuals'</i> must be reported within 72 hours of the data processor first having become aware of the breach. Customers and controllers must be notified <i>'without undue delay'</i> after first becoming aware of a data breach. - Data subjects have the right to obtain from the data controller confirmation from the data controller as to whether or not their personal data is being processed, where, and for what purpose. Furthermore, the controller must provide a copy of the personal data, free of charge, in an electronic format on request. - Data subjects also have the right to be forgotten (also known as data erasure). On

	request, the data subject is entitled to have the data controller erase their personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in Article 17, include the data no longer being relevant to the original purpose for processing, or a data subject withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to <i>'the public interest in the availability of the data'</i> when considering such requests. • Data subjects have the right to receive the personal data concerning them, which they have previously provided in a <i>'commonly used and machine- readable format'</i> and have the right to transmit that data to another controller. • Privacy by design has become part of the GDPR legal requirement. Controllers must implement appropriate technical and organisational measures to meet the GDPR requirements. Only the data that is absolutely necessary for the completion of their duties should be held and processed.
Data Protection Officers (DPOs)	A DPO must be appointed by public authorities: companies whose core activities require large-scale, regular and systematic monitoring of individuals, and companies whose activities consist of large-scale processing of special categories of data or data relating to criminal convictions and offences. The DPO:

	• must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices • may be a staff member or an external service provider • contact details must be provided to the relevant DPA • must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge • must report directly to the highest level of management, and • must not carry out any other tasks that could result in a conflict of interest.
--	--

1.5.2 Market Integrity

There are a number of regulations dealing with market integrity:

Regulation	Key issues
Markets in Financial Instruments Directive (MiFID III) and the Markets in Financial Instruments Regulation (MiFIR 2)	• EU Directive and its associated regulation with the key aim to provide investor protection by placing significant importance on the fiduciary duties of a firm: ◦ Obligation to obtain the best possible result for the client. ◦ Information disclosure requirements.

- Client-specific rules on suitability and appropriateness of financial products.
- Rules on inducements.
- Ban on payments for order flows.
- Suitability, marketing communications, and EU-wide Consolidated Tape.
- Enhanced transaction reporting and reference data.
- Sanctions for violations.
- Key policy goals:
 - Extending the range of investment services for which a firm can obtain an EU 'passport' (ie, obtaining **authorisation** in one EU state (the home state) enabling a firm to provide investment services in another EU member state (the host state) without requiring any further local authorisations).
 - Removing a major hurdle to cross-border business by no longer applying 'host state' rules to incoming passported firms.
 - MiFID III and MiFIR 2 extend the application to Alternative Investment Fund Managers and management companies, and extend the scope of derivatives

	subject to the clearing obligation.
Market Abuse Regulation (MAR)	• EU Regulation with the aim to increase market integrity and investor protection. The regulation establishes a common regulatory framework on insider dealing, the unlawful disclosure of inside information, market manipulation as well as measures to prevent market abuse. Applies to the following: a. Financial instruments admitted to trading on a regulated market or for which a request for admission to trading on a regulated market has been made. b. Financial instruments traded on a multilateral trading facility (MTF), admitted to trading on an MTF, or for which a request for admission to trading on an MTF has been made. c. Financial instruments traded on an organised trading facility (OTF). d. Financial instruments not covered by points (a), (b) or (c), the price or value of which depends on or has an effect on the price or value of a financial instrument referred to in those points, including, but not limited to, credit default swaps (CDSs) and contracts for difference (CFDs). • Incorporates guidelines on inside information, delay of disclosure of inside

	information, market soundings, and requirements for the disclosure of emission allowances. • Inside information is information that would be likely to have a significant effect on the price of financial instruments or issuers if it were to be made public. Financial instruments include spot commodity contracts, emission allowances, and related auction products. The use of inside information to execute a transaction, or to amend or cancel an existing transaction constitutes insider dealing. • Market sounding is a communication or information that is disclosed to one or more investors prior to the announcement of a transaction. The purpose of a market sounding is to assess the interest of potential investors in relation to the transaction, potential size, and pricing. Market manipulation covers any activity that gives or may give false or misleading signals about the demand, supply, or price of a financial instrument, thus impacting trading in the instrument in a way intended by the person.
European Market Infrastructure Regulation (EMIR)	European regulation that requires over-the-counter (OTC) derivative contracts to be cleared and derivatives contracts to be reported. EMIR sets the framework to enhance the safety of central counterparties (CCPs) and trade repositories (TRs). EMIR also covers the

	regulations on OTC derivatives, CCPs and TRs. The main obligations under EMIR are: • central clearing for certain classes of OTC derivatives • application of risk mitigation techniques for non-centrally cleared OTC derivatives • reporting to TRs • application of organisational, conduct of business and prudential requirements for CCPs, and • application of requirements for TRs, including the duty to make certain data available to the public and relevant authorities.
Payment Services Directive 3 (PSD3)	European Directive which defines payment services as follows: <i>'Services enabling cash to be deposited in or withdrawn from, for example, a bank account, as well as all the operations required to operate the account. This can include transfers of funds, direct debits, credit transfers and card payments. Paper transactions are not covered by the directive.'</i> The aim of the directive is to: • provide the legal foundation for the further development of a better integrated internal market for electronic payments within the EU • put in place comprehensive rules for payment services, with the goal of making international payments within

	the EU as easy, efficient, and secure as payments within a country • open up payment markets to new entrants leading to enhanced competition, greater choice, and better prices for consumers, and • provide the necessary legal platform for the single euro payments area (SEPA).
Sarbanes-Oxley (SOX) Act 2002	United States (US) Regulation SOX concerns the improvements of the financial reporting process and restoration of investor confidence in the US financial markets. The objective: • <i>'To protect investors by improving the accuracy and reliability of corporate disclosures'</i>. • Applies to US public companies and their global subsidiaries. In addition, it applies to foreign companies with shares listed on US stock exchanges. Section 404 lays out the requirement for the management of a US public company to report annually on the operational effectiveness of the company's internal controls over financial reporting. The company's auditors must attest to and report on the management's assertion over the effectiveness of internal financial controls. This section significantly impacts the governance and behaviour of any business with a US listing, including non-US companies, and their global subsidiaries and joint ventures. Key issues related to audits:

- Audit firms that both perform audits and provide consulting – auditors are prevented from providing certain non-audit services, and are only permitted to provide other services, such as tax advice, if this is disclosed and approved by the audit committee of the company receiving the advice.
- Auditors have to be appointed by the audit committee of a company's board of directors rather than by company management and members of the audit committee must be independent of management.
- The lead accounting firm partner on an audit has to be replaced every five years.

An accounting firm may not audit a company where senior executives previously worked for the firm and participated in the audit within the previous year. Internal control standards to ensure the accurate reporting of their financial position:

- The chief executive officer (CEO) and chief finance officer (CFO) are responsible for ensuring that internal controls and procedures can provide accurate financial disclosures.
- The controls must ensure that the CEO and CFO are aware of material information.
- Compliance work must be performed on a continual basis to document and attest to the effectiveness of their internal controls.

	Related crimes: • Defrauding securities investors – up to 25 years in prison. • CEOs knowingly signing a false financial statement – fines of up to \$5 million and 20 years in prison for wilful violations. • Obstruction of justice by destroying documents – fines and prison terms of up to 20 years.
Central Securities Depositories Regulation (CSDR)	EU regulation that came into force in 2014, introducing uniform requirements for the settlement of financial instruments in the EU as well as rules related to the organisation and conduct of central securities depositories (CSDs) to promote safe, efficient, and smooth settlement. Applies to all firms that trade securities in the EU regardless of their location. A CSD is an institution that holds financial instruments including equities, bonds, money market instruments and mutual funds. Settlement fail: non-occurrence of settlement or partial settlement of a securities transaction on the intended settlement date, due to a lack of securities or cash and regardless of the underlying cause. CSDR introduces measures to prevent settlement fails, or to resolve them between trade date and intended settlement date.

1.5.3 Financial Crime

There is no internationally accepted definition of 'financial crime'. It is generally understood to include the laundering of the proceeds of any crime, terrorist financing, the financing of the proliferation of weapons of mass destruction (WMDs), breaches of financial and trade sanctions, market abuse, and tax evasion. In the UK, FSMA broadly defines the term to include 'any offence involving fraud or dishonesty; misconduct in or misuse of information relating to, a financial market; or handling the proceeds of crime', and defines the term 'offence' as behaviour that 'includes an act or omission which would be an offence if it had taken place in the UK'. Thus, expanding the remit of the legislation to include conduct occurring outside the UK. In the context of global financial compliance, the UK Bribery Act and the Foreign Corrupt Practices Act are of particular importance. There are a number of financial crime related regulations with extra-territorial reach such as the ones summarised in the table below.

Legislation	Description
UK Bribery Act (2010)	Designed to implement the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. The Act created offences of: • offering or receiving a bribe • bribery of foreign public officials, and • a failure to prevent a bribe being paid on an organisation's behalf. Courts have jurisdiction over offences committed in the UK, but also outside the UK if the person committing the offence has a close connection with the UK because they are a British national or ordinarily resident in

the UK, a body incorporated in the UK, or a Scottish partnership.

In addition, the offence of failing to prevent a bribe extends the jurisdiction of the UK courts to relevant foreign commercial organisations. A relevant commercial organisation is defined as:

'a body or partnership incorporated or formed in the UK irrespective of where it carries on a business, or an incorporated body or partnership which carries on a business, or part of a business in the UK irrespective of the place of incorporation or formation.'

The act provides a defence to failing to prevent a bribe where an organisation can show that it has 'adequate procedures' in place.

For example, a foreign company which carries on any 'part of a business' in the UK could be prosecuted under the Bribery Act for failing to prevent bribery committed by any of its employees, agents or other representatives, even if the bribery takes place outside the UK and involves non-UK persons. 'Part of a business' is not defined in the Act, but even a UK representative office or agent may be sufficient for the purposes of the corporate offence.

It is up to the courts to determine whether an organisation carries on a business in the UK, taking into account the particular facts in individual cases

**Foreign Corrupt
Practices Act
(1977)**

The provisions of the FCPA make it unlawful for a US person, and certain foreign issuers of securities, to make a corrupt payment to a foreign official for the purpose of obtaining or retaining business for or with, or directing business to, any person.

The provisions also apply to foreign firms and persons who take any act in the furtherance of such a corrupt payment while in the US. In 1977, the International Chamber of Commerce (ICC) published Rules of Conduct to Combat Extortion and Bribery. These rules set out basic measures by which companies can reduce the likelihood of corrupt practices.

FCPA has had significant impact on the way American firms do business, both in the US and overseas.

Between 2020 and 2023, 29 international companies have agreed to pay settlements in excess of USD 2 billion in relation to FCPA violations. ♦

Firms need to have Know Your Customer (KYC) controls in place, particularly for politically exposed persons (PEPs). Controls must include the details of the management and ownership of the entities with whom they do business.

FCPA assists with SOX compliance since SOX legislation also imposes requirements on firms to disclose instances of fraud as well as reporting annually on their systems of internal control.

	Detailed compliance programmes have to be in place to prevent and detect any improper payments by employees or agents, particularly those operating in the field in tough emerging markets, where competition and general business practice often mean that rules set at head office are difficult to implement in practice and managers may attempt to circumvent regulations to achieve a sale. Particular controls include: • due diligence checks on third parties to establish their bona fides at the outset of the relationship but, very importantly, as the relationship continues • committees with senior executive representation to oversee the risks of bribery and corruption, to receive periodic management information • detailed training for staff, and • general monitoring of processes and controls by independent risk, compliance or audit functions.
Foreign Account Tax Compliance Act (FATCA) 2010	Enacted by the US in 2010 as part of the Hiring Incentives to Restore Employment (HIRE) Act. Important development in US efforts to combat tax evasion by US persons holding investments in offshore accounts. US taxpayers holding financial assets outside the US are required to report those assets to the Internal Revenue Service (IRS).

	Foreign financial institutions (FFIs) must report directly to the IRS certain information about financial accounts held by US taxpayers, or by foreign entities in which US taxpayers hold a substantial ownership interest. Firms outside the US are not directly subject to US legislation, but are required to comply via intergovernmental agreements to improve tax compliance. Certain information about the financial accounts held by US taxpayers, or by foreign entities in which US taxpayers hold a substantial ownership interest, need to be reported via their national tax authorities. An FFI in a country not party to an intergovernmental agreement is expected to register with the IRS.
EU Anti-Money Laundering Directives	A series of EU directives providing a risk-based approach that requires EU-wide risk assessments in combination with national and institutional risk assessments. Implements the Financial Action Task Force's (FATF) recommendations and covers customer due diligence (CDD) and other requirements concerning financial institutions and designated non-financial businesses and professions (DNFBPs). DNFBPs are non-financial sectors identified to be vulnerable to money laundering abuse, such as lawyers, accountants, real estate agents and some types of businesses that deal in high-value goods. Extends the definition of PEPs to also include those in the home country of the institution.

	Over time, amendments have been made to the directives to ensure they remain current. The Anti-Money Laundering Directive (AMLD) is incorporated in law within individual member states.
Common Reporting Standard (CRS) for the Exchange of Financial Information	Framework to automatically share information on an annual basis on residents' assets and incomes in conformation with the standard, replacing individual treaties for sharing information on request. Step towards an internationally coordinated approach to the disclosure of income earned by individuals and organisations. As a measure to counter tax evasion, it builds upon other information-sharing legislation, such as FATCA and the EU Savings Directive, but is wider in scope. Sets out the financial account information to be exchanged. The FIs are required to report the different types of accounts and taxpayers covered, as well as the CDD procedures to be followed. These initiatives involve governments obtaining information from their FIs and exchanging data automatically with other nations. In practical terms, it is a framework of an information standard for the Automatic Exchange of Information (AEOI). FIs (and other investment entities) will have significant additional reporting responsibilities, in order to disclose details of their account holders, with potential penalties for those unable or unwilling to comply fully.

The legal basis for the exchange of data is the Convention on Mutual Administrative Assistance in Tax Matters and the idea is based on the FATCA implementation agreements.

The AEol consists of two regulations or agreements:

- **OECD Competent Authority Agreement (CAA)** – bilateral agreement between jurisdictions that have signed up to the AEol which allows the competent authorities (typically the jurisdiction's tax authority) to exchange information.
- **OECD Common Reporting Standard (CRS)** – baseline regulation to be adopted in the jurisdictions that have signed up to AEol. It sets out who will be reporting, what will be reported, and to some degree, the format of the reporting. This could be seen as the minimal requirements for the regulations.

Financial information to be reported includes interest, dividends, account balance, income from certain insurance products and sales proceeds from financial assets. In gathering data, residency or tax residency within a country is the decisive factor, not citizenship. The CRS relies heavily on local anti-money laundering (AML) and KYC requirements, and on self-certification by account holders, although it includes some documentation remediation.

Example – UK Bribery Act

A German construction company with a UK subsidiary appoints an intermediary to facilitate business in Africa, and the intermediary pays a bribe to a local official. In some circumstances, the German parent could be liable under the UK Bribery Act for failing to prevent bribery. The Act is engaged simply by virtue of the existence of a UK operation.

In turn, the UK subsidiary is itself at risk of prosecution if a person or company associated with it is involved in bribery, as are any German nationals working for the UK subsidiary and, therefore, 'ordinarily resident' in the UK, if they are found to have paid or received a bribe. 'Part of a business' is not defined in the Act, but even a UK representative office or agent may be sufficient for the purposes of the corporate offence.

1.6 Exchanges, Multilateral Trading Facilities (MTFs), Organised Trading Facilities (OTFs), and Systematic Internalisers (SIs)



1.1.7 Understand how regulation operates in an exchange-traded environment

1.1.8 Understand the key benefits of regulated market structures: trading venues (exchanges, multilateral trading facilities, and organised trading facilities); systematic internalisers

1.6.1 Exchanges

A large proportion of trades in financial instruments are carried out through established stock exchanges, such as the London Stock Exchange (LSE), the New York Stock Exchange (NYSE) and the Tokyo Stock Exchange (TSE).

Typically, stock exchanges are responsible for:

- regulating the stock market
- approving applications for listing
- provision and administration of business and listing rules
- supervising admission of members and compliance by listed companies with the listing rules and corporate disclosure policies
- market surveillance and risk management for the clearing of securities and derivatives, and
- overseeing the capital requirements of brokers and investigating brokers as and when they deem necessary.

Exchanges and their operators are normally subject to regulation and supervision by monetary authorities or other regulatory authorities. For example, in Singapore, the Monetary Authority of Singapore (MAS) is the body charged with these responsibilities; while in the UK it is the FCA.

In the UK, any corporate body or an unincorporated association may apply to the FCA for an order declaring it to be a recognised investment exchange (RIE).

The FCA will look to establish:



Whether the applicant is 'fit and proper' to operate as an exchange.



Whether it has sufficient financial resources to properly carry out its activities.



That the applicant is willing and able to share information with the FCA, and to promote and maintain high standards of integrity and fair dealing, including laying down rules for activities on the exchange.



That the applicant will record, monitor and enforce compliance with the rules of the exchange.

Exchange operators are expected to take disciplinary action against members, directors, employers and trading representatives, or against any person registered by the exchange.

Disciplinary Actions under an Exchange Environment

Disciplinary action and enforcement penalties are usually determined by a disciplinary committee. The following actions may be available – either individually or in combination:

- A reprimand.
- A fine (usually within limits laid down/agreed by the exchange).
- Suspension of the member.
- Expulsion of the member or trading representative.

Where the matter involves a violation of the law, the matter may be referred to the relevant authorities for further action. An appeal process is normally provided so that members of the exchange may appeal to an appeals committee against the decision of the disciplinary committee.

1.6.2 MTFs, OTFs and SIs

Under MiFID and MiFID II, a new regime was introduced for trading platforms, namely **Multilateral Trading Facilities (MTFs)**, organised trading facilities (OTFs) and systematic internalisers (SIs).

MTFs offer an alternative to traditional trading exchanges. They are described by the FCA as being any system that brings together multiple parties (eg, retail investors or other investment firms) that are interested in buying and selling financial instruments. Operated by an investment firm or a market operator, MTFs facilitate multilateral transactions in instruments such as shares, bonds and derivatives. This is done within the MTF operator's system.

The introduction of MTFs, under MiFID, allows greater competition to the formalised investment exchanges subject to direct prudential and supervisory oversight by national regulators.

Accordingly, MiFID replaced rules in many markets that required trades to be executed at local exchanges. Instead, for example, banks are allowed to act as systematic internalisers (SIs), matching customer orders internally rather than showing these to the market.

Organised Trading Facilities (OTFs)

An OTF is a new category of trading venue introduced by MiFID II. It is a multilateral trading system that is not a regulated market or an MTF. Bonds, structured finance products, emission allowances and derivatives can be traded on an OTF, but equities cannot. As a result of the introduction of OTFs, transactions previously categorised as off-venue now fall under a multilateral trading environment which increases overall market transparency, reduces the prevalence of opaque market models and products, and increases the quality of price discovery, investor protection, and liquidity.

OTFs assist market participants in meeting MiFID II platform-trading obligations for derivatives and provide an additional trading venue for derivatives, bonds, structured financial instruments, and emission rights that are sufficiently liquid for the trading obligations to apply. Instruments not subject to the trading obligation can be traded on OTFs through market making schemes.

Since both are multilateral trading environments, the rules for OTFs and MTFs are the same. For example, OTFs are subject to the same pre- and post-trade transparency requirements as an MTF, which apply to any order or transaction executed through their systems or under their rules. The key difference is the ability and requirements of an OTF to use discretion when matching buying and selling interests. The use of discretion must be in line with fair and orderly trading and best execution obligations to clients.

OTFs:

- must establish clear trading rules and processes, including clear and non-discriminatory access rules,
- need to have the ability to suspend instruments from trading and maintain resilient systems to facilitate continuity of trading under stressed conditions,
- are subject to the same pre- and post-trade transparency requirements as MTFs, which apply to any order or transaction executed through their systems or under their rules,

- have to publish the details of current bids and offers and the depth of trading interests of those prices; in addition, details of transactions have to be made public as close to real time as is technically possible, and
- can operate under any trading protocol as it is consistent with fair and orderly trading and the exercise of discretion.

Effective arrangements and procedures need to be established and maintained to enable the regular monitoring of compliance by their members. OTFs need to identify, and act upon, breaches of rules, disorderly trading conditions or conduct that may involve market abuse in relation to any transactions undertaken by their members on the OTF's systems. OTF operators must use discretion when deciding when to place or remove an order on their OTF, and whether or not to match a specific client order with orders available in the system, subject to best execution obligations. Investment firms or market operators running an OTF need to ensure client orders are not executed against the proprietary capital of:

- the firm, or
- any entity that is part of the firm's legal group.

The use of proprietary capital is only permitted for illiquid sovereign debt instruments. An OTF may only engage in matched principal trading if this has been agreed by clients, although matched principal trading is not permitted for derivatives subject to the EMIR - clearing obligation.

Systematic Internalisers (SIs)

Traditionally called **market makers**, SIs are investment firms who match 'buy' and 'sell' orders from clients in-house, providing that they conform to certain criteria. Instead of sending orders to a central exchange, such as the LSE, and showing them on the market, investment banks, such as UBS, can match them with other orders on their own book. It should be noted that an SI may only act as an SI for as little as one asset class under MiFID II. Furthermore,

European Securities and Markets Authority (ESMA) does not have any immediate plans to issue a register of SIs.

SIs are able to compete directly with stock exchanges and automated dealing systems, but they have to make such dealings transparent. They must show a price before a trade is made. After a trade is made, they have to give information about the transaction, just like conventional trading exchanges.

The same legal entity cannot operate both an OTF and an SI. OTFs are prohibited from interacting with an SI if this allows any quotes or orders in the SI to interact. This prohibition also applies to quotes and orders in another OTF where two OTFs are interacting.

1.6.3 Key Benefits of Regulated Market Structures

The following table highlights the key features and benefits of the various types of trading venue:

Type of Trading Venue	Features	Benefits
Recognised investment exchange (a regulated market)	A more formal market with the highest standards of entry. Companies raising capital must subscribe to sets of listing and disclosure standards.	Demonstrates quality of business- raising capital. Encourages investor confidence. Maintains pool of capital.
MTFs (regulatory permission required)	Described as a form of 'exchange lite'. Does not have a listing process and cannot	Introduction enabled greater competition between trading venues.

	change the regulatory status of a security. Must be pre-trade transparent, the price of existing orders must be available on market data feeds. Must be post-trade transparent, any trades must be published in real time. Prices/charges are public and applied consistently across all members.	Higher trading speeds which are attractive to high-frequency traders. Lower cost base. Trading incentives for members relating to trade volumes.
OTFs	Multilateral system which is not a regulated market or MTF. Order execution is carried out on a discretionary basis.	Similar to MTFs in having lower costs. Allows the operator to provide a tailored service. Provide greater choice to clients by allowing discretion over permitted execution.
SI	A firm that executes orders from its clients against its own book or against orders from other clients.	Similar to MTFs in having lower trading costs. Speed of trade.

	Also treated as a 'mini-exchange', hence subject to pre- and post- trade price transparency.	
--	--	--

1.7 Off-Market Transactions



1.1.9 Understand how regulation applies to OTC derivatives transactions

OTC transactions are those that are conducted off-market, or off-exchange. OTC markets are decentralised markets, whereby market participants trade various assets (eg, stocks, currencies and commodities and other instruments) directly between two parties, without a central exchange or broker. As OTC markets do not have physical locations, trading is conducted electronically.

In its simplest form, a derivative is a security which is based upon or derived from another asset. Derivatives can either be standardised and traded on public exchanges (eg, futures), or can be customised and traded OTC (eg, credit default swaps (CDSs)). The latter are subject to counterparty risk (ie, when one or either party to such an OTC agreement could potentially default on its obligations – see below), whereas exchange-traded derivatives are cleared by a centralised clearing exchange and the risk of default is therefore transferred to a clearing house.

Trading in OTC derivatives is opaque because they are privately negotiated contracts and consequently any information concerning any one of them is usually only available to the contracting parties.

The global financial crisis brought the OTC derivatives market to the forefront of regulatory attention. The near collapse of Bear Sterns – the default of Lehman Brothers, and the bailout of American International Group inc (AIG) in 2008 highlighted the shortcomings in the functioning of this market. The main observations are summarised in the sections below.

Transparency

The global financial crisis highlighted a lack of information on positions and exposures of individual firms in OTC derivatives. On the one hand, this lack of information prevented regulators from a timely detection of risks building up at individual institutions and in the system as a whole. It also prevented them from accurately assessing the consequences of a default of a market participant and, therefore, from responding in an appropriate manner should such a default occur (Lehman's case was a clear demonstration of this). On the other hand, it helped fuel suspicion and uncertainty among market participants during the crisis.

Counterparty Risk

OTC derivative contracts bind counterparties together for the duration of the transaction. Throughout the lifetime of a contract, counterparties build up claims against each other, as the rights and obligations contained in the contract evolve with the underlying that the contract is derived from. This gives rise to counterparty risk. Clearing is the function by which these risks are managed over time. It can be carried out centrally, through a CCP, or bilaterally between two parties directly. Although both types of clearing are used in the OTC derivatives market, bilateral clearing is the most used form of the two.

The global financial crisis highlighted that the level of counterparty risk related to OTC derivatives was much higher than previously thought by both market participants and regulators. The main reason for this lies in inadequate collateralisation in the part of the market that is cleared bilaterally, either because some market

participants are not required to provide collateral to secure their OTC derivatives trades or because of issues related to the risk management processes of those market participants that do provide collateral.

Operational Risk

Between the agreement and the confirmation of the transaction, an OTC derivative follows a number of processing steps. In addition, the transaction is subject to a number of events, such as collateral management and settlement of cash payments, that are inherent in the rights and obligations of the contract.

The OTC derivatives market allows for a high degree of flexibility in defining the economic and legal terms of derivatives contracts, resulting in highly bespoke and complex contracts. These contracts require significant manual intervention in many stages of the processing. This increases operational risk, may lead to legal risk, may limit transparency, and may result in an increase of counterparty [credit risk](#).

Actions Taken

As a result of the financial crisis, government bodies, like the EU Commission, identified policy actions to:

- increase transparency of the derivatives market by requiring market participants to report all necessary information on their OTC derivatives portfolios to a trade repository (TR) or, if that is not possible, directly to regulators
- require the publication of aggregate position information
- reduce counterparty credit risk and operational risk in trading through the use of CCP clearing for OTC derivatives that meet predefined eligibility criteria and by the setting of specific targets for legal and process standardisation, and
- enhance market integrity and oversight, through the use of a post-trading market infrastructure.

1.8 FinTech



- 1.1.10 Understand how regulators approach FinTech products: distributed ledger technology (DLT); digital assets; robo-advice; artificial intelligence and big data; regulators' expectations on the compliance function regarding FinTech products
-

In general terms, financial technology (Fintech) is defined as the use of technology to boost competitive advantage in the financial services sector. Examples include innovative mobile solutions, cryptocurrencies, and artificial intelligence (AI). Fintech is disruptive in that it allows newcomers in the market to provide financial services in new and innovative ways. New ways of working come with new challenges and require additional governance and regulations to ensure continuing stability of the financial infrastructure.

1.8.1 Distributed Ledger Technology (DLT) and Digital Assets

Distributed ledger technology (DLT) is the technological infrastructure that allows simultaneous access, validation, and updating across a network spread out over multiple entities or locations. It is commonly referred to as blockchain technology and was first introduced by Bitcoin in 2009. Bitcoin is a cryptocurrency that can be transferred between users without an intermediary. A cryptocurrency is a digital currency which uses decentralised systems to verify transactions and maintain records.

Cryptocurrencies are wholly or partially banned in several countries. For example, China has banned both initial coin offerings and trading platforms quoting concerns about financial stability and money laundering as the reasons. Bolivia has also completely

banned cryptocurrencies due to lack of consumer protection and the potential for money laundering.

Changes in the technological environment are fast-paced and requires a new approach to regulations. Most regulators have set up a regulatory sandbox in which new technology can be trialled. This is referred to as a technology neutral approach, aimed at assessing the regulatory requirements for business models and client outcomes arising from the use of the new technologies.

Regulations do not focus on the technical details but on implementation. The regulatory sandbox allows the regulator to review the implementation and assess whether new regulations are required or whether existing rules contain sufficient flexibility for firms to use the new technology. Regulators are catching up with these developments and have been introducing new regulations such as the EU rules on cryptomarkets (Markets in Crypto-Assets (MICA) Regulation).

The high volatility of cryptocurrency prices, which is the result of supply and demand on unregulated crypto exchanges, makes them unsuitable for daily use since it means they do not retain purchasing power, and do not encourage spending. Stable coins have been developed in an attempt to offer price stability with the lowest possible level of inflation. Although they can be backed by any asset, they are typically backed by a reserve asset (eg, US dollar, euro, gold) providing the stability of fiat currencies whilst ensuring the privacy of payments offered by cryptocurrencies. The main benefit is that they allow international transfers without the need to have bank accounts in multiple currencies.

1.8.2 Robo-Advice

Robo-advice or robo-advisors are digital platforms that provide automated financial planning services with little or no human intervention. A robo-advisor collects information from customers

concerning their financial situation, future goals, and risk appetite by means of online surveys. This information is then used as input into an algorithm to provide investment advice.

There is a wide range of robo-advisors in the market, with the quality and customer take-up depending on a number of key characteristics such as:

- ease of account setup
- robust goal planning
- security features
- customer services, and
- fees.

Robo-advisors mostly use passive indexing strategies, are typically inexpensive and only require a small opening balance. As a result, they are open to a wide range of customers. The global robo-advisory market size was valued at USD 10.86 billion in 2025 and is projected to grow from USD 14.08 billion in 2026, to USD 102.03 billion by 2034♦.

From a regulatory perspective, robo-advice falls under the same category of services as other financial advice and regulations such as KYC, fair treatment of customers, and suitability of advice.

Robo-advisors have to follow the same rules and regulations as human advisors including a requirement to be authorised by the appropriate regulatory authority. In the US, robo-advisors must be registered with the SEC and are subject to the same securities laws and regulations as other broker-dealers. In addition, most are registered with the Financial Industry Regulatory Authority (FINRA), a self-regulation organisation.

1.8.3 Artificial Intelligence (AI) and Big Data

AI refers to the application of computers and machines to mimic the problem-solving and decision-making capabilities of the human

mind. It can be applied in financial services in the following ways:

- Enhance accuracy of credit scoring using algorithms and large volumes of data from a range of different sources. Due to the absence of bias and judgement, the decision-making process is more rational.
- Combatting and preventing fraud and ML by identifying irregular patterns in customer behaviour and suspicious transactions.
- Automated trading platforms making recommendations and predictions based on algorithms that assess large volumes of data. The use of AI reallocates time to customer interaction rather than data analysis and circumvents bias and judgement.
- Chatbots to interact with customers applying a combination of AI and big data, addressing the simple, rules-based queries with a transfer to a customer representative for complex queries.

The main advantages of using AI are that it saves time due to the capacity to analyse large amounts of data much faster than a human can, it reduces bias and judgement in decision making, and is self-learning. The main disadvantages of AI are associated with high development costs, risks to employment, and the potential for bias, which can occur because humans chose the algorithms and decided how they will be applied.

Big Data

The term big data refers to large, complex data sets, particularly from new data sources that can be used to address complex business problems. Big data is higher in volume, variety and velocity, and allows for more complex and complete answers. It refers to a combination of structured and unstructured data collected by firms that can be mined for information to detect trends, for targeted marketing, and other advanced modelling applications.

The advantage of big data is that it enables firms to unlock insights that would not be possible to see without large amounts of data. The disadvantage is that there is a risk that too many variables are included in the analysis to fit the expected trend instead of highlighting the actual trend.

1.8.4 Regulatory Expectations

Although Fintech has been around for a while, the roll-out of new technological solutions by financial institutions has accelerated since 2020 in light of the coronavirus (COVID-19) pandemic to allow banks and other financial institutions to continue their operations.

Fintech, AI, big data and other technological advances provide financial institutions with significant opportunities to increase customer-focused initiatives, but also present a number of challenges including regulatory expectations. In the UK, for example, Fintech companies that are considering providing financial services will need to be regulated by the FCA and, for Fintech companies providing payment services, the Payment Systems Regulator.

Regulators expect firms to have appropriate corporate governance in place to manage the deployment of new systems, which includes the following:

- Sufficient involvement at board level.
- Engagement of risk and compliance functions.
- Training and development of staff in general, and board members, risk and compliance functions in particular.

In the context of compliance functions, Regtech is a subset of Fintech which refers to the management of regulatory processes through technology. Examples in the context of compliance and Fintech are:

- crypto assets and stablecoins – the Financial Stability Board (FSB) has issued recommendations related to risk-proportionate regulation, supervision, and oversight
- cyber and data security in relation to cloud services
- governance of AI and machine learning solutions
- update of the [Money Laundering Regulations](#) to incorporate cryptocurrencies and prepayment cards, and
- updated Payment Services Directive (PSD).

The main challenges for the compliance function are associated with the speed at which new technology solutions are developed, budget and cost, and uncertainty about regulatory expectations. Firms deal with this by keeping up to date with recent developments and trends, for example, via specialised training and industry groups.



2. The International Approach to Regulation

2.1 Jurisdiction of Different Regulators



1.2.1 Know the jurisdiction of different types of regulators

The responsibilities of international regulatory organisations range from coordination and guidance through to setting cross-border principles and detailed rules.

The following summarises the typical jurisdiction of different types of regulators:

Type of Regulator	Jurisdiction
Recognised investment exchanges	Members of the exchange and listed securities, contracts or relevant financial instruments. Many stock exchanges have a national remit, but they are becoming more international in nature as global markets develop. Membership is often international, subject to the exchange rules and terms of membership.
Other SROs	Typically cover insurance markets and investment services, such as financial advice,

	investment management, and mortgages. Members are usually national and, accordingly, the focus of the SRO is essentially national in nature.
Government-appointed national regulatory bodies, such as central banks and other statutory-based regulatory authorities	Broad jurisdiction covering most financial markets, participants and products. Includes banking, insurance, and investment-related activities, both retail and wholesale. Although national in focus, increasingly forced to coordinate approaches because of the global interdependent nature of financial markets.
International regulatory authorities and national authorities with international reach	Regional jurisdiction covering a number of states with a broad coverage of banking, insurance and investment. Cross-border and international in nature with extraterritorial reach. Establish principles of regulation and develop detailed rules.
International regulatory organisations	International focus, established to coordinate at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies.

2.2 International Regulatory Organisations and Standard Setting



- 1.2.2 Understand the role of international regulatory organisations: Bank for International Settlements (BIS); Financial Stability Board (FSB); The International Organisation of Securities Commissions (IOSCO); European regulatory bodies: The European System of Financial Supervision (ESFS)/ European Supervisory Authorities (ESAs)/The European Systemic Risk

Board (ESRB); Securities and Exchange Commission (SEC);
International Sustainability Standards Board (ISSB)

- 1.2.3 Know the role that professional bodies play in relation to regulatory requirements
 - 1.2.4 Understand how international regulatory organisations aid the implementation of regulation in developing countries
 - 1.2.5 Know the three objectives of securities regulation as defined by IOSCO
-

2.2.1 Bank for International Settlements (BIS)

Established in 1930, the BIS serves as a central bank for central banks to foster international monetary and financial cooperation. BIS customers are central banks and international organisations. The BIS does not accept deposits from, or provide financial services to, private individuals or corporate entities. The BIS is headquartered in Basel, Switzerland.

The regulatory guidelines produced by the BIS, such as the Basel Capital Accords and the guidelines for corporate governance, do not automatically have any force in national or international law. Countries around the world that choose to implement them do so by making changes to their own legal and regulatory processes. The International Banking Federation (IBFed), incorporated in 2004, facilitates this effort. The IBFed represents the combined views of their members which are national banking associations. Collectively, they represent in excess of 18,000 banks.

Their global reach enables IBFed to function as the key international forum for addressing legislative, regulatory and other issues of interest to the global banking industry. For countries that are required to implement international laws through membership of a trading bloc or political union, an extra layer of complexity exists when implementing the BIS regulation since the union or bloc's laws may not be the same as the BIS requirements.

The Basel Committee on Banking Supervision (BCBS) is part of the BIS and provides a forum for international cooperation on bank regulation. It was established in 1974 and has 45 members representing 28 jurisdictions. Members are central banks or the country's authority responsible for banking supervision. The BCBS's objective is to enhance financial stability by improving supervisory know-how and the quality of banking supervision worldwide. This

is achieved by exchanging information on national supervisory issues and techniques, with a view to promoting common understanding between national supervisors.

The BCBS best practice standards can be used by individual regulatory authorities when designing their local arrangements. These publications include the following high-level guidelines and supervisory standards:

- International Standards on Capital Adequacy (Basel Accords).
- Core Principles for Effective Banking Supervision.
- Core Principles Methodology.
- Concordat on cross-border banking supervision.

The BCBS is supported by five working groups:

- Policy Development.
- Supervision and Implementation.
- Basel Consultative Group.
- Macroprudential Supervision.
- Accounting Experts.

2.2.2 Financial Stability Board (FSB)

The purpose of the FSB is to coordinate, at the international level, the work of national financial authorities and international standard-setting bodies and to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies.

The FSB Secretariat is located in Basel, Switzerland, and hosted by the BIS. The mandate of the FSB is to:

- assess vulnerabilities affecting the financial system and identify and oversee action needed to address them
- promote coordination and information exchange among authorities responsible for financial stability
- monitor and advise on market developments and their implications for regulatory policy
- advise on and monitor best practice in meeting regulatory standards
- undertake joint strategic reviews of the policy development work of the international standard-setting bodies to ensure their work is timely, coordinated, focused on priorities, and addressing gaps

- set guidelines for and support the establishment of supervisory colleges
- manage contingency planning for cross-border crisis management, particularly with respect to systemically important firms, and
- collaborate with the International Monetary Fund (IMF) to conduct early warning exercises.

The FSB has a unique composition among international bodies, because it brings together senior policy makers from ministries of finance, central banks, and supervisory and regulatory authorities, the G20 countries, plus four other key financial centres – Hong Kong, Singapore, Spain and Switzerland. In addition, it includes international bodies, including standard-setters and regional bodies like the European Central Bank and European Commission. This means that all the main players who set financial stability policies across different sectors of the financial system are at one table. So, when policies are agreed, they also have the authority to carry them out.

The FSB is not a treaty-based organisation. Policies agreed by the FSB are not legally binding, nor are they intended to replace the normal national and regional regulatory processes. Instead, the FSB acts as a coordinating body, to drive forward the policy agenda of its members to strengthen financial stability. It sets internationally agreed policies and minimum standards that its members commit to implement at national level.

The FSB regularly reports to the G20 which regularly endorses the FSB's policy agenda and supports implementation of agreed international standards. However, the FSB is not run by the G20 – membership is somewhat wider, and the FSB comes to independent policy views on issues.

The FSB operates through a three-stage process for the identification of systemic risk in the financial sector (the vulnerabilities assessment), for framing the financial sector policy actions that can address these risks (policy development), and for overseeing implementation of those responses (implementation monitoring).

2.2.3 International Organisation of Securities Commissions (IOSCO)

The IOSCO is an international association of securities regulators, created in 1983 and, as of February 2026, it has 134 ordinary members. Any regulatory body responsible for securities regulation can become an ordinary member. In the absence of a governmental or statutory regulatory body in a jurisdiction, a

self-regulatory body, such as a stock exchange, may be an ordinary member until such time as a governmental regulatory body from the same jurisdiction becomes the ordinary member for that jurisdiction. Through their permanent structures, member agencies currently assembled together in IOSCO have resolved to:

- cooperate in developing, implementing and promoting adherence to internationally recognised and consistent standards of regulation, oversight and enforcement, in order to protect investors, maintain fair, efficient and transparent markets, and seek to address systemic risks
- enhance investor protection and promote investor confidence in the integrity of securities markets, through strengthened information exchange and cooperation in enforcement against misconduct and in supervision of markets and market intermediaries, and
- exchange information at both global and regional levels on their respective experiences in order to assist the development of markets, strengthen market infrastructure and implement appropriate regulation.

IOSCO's 38 principles of securities regulation have received support from the G20 group of countries and the FSB. These principles are based on three objectives of securities regulation which are:

- the protection of investors
- ensuring that markets are fair, efficient and transparent, and
- the reduction of systemic risk.

The 38 principles do not have any legal force themselves but need to be practically implemented under the relevant legal framework in member countries in order to achieve the objective of regulation described above. The principles are grouped into ten categories as follows:

1	Relating to the Regulator	6	Auditors, Credit Rating Agencies, and other information providers
2	Self-Regulation	7	Collective Investment Schemes
3	Enforcement of Securities Regulation	8	Market Intermediaries
4	Cooperation in Regulation	9	Secondary Market

IOSCO, the BIS and the FSB are all involved in setting standards that are intended to be adopted as broadly as possible. Their membership, particularly that of IOSCO, is drawn from a wide range of countries, and by sharing information and analysis and organising collaborative events, they all seek to aid both developed and developing countries.

2.2.4 European Regulatory Bodies

The European System of Financial Supervision (ESFS)

The European System of Financial Supervision (ESFS) is the institutional architecture of the EU's framework of financial supervision created in response to the financial crisis. It consists of two components, the European Supervisory Authorities (ESAs), and the European Systemic Risk Board (ESRB) under the responsibility of the European Central Bank (ECB).

European Supervisory Authorities (ESAs)

Since January 2011, the regulation of financial services across Europe is now overseen by three **European Supervisory Authorities (ESAs)**, each covering rules and regulations for a specific part of the financial services industry, and they are:

- **European Banking Authority (EBA)** – banking
- **European Securities and Markets Association (ESMA)** – securities markets, and
- **European Insurance and Occupational Pensions Authority (EIOPA)** – insurance and pensions companies.

The ESAs work with the ESRB to ensure financial stability and to strengthen and enhance the EU supervisory framework. They will work to improve coordination between national supervisory authorities and raise standards of national supervision across the EU.

What is the ESAs' Role?

- Create a single EU rulebook by developing draft technical standards, which will then be adopted by the European Commission as EU law. The ESAs also issue guidance and recommendations with which national supervisors and firms must make every effort to comply.

- Investigate national supervisory authorities in the event they believe a national supervisory authority is failing to apply EU law or is doing so in a way which appears to be in breach of EU law. Their findings may lead to recommendations to the national supervisor, followed by a formal opinion from the European Commission (EC) in the event the recommendation is not acted upon. If the supervisor does not comply with the EC's formal opinion, the ESAs may take decisions binding on firms or market participants to ensure they are complying with EU law.
- Temporarily ban certain financial activities. Legislation sets out what they can ban and in what circumstances. Where an emergency has been called by the EC, they have wide-ranging powers to ban financial activities.
- Provide EU-wide coordination in a crisis. If an emergency is declared, the ESAs may make decisions that are binding on national supervisors and on firms. However, these would be subject to certain conditions and would be limited to ensuring compliance with EU law.
- Mediate where national supervisory authorities disagree. If necessary, they will be able to resolve disputes by making a decision that is binding on both parties to ensure compliance with EU law.
- Ensure EU supervisory colleges function efficiently and that consistent approaches and practices are followed.
- Conduct regular peer reviews of national supervisory authorities to improve the consistency of supervision across the EU.
- Collect information from national supervisors to allow them to fulfil their role. This information will be used for analysing market developments, coordinating EU-wide stress tests and the macroprudential analysis undertaken by the ESRB.
- Consider consumer protection issues.
- Direct supervisory responsibility for credit rating agencies.

European Systemic Risk Board (ESRB)

The ESRB was established in 2010 in response to the global financial crisis and has responsibility for the macroprudential oversight of the financial system within the EU. As such, it is a key part of the ESFS framework.

The operation of the board has been entrusted to the ECB. In order to take advantage of existing and compatible structures, and to minimise any delay to the commencement of its operations, the ECB provides analytical, statistical,

administrative and logistical support to the ESRB, and technical advice is also drawn from national central banks and supervisors.

2.2.5 US Securities and Exchange Commission (SEC)

The US **Securities and Exchange Commission (SEC)**, established in 1934, is an independent agency of the US federal government. The SEC's main responsibility is to enforce federal securities laws, propose securities rules, and to regulate the securities industry. The mission of the SEC is to:

- protect investors
- maintain fair, orderly, and efficient markets, and
- facilitate capital formation.

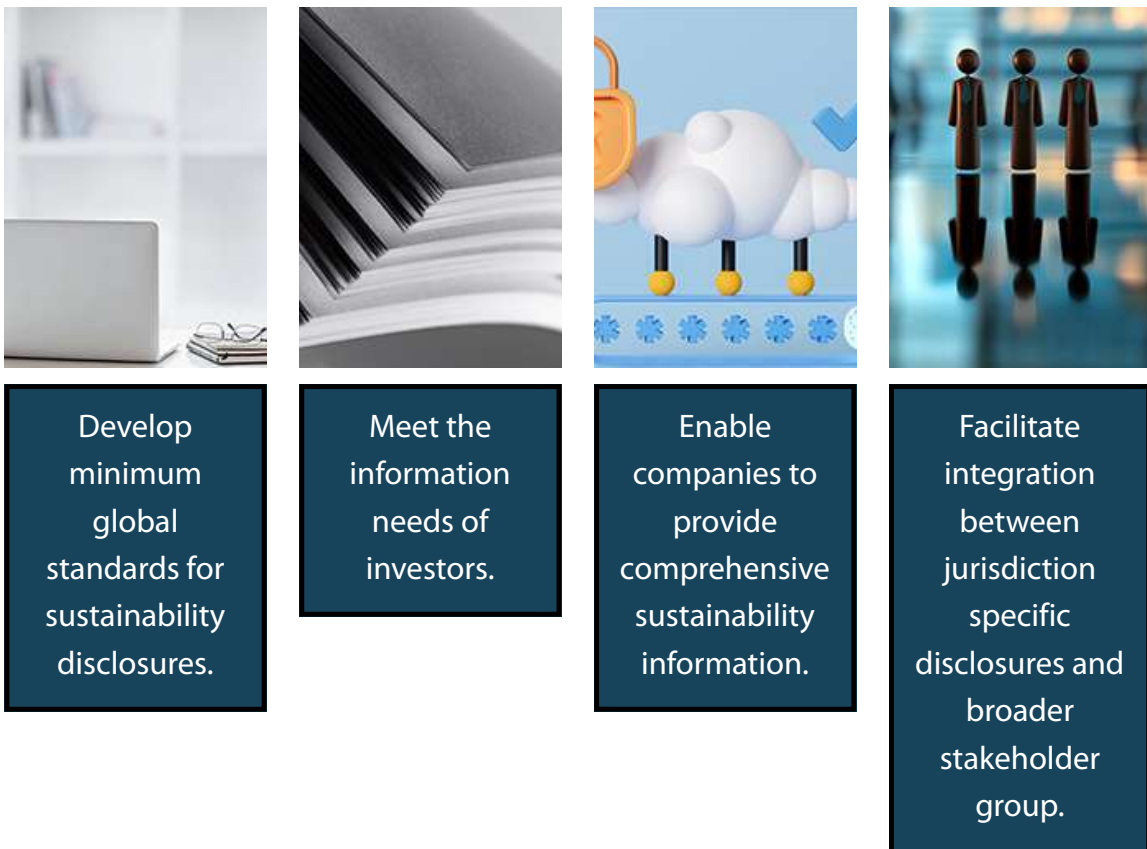
The SEC strives to promote a market environment worthy of the public's trust. The laws and rules governing the US securities industry derive from the concept that all investors should have access to certain basic facts about an investment before buying it, and as long as they hold it. Therefore, public companies are required to openly disclose meaningful financial and other relevant information in a timely manner.

The SEC supervises key market participants including securities exchanges, securities brokers and dealers, investment advisers, and mutual funds. Although it is the primary overseer and regulator of the US securities markets, the SEC works closely with many other institutions, including Congress, other federal departments and agencies, self-regulatory organisations (eg, the stock exchanges), state securities regulators, and various private sector organisations. In addition, the Chairman of the SEC represents the agency as a member of the Financial Stability Oversight Council (FSOC). The FSOC is established to provide comprehensive monitoring of the stability of the US financial system.

2.2.6 International Sustainability Standards Board (ISSB)

The ISSB is established by the International Financial Reporting Standards (IFRS) Board to develop high-quality standards for sustainability disclosures with a focus on the needs of investors and financial markets.

Its key objectives are to:



The ISSB's first set of standards was issued in June 2023 consisting of the following:

- **FRS1** – a set of disclosure requirements for sustainability related risks and opportunities.
- **FRS2** – specific climate related disclosures to be used in combination with FRS1.

Both standards incorporate the recommendations of the Task Force on Climate-related Financial Disclosures (TCFD).

2.2.7 Regulation in Developing Countries

Financial markets in developing countries are typically in the early stages of development, and may not require the same level of regulations as developed countries. Therefore, some of the international regulations are too comprehensive to be effective. However, they can be used as a starting point to tailor regulations to the local financial system. Implementing international regulations, even in a simplified form, will facilitate **integration** in the global financial system and the ability to transact with financial institutions in other

countries. In addition, it can attract foreign financial institutions to establish branches in the country.

2.2.8 Professional Bodies

Most industries and professions maintain structures to look after the overall well-being of that market and its participants. Similarly, the professional bodies within financial services markets perform a range of important functions:

- They uphold the standards of conduct of their members.
- They deliver training and other support mechanisms.
- They provide a forum for industry developments – whether self-initiated or in respect of proposed regulatory/legislative change.
- They provide a public face for agreed industry positions to be publicised, whether for public information or as part of specific lobbying efforts.

Professional bodies will often have discussions with regulators to discuss the approach to areas of concern and will provide their members with guidance on how regulatory requirements might be satisfied.

2.3 Implementing Regulatory Objectives and the Approach to Supervision



1.2.6 Understand how regulators implement their regulatory objectives

1.2.7 Understand the different regulatory approaches: risk-based; rules-based; thematic; relationship-based; principles-based

Financial institutions that want to establish themselves in a certain jurisdiction typically need to apply for a licence. Regulators will ensure that minimum entry standards are applied and approve those applications where it is certain that the firm will be prudently managed with a viable business model (in relation to all its activities) and effective controls for risk mitigation. This could lead to a regulator imposing limitations and requirements on any part of the business model or even refusing to authorise a firm and grant permission for it to undertake **regulated activities**.

The methods used by regulators will typically involve:

- the setting of prudential requirements to ensure that an authorised firm or person maintains sufficient capital resources commensurate with the level of risk they are running
- establishing business conduct rules, evidential provisions and guidance that will govern an authorised firm's relationship with its customers or counterparties
- providing detailed product regulations, often in the areas of packaged retail products, such as collective investment schemes and pensions, which set minimum standards aimed at the protection of retail investors and establish dispute resolution and compensation arrangements, and
- the setting of requirements and processes for investigation, supervision and enforcement of the rules.

Regulators will seek to maintain arrangements to supervise compliance with the requirements imposed on authorised persons. These arrangements may include the following:

- Requiring regular and potentially detailed reporting to the regulator covering, for example, the financial position of the firm, transactions undertaken, risk assessments undertaken by the firm itself and any relevant changes to its business.
- Considering the extent to which a firm represents a risk to the regulator's objectives, ie, adopting a risk-based approach in allocating the regulator's resources and focusing more on those risks which pose a threat to its objectives.

There are a number of approaches to regulation and supervision, each of which is detailed in the sections below. Regulators typically adopt one of the approaches, although some elements of other approaches may also be used.

2.3.1 The Risk-Based Approach

The risk-based approach to regulations means that countries' competent authorities and financial institutions are expected to identify, assess and understand the risks to which they are exposed and take the appropriate measures commensurate to those risks in order to mitigate them effectively. Regulators assess individual firms concerning the risk they present to the regulator's objectives, which assists them in assessing the level of supervisory attention required for each firm.

When assessing risk, it is necessary for countries, competent authorities, and financial institutions to analyse and seek to understand how the risks they identify affect them. Risk assessments are designed to tie in the regulator's activity with meeting its objectives by:

- identifying the main risks to the regulator's objectives as they arise
- measuring how important they are (impact, probability)
- mitigating them if their size justifies it (the proportionate, cost-benefit approach), and
- monitoring and reporting on the progress of the process in terms of risk management.

The risk assessment provides the basis for the risk-sensitive application of measures and, therefore, compliance with the regulations.

The risk-based approach is not a 'zero failure' approach; there may be occasions where an institution has taken all reasonable measures to identify and mitigate risks, but is still subject to losses. It also does not exempt countries, competent authorities and financial institutions from mitigating risks which are assessed as low.

The impact of a risk posed by an individual firm is assessed using a range of factors established by reference to the regulator's objectives. They may include:

- the degree to which the risks related to the firm would **damage confidence and trust in the markets** if they were to materialise
- the possibility of the risks if they materialise leading to **market or system failure**
- the extent to which the firm may pose risks to achieving the objective of **promoting public understanding**
- the extent to which **consumers may be adversely affected** by the firm's actions or failures
- the incidence or materiality of any **financial crime** that may be perpetrated through, or by, the firm, or
- the degree to which the firm may pose a risk to the country's **financial stability**.

The probability of a firm posing a risk to the regulator's objectives depends on a number of discrete sources of risk (sometimes referred to as 'risk to objectives (RTO) groups'), and on the firm's internal controls for negotiating those risks.

The RTO groups may include elements such as:

- the firm's strategy
- the firm's **business risk** (those risks that are inherent in the business, such as credit, market and operational risk)
- the financial soundness of the firm
- the nature of the firm's customers and the products and services it offers
- the internal systems and controls and the compliance culture of the firm, or
- the organisation of the firm and the role played by its governing body, management and staff in mitigating risk.

The regulator may also compare risks across different sectors, using its cross-sectoral experience to produce benchmark assessments and guidance, so that an appropriate baseline can be established. This may also involve detailed communication between the regulator and firms in terms of feedback on their risk assessment – focusing on the key risks identified, and the response the regulator expects from firms. This develops a greater capacity for the regulator to gain a better understanding of emerging trends and risks, through improved sector intelligence.

2.3.2 The Rules-Based Approach

Rules-based regulation provides a set of detailed rules that govern firms' behaviour. Such rules enable firms to 'tick the box' to guarantee compliance with laws and regulations. In practice, very few regulatory regimes apply pure rules-based systems, with most involving a mixture of rules and principles. Even the US, considered by many in the past to have been solely rules-based, has laws and regulations which use a combination of rules and principles.

Following the global financial crisis, many international organisations have made improvements to supervisory approaches which involve more intensive and intrusive styles of supervision and a move to a stronger outcomes-focused model. This shift requires a significant enhanced analysis and risk identification capacity which will focus on business model risk and interact with macroprudential analysis. However, increasing the focus on outcome testing over matters such as ensuring firms have the appropriate systems and controls, also requires capacity and structures for early, and more direct, regulatory intervention.

This may require the development of new rules on, for example, the suitability of products and services for consumers. For example, requiring firms to complete appropriate reviews and testing. It may also give greater powers for regulators to affect a more intensive and intrusive style of supervision which may also include product intervention at an early stage. The latter means that regulators will have to devote more resources to analysis and risk assessments and be prepared to take decisions where they believe the (potential) risks require them to act to protect consumers and markets.

The risks may not have materialised at this stage and one of the possible outcomes could be to reduce consumer choice and innovation, although governments may well regard this as an acceptable trade-off for a safer financial environment.

2.3.3 Principles-Based Approach

The principles-based approach applies a broad set of principles of conduct which are then implemented by regulated institutions in the way they see fits best with their organisation. Supervision is based on how the principles are implemented and the outcomes achieved. This is contrary to the rules-based approach to supervision, in which firms are required to follow a precise set of rules. This approach provides firms with the flexibility to meet regulatory requirements in a way that best fits their business models. The disadvantage is that the spirit of the rules is open to interpretation.

2.3.4 Thematic Approach

A thematic approach allows the regulator to look at specific issues associated with themes using a specialised team and helps it focus its resources and information efficiently. Regulators have a range of tools they can use to aid their supervision of regulated firms. Typically, these are:

- **diagnostic tools** – designed to identify, assess and measure risk
- **monitoring tools** – to track the development of identified risk, wherever it arises
- **preventative tools** – to limit or reduce identified risks and so prevent them from crystallising or increasing, and
- **remedial tools** – to respond to risks when they have crystallised.

For example, according to its website, the Dubai Financial Services Authority (DFSA):

'...has a range of supervisory tools available to diagnose and monitor risks, and to prevent them from occurring. It chooses appropriate tools for each situation, with a view to cost-effective regulation for the DFSA and the firm, and to preserve and enhance the marketplace. Increasingly, the DFSA uses thematic reviews as a key tool to assess risk in the marketplace.'

The UK's financial regulators also use thematic supervision. Analysis of a particular product, market, or practice can enable the regulator to identify a wide-scale issue that requires attention. This thematic effort is performed separately from the regulator's ongoing processes to monitor firms, though the two approaches are mutually supportive. The regulator's discussions with individual firms enable behaviours to be monitored (which may identify a new issue for thematic attention), while also enabling the regulator to observe changes made by individual firms in the light of previous thematic reviews.

By considering the activity taken by different firms across a particular sector in a consistent way, the regulators can identify good and bad practice. The results are then usually published to help firms improve their practices and reduce the risk of bad practice. The UK's FCA and [Prudential Regulation Authority \(PRA\)](#) expect firms to take note of such published material, as implementing the good practices identified is a way for firms to demonstrate a proactive approach to compliance and reducing risks.

2.3.5 Relationship-Based Supervision

Due to the number of firms for which a regulator may be responsible, the regulator must consider how to align its resources with the risks each firm may pose to market stability. Where its risk assessments indicate that a firm may pose a risk to the regulator's objectives, the regulator may assign particular staff members to have an ongoing direct relationship with the firm. Such an approach is normally supported by periodic visits and meetings with the management of the firm, as well as ongoing desk-based monitoring of the firm's financial and information returns.

In a small number of cases, the intensity of relational oversight may be increased. This can, for example, occur if a significant concern has been identified by the firm or the regulator. If the firm is a large bank, this represents a substantial risk to the overall market.

Such intensive oversight is reflected in the regulator:

- paying close attention to the firm's activities
- increasing the frequency of meetings, and
- requesting additional types of data/reporting.

This approach is sometimes referred to as 'close and continuous supervision' (although each regulator will determine its own label).

This more intensive supervision is characterised by frequent dialogue with the firm on the full range of supervisory issues, through ad hoc meetings, regular telephone conversations and emails. The regulator's activity may include:

- reviewing strategic and business developments through discussions with the firm
- reviewing updates from the firm regarding resolution of specific known issues
- attending results presentations
- monitoring the market in which it operates
- assessing the ongoing validity of the regulator's risk assessment
- monitoring financial data, supervisory returns and management information
- reacting to specific requests from the firm, such as around capital requirements
- undertaking the formal review process which sets the capital requirements of the firm on the basis of the risks identified by the firm, and
- selecting the firm to be included in thematic reviews where they relate to a specific area of its business.

2.4 IOSCO's Principles Relating to the Regulator



1.2.8 Know IOSCO's Principles 1 to 8 relating to the regulator

IOSCO has produced 38 principles of securities regulation; 15 apply to regulators, including those relating to self-regulation and principles for enforcement and cooperation in regulation. As noted in section 2.2.3, IOSCO has introduced 38 principles subdivided into ten categories.

The first category relates to Principles Relating to the Regulator and contains principles 1–8, which are as follows:

Principles Relating to the Regulator

1. The responsibilities of the regulator should be clear and objectively stated.
2. The regulator should be operationally independent and accountable in the exercise of its functions and powers.
3. The regulator should have adequate powers, proper resources and the capacity to perform its functions and exercise its powers.
4. The regulator should adopt clear and consistent regulatory processes.
5. The staff of the regulator should observe the highest professional standards including appropriate standards of confidentiality.
6. The regulator should have, or contribute to, a process to monitor, mitigate and manage systemic risk appropriate to its mandate.
7. The regulator should have, or contribute to, a process to review the perimeter of regulation regularly.
8. The regulator should seek to ensure that conflicts of interest and misalignment of incentives are avoided, eliminated, disclosed or otherwise managed.

2.5 Regulator Enforcement Powers



1.2.9 Know regulators' enforcement powers

IOSCO's Principles for the Enforcement of Securities Regulations (Category C, principles 10–12) (see section 2.2.3) provide an overview of the types of enforcement powers that financial services regulators may seek to use. Each of these is detailed further in the sections below.

2.5.1 Inspection and Compliance Programmes

Supervision of market intermediaries conducted through inspection and surveillance helps to ensure the maintenance of high standards and the protection of investors. These preventative programmes are a necessary complement to investigation and enforcement programmes. The regulator has

the power to require the provision of information or to carry out inspections of business operations whenever it believes it is necessary to ensure compliance with relevant standards.

The suspicion of a breach of law should not be a necessary prerequisite to use inspection powers in respect of authorised or licensed persons.

Inspections may be carried out by the regulator itself or another competent authority. Alternatively, the regulator might consider delegating such authority to SROs or using third parties, properly supervised, to carry out some of this inspection work on its behalf. These third parties should also be subject to disclosure and confidentiality requirements. Such inspections must be carried out with adequate instruments and techniques, and these may vary between jurisdictions. In some areas such as the scrutiny of trading on an exchange, the use of technology will be necessary for effective regulation.

In other areas, including the inspection of broker conduct, consideration needs to be given to the balance between on-site inspection and interview and the requirement to provide information from time to time which can be reviewed off-site. Inspection visits may be rotational or driven by risk assessment or complaint. In making decisions on the efficient use of resources, the regulator must consider both the need for wide market coverage and the importance of adequate inspection in areas of high risk to investors or which threaten systemic stability.

2.5.2 Comprehensive Enforcement Powers

The complex character of securities transactions and the sophistication of fraudulent schemes require strong and rigorous enforcement of securities laws. Investors in the securities markets are particularly vulnerable to misconduct by intermediaries and others.

The regulator or other competent government authority should, therefore, be provided with comprehensive investigatory and enforcement powers including:

- regulatory and investigative powers to obtain data, information, documents, statements and records from persons involved in the relevant conduct or who may have information relevant to the inquiry
- power to seek orders and/or to take other action to ensure compliance with these regulatory, administrative and investigation powers

- power to impose administrative sanctions and/or to seek orders from courts or tribunals
- power to initiate or to refer matters for criminal prosecution
- power to order the suspension of trading in securities or to take other appropriate action, and
- where enforcement action is able to be taken, the power to enter into enforceable settlements and to accept binding undertakings.

These enforcement powers should, however, not compromise private rights of action.

Private persons should be able to seek their own remedies (including, for example, for compensation or specific performance of an obligation). The responsibility for all aspects of enforcement of the securities law are not necessarily given to a single body. Effective models require responsibilities to be shared between several government or quasi-government agencies or where responsibility is shared with SROs.

The sharing of responsibility and the need for close cooperation may be particularly important in ensuring that only those who have the necessary authorisation are active participants on the markets; unlicensed persons should be prosecuted.

2.5.3 International Enforcement

Securities markets facilitate international transactions, and so matters of conduct may involve multiple jurisdictions.

Legislation and the enforcement powers of the regulator should be sufficient to ensure that it can be effective in cases of cross-border misconduct.

This means the regulator should strive to ensure that it or another authority in its jurisdiction:

- has the necessary authority to obtain information, including statements and documents, which may be relevant to investigating and prosecuting potential violations of laws and regulations relating to securities transactions, and
- that such information can be shared directly with other regulators or indirectly through authorities in their jurisdictions for use in investigations and prosecutions.

2.6 Regulated Activities and Products



1.2.10 Understand what types of activities and investment products are generally required to be regulated

In the UK, for example, regulated activities can be split into four broad categories:

- banking activities
- investment activities
- insurance activities, and
- home finance activities.

For each of the activities the firm intends to perform, it has to obtain authorisation and identify the types of specified investments it plans to offer. Also, for each proposed activity, the firm must identify the types of specified investments to which its regulated services will relate. A UK-regulated firm may, for instance, obtain permission to deal in investments as agent, in respect of **futures** and **options**, while being authorised to manage investments that are units in a collective investment scheme (CIS) or shares. Although the terminology used and the regulated activities mentioned in the remainder of this section are derived from UK regulations, they are closely aligned with other jurisdictions.

2.6.1 Banking Activities

- Accepting deposits.
- Issuing e-money.

2.6.2 Investment Activities

- Dealing in investments (as principal or agent).
- Arranging deals in investments.
- Operating an MTF or OTF.
- Managing investments.
- Safeguarding and administering investments.
- Sending **dematerialised** instructions.

- Establishing collective investment schemes (CISs).
- Establishing stakeholder pension schemes.
- Providing basic advice on stakeholder products.
- Advising on investments.
- Operating an electronic system in relation to lending.
- Managing an Undertakings for Collective Investments in Transferable Securities (UCITS).
- Acting as **trustee** or depositary of a UCITS.
- Managing an alternative investment fund (AIF).
- Acting as trustee or depositary of an AIF.

2.6.3 Insurance Activities

- Effecting or carrying out contracts of insurance as principal.
- Assisting in the administration and performance of a contract of insurance.
- Lloyd's market activities.

2.6.4 Home Finance Activities

- Arranging home finance activities.
- Advising on home finance activities.
- Entering into a home finance activity.
- Administering a home finance activity.
- Agreeing to do most of the above activities.

2.6.5 Specified Investments

A firm must identify the range of investment types applicable to each activity it will perform. The profiles of individual firms can, therefore, be quite dynamic in terms of the combination of activities and products. For small firms, the regulators may have standard profiles which act as guides for applicants for authorisation. Specified investments are shown in the following list:

- Deposits.
- Electronic money.
- Shares.

- Instruments creating or acknowledging indebtedness.
- Government and public securities.
- Certificates representing certain securities.
- Instruments giving entitlement to investments.
- Units in a CIS.
- Futures.
- Options.
- Lloyd's syndicate capacity and syndicate membership.
- Contracts for differences (CFDs).
- Rights under a contract of insurance.
- Rights under a personal pension scheme.
- Rights under a stakeholder pension scheme.
- Rights under regulated mortgage contracts.
- Rights under funeral plan contracts.
- Rights under a home purchase plan.
- Rights under a home reversion plan.
- Rights to or interests in anything that is a specified investment listed, excluding 'rights under regulated mortgage contracts', 'rights under regulated home reversion plans' and 'rights under regulated home purchase plans'.
- Cryptoassets.

2.7 Regulatory Requirements on Firms



1.2.11 Understand the requirements regulation places on firms: minimum entry standards; initial and ongoing capital and other prudential requirements; requirement to establish an internal compliance function; conduct of business

The IOSCO principles 29-32 are related to Market Intermediaries, and cover, among others, entry standards and capital requirements. These provisions include the typical requirements firms are required to meet in relation to authorisation, supervision, capital adequacy and the conduct of business rules and other prudential requirements.

2.7.1 Authorisation (including Licensing and Registration) and Supervision

The regulator will set minimum standards for market participants and provide consistency of treatment for all similar firms. It should also reduce the risk to investors of loss caused by negligent or illegal behaviour or inadequate capital.

The authorisation process typically requires a comprehensive assessment of the applicant and all those who are in a position to control or materially influence the applicant. The regulatory authority has the power to reject applications that do not meet the standards set.

The regulator also has the power to withdraw or suspend the licence or otherwise sanction the licensee, whenever the entry criteria are not fulfilled. Changes of control or material influence should be made known to the regulator or another competent authority in order to ensure that its assessment of the firm remains valid. The regulator should be empowered to withdraw a licence or authorisation where a change in control results in a failure to meet relevant requirements.

The following matters should be the subject of consideration:

- Regulation should set conditions of entry that make the basis of participation clear. The entry conditions should be consistently applied and do not need to be determined by the regulator. For example, the entry conditions could be defined by the SRO, in which case, the process should be subject to appropriate oversight by the regulator.
- Regulation should determine whether participation in the market by a firm should be based upon a demonstration of appropriate knowledge, resources, skills and ethical attitude (including a consideration of past conduct); this is sometimes referred to as the 'fit and proper' test.
- The regulator should have the authority to refuse authorisation of a firm if these requirements have not been met.
- There should be an initial capital requirement for securities firms as a condition of entry into the market. This ensures that the owners of the business have a direct financial stake in the business. The capital requirement should be maintained and should be the subject of periodic reporting to the regulator or competent SRO. The ongoing capital requirement should be directly related to the nature and amount of business undertaken by a firm. The financial position of the firm should be regularly audited by independent auditors.

To ensure that continued authorisation remains appropriate, the periodic updating of relevant information should be required as well as the reporting of material changes in circumstances affecting the conditions of authorisation.

To enable investors to better protect their own interests, the regulator should ensure that the public has access to relevant information concerning the authorised firm, such as the category of **permissions** held, the scope of its authorised activities, the identity of senior management and those authorised to act in the name of the firm.

2.7.2 Capital Adequacy

The protection of investors and stability of financial systems are increased through adequate supervision of ongoing capital standards.

Capital adequacy standards foster confidence in the financial markets and are designed to allow a firm to absorb some losses, particularly in the event of large adverse market moves. It helps achieve an environment in which a firm could wind down its business over a relatively short period without loss to its customers or the customers of other firms, and without disrupting the orderly functioning of the financial markets. Capital standards are designed to provide supervisory authorities with time to intervene to accomplish the objective of orderly wind down.

Regulators require a firm to reserve a certain level of capital as part of the authorisation process, relative to the type of activity it will be permitted to perform. Once authorised, a firm should ensure that it maintains adequate financial resources to meet its business commitments and to withstand the risks to which its business is subject. Risk may result from the activities of unauthorised and off-balance sheet affiliates and regulation should consider the need for information about the activities of these affiliates.

A capital adequacy test will be used to address the risks faced by securities firms judged by reference to the nature and amount of business undertaken by the firm.

2.7.3 The Conduct of Business Rules and Other Prudential Requirements

Firms should conduct themselves in a way that protects the interests of their clients and helps to preserve the integrity of the market. The management of a

firm bears primary responsibility for ensuring the maintenance of appropriate standards of conduct and adherence to proper procedures by the whole firm. This includes the proper management of the risks associated with the business of the firm. Regulation is not expected to remove risk from the marketplace, but it should ensure that there is proper management of that risk. Periodic evaluation of risk management processes within a regulated entity is appropriate. SROs and third parties, such as external auditors, may be used to assist in this process.

Most supervisors and SROs have published guidance and rules related to the conduct of business. These rules are included, for example, within the FCA Handbook (Conduct of Business), the CISI's Code of Conduct, and the Chartered Financial Analyst (CFA) Institute's Code of Ethics and Standards of Professional Conduct. These rules typically address issues including acting honestly, fairly and professionally. They also apply to transparency, client communication (via any medium, and regarding any type of information provided) and assessing the suitability of the products offered given client needs. Instances of operational breach can occur despite the existence of internal procedures designed to prevent relevant misconduct or negligence. It is not practical for the regulator to oversee adherence to those internal procedures on a day-to-day basis. Instead, this is the responsibility of the senior management of the firm. Senior management must ensure that they:

- are able to discharge that responsibility
- understand the nature of the firm's business, its internal control procedures and its policies on the assumption of risk
- clearly understand the extent of their own authority and responsibilities, and
- have access to all relevant information about the business on a timely basis and have available to them all necessary advice on that business and on their own responsibilities. That information must also be available to the regulator upon request.

2.7.4 Internal Compliance Function

It is important that a firm maintains an independent function to ensure that the firm's activity is aligned with regulatory requirements. While the operational areas will have controls in place to ensure processes are performed as intended, this internal compliance function will also ensure that those processes remain aligned with the rules.

The internal compliance function should be a permanent and effective part of the firm's governance structures and proportionate to the scale and complexity of the firm's business. Guidance from regulators tends to reflect the following responsibilities:

1. To monitor and, on a regular basis, assess the adequacy and effectiveness of the measures and procedures put in place, and the actions taken to address any deficiencies in the firm's compliance with its obligations.
2. To advise and assist the relevant persons responsible for carrying out regulated activities to comply with the firm's obligations under the regulatory system.

In order to enable the compliance function to discharge its responsibilities properly and independently, a firm must ensure that the following conditions are satisfied:

- The compliance function must have the necessary authority, resources, expertise and access to all relevant information.
- A compliance officer is appointed and must be responsible for the compliance function and for any reporting as to compliance required by the regulator.
- The relevant persons involved in the compliance functions must not be involved in the performance of the services or activities they monitor.
- The method of determining the remuneration of the relevant persons involved in the compliance function must not compromise their objectivity and must not be likely to do so.

Where the firm's size or level of activity is at a scale that would not warrant the appointment of an independent compliance officer, the firm would be expected to allocate to a director or senior manager the function of:

- a. having responsibility for oversight of the firm's compliance, and
- b. reporting to the governing body in respect of that responsibility.

In some jurisdictions, the tasks performed by the compliance function may be delegated to appropriate skilled individuals, but generally, the regulatory responsibility will remain with the senior management of the firm and the person allocated the responsibility for oversight of compliance.

2.8 Regulation of Cross-Border Business



- 1.2.12 Understand how regulators facilitate and regulate cross-border business: specific legislation; memoranda of understanding between individual regulators; regulatory colleges; recognition of third countries
 - 1.2.13 Understand what regulations apply to a firm with international branches and subsidiaries: contractual agreements between regulators; home/hosts
 - 1.2.14 Understand the challenge of conducting business whilst meeting the regulatory expectations and approach of multiple regulatory bodies: international; domestic
-

Earlier in this chapter, we looked at the extraterritorial reach of some major pieces of legislation. In addition, we considered the IOSCO principles around regulatory cooperation and international enforcement that are aimed at the need for national regulators to share information and assist one another. This reflects the threats to domestic financial markets and financial stability resulting from the behaviour and actions of firms involved in international financial activities and the globalisation of markets.

For example, cases of fraud and ML that involve dealings in securities or other financial products may require close cooperation between two or more domestic regulators, including law enforcement, regulatory and judicial authorities.

Other examples where cross-border cooperation may be required is where firms may have shares listed in more than one jurisdiction, where investors invest in foreign markets, either directly or through managed funds, where financial products are traded on various markets in several countries or, as in the case of derivatives, are based on an underlying product or indices traded, produced or derived on foreign markets. Fraud, market manipulation, insider trading, and other illegal conduct that crosses jurisdictional boundaries can and does occur more frequently in a world aided by modern telecommunications.

Cooperation mechanisms are, therefore, important at an international level to facilitate the detection and deterrence of cross-border misconduct and to assist in the discharge of authorisation and supervisory responsibilities.

A memorandum of understanding (MoU) is one such mechanism that may be established between two regulatory authorities. The two supervisors write the MoU to set out how they would each act where a given need for oversight straddles their respective areas of responsibility. An MoU between regulators might, therefore, include:

- defining which regulator would take the lead role in investigating certain types of issues
- the manner of support that each regulator might provide to the other, and
- the way in which data exchanged between the regulators would be protected, and how that data might be used.

In this way, the framework for cross-border regulation can be communicated to the market, and expectations set.

The FSB has identified three key standards in the financial regulatory and supervisory area. They are:

- IOSCO's Objectives and Principles of Securities Regulation
- the BCBS Core Principles for Effective Banking Supervision, and
- the International Association of Insurance Supervisors (IAIS) Insurance Core Principles.

The FSB, in consultation with the BCBS, IAIS and IOSCO identified, within each of these standards, principles concerning international cooperation and information exchange.

Countries not part of the EU are, for the purpose of EU regulations, considered to be third countries. Third countries could be considered as equivalent, for the purpose of regulation, if their regulatory environment is deemed to be equivalent with the regulations in the EU. In addition, third country CCPs may be recognised as equivalent, provided they meet the requirements.

2.8.1 Internal Compliance Function

The Basel Committee has provided clarity and consistency in how different regulators will relate to a firm that is active in multiple jurisdictions. The approach distinguishes between the home supervisor (country of incorporation) and the host supervisor (country or countries in which the firm operates).

In general, matters relating to the firm's structure and organisation (such as regulatory capital and authorisation processes) are a matter for the home supervisor. Matters relating to customer interaction tend to be addressed by the host supervisor(s).

In the EU, this approach is seen as beneficial for consumers, who should be similarly protected regardless of the EU domicile of the firm servicing them. For firms, the combination of home and host regulations requires additional effort, and any misalignment between the rules of the different jurisdictions can add complexity to the ability to effectively perform cross-border business.

2.8.2 Supervisory Colleges

Rather than the simplistic approach of home and **host state** regulation, a supervisory college brings together all national regulators relevant to the operations of a given banking group to agree a model of supervision that will satisfy the needs and objectives of each regulator. The supervisory colleges are of particular importance given the size and reach of financial institutions' cross-border activity within the EU.

The college is the means by which the regulators coordinate their efforts, ensuring that all necessary aspects of oversight are achieved. Their work will consider aspects such as risk management across the banking group (including its **liquidity risk**), and ensuring that the group's recovery plans are sufficiently robust in respect of the various markets being serviced.

The aim of the supervisory college is to provide regulators with a more flexible model for cross-border supervision, enabling the approach to be tailored according to the needs of each banking group.

2.8.3 Implications for Firms

The practical application of this for firms is that expanding an existing business or service into multiple jurisdictions introduces a mix of regulatory obligations. While these regulatory mechanisms are intended to standardise the regulatory requirements, even within Europe a point of full harmonisation has not yet been achieved.

While a firm should, therefore, have a full understanding of how to apply the rules of its domestic regulator, expanding into additional countries requires the firm to understand what cross-border supervision approach will be applied

– and then understand which rules must be followed in respect of the **home state** and host state. The firm needs to determine whether it requires additional authorisation in either jurisdiction, in order to perform its proposed expanded business. Where an EU firm is simply expanding to perform its existing authorised business in other EU member states, it will usually be possible to avoid full authorisation through use of a ‘passport’. If the business expansion sees the firm entering non-EU jurisdictions, a formal authorisation process might be required. This form of cross-border authorisation is also in place in the countries being part of the Gulf Cooperation Council (GCC).

When a firm first begins cross-border activity, it is vital they gain a detailed understanding of the new jurisdiction’s regulations and applicable legislation. The firm can review the regulator’s website for information or make contact with a relevant trade association in the new jurisdiction in order to better understand the approach taken in that country. It is also common to obtain external legal advice, or to recruit personnel with experience of that jurisdiction.

The firm should then assess how its relationship with its domestic regulator will change. For example, which of the additional business activities will be included in domestic regulatory returns and capital adequacy calculations. At the same time, the firm needs to understand the implications of any MoU in place between the relevant regulators. A banking group operating in multiple jurisdictions should confirm whether a supervisory college will be assembled and understand how it should best relate with the members of that college.

There may be a need to submit certain filings to the regulators before commencing the cross-border business, and the firm might need to update its policies and procedures to ensure that the needs of all relevant regulations are satisfied. Its structures for identifying regulatory change need to have an expanded scope to ensure that regulatory change in the expanded list of jurisdictions is identified and assessed for impact.



End of Chapter Questions

1. State two of the objectives of regulation.

The objectives and benefits of regulation can be summarised as:

- increase in confidence and trust in financial markets, systems and products
- establish an environment to encourage economic development and wealth creation
- reduce the risk of market and system failures, including their economic consequences
- enhance consumer protection, giving them the reassurance they need to save and invest, and
- reduce financial crime by ensuring financial systems cannot easily be exploited

Answer reference: Section 1.1

2. State the main differences between rules-based and principles-based approaches to regulation.

- **Rules-based** regulations are mainly prescriptive procedures including very detailed rules. These rules specify exactly what individuals and firms must do to ensure they comply. A rules-based approach requires strict adherence to precise rules with little allowance for interpretation. It is typically inflexible and may result in a tick-box exercise.
- **Principles-based** regulations focus on the spirit of the rules and, therefore, the types of behaviour and outcomes. Unlike the rules-based approach, it is not about blindly following the rules. A principles-based approach acts as a fundamental source of guidance on how firms and individuals are expected to act. How individuals and firms ensure they comply with the regulations, and to what extent the principles are met, is their own responsibility.

Answer reference: Section 1.3

3. What is the mission of the Islamic Financial Services Board (IFSB)?

The IFSB is an international standard-setting organisation with a mission to promote and enhance the soundness and stability of the Islamic financial sector by issuing global prudential standards and guiding principles for the industry, broadly defined to include banking, capital markets and insurance sectors. The IFSB standards are mainly based on the identification, management and disclosure of risks relevant to Islamic products and operations. Full members of the IFSB are typically **central banks** in countries where Islamic financial institutions are incorporated. These countries are invited to apply the (optional) IFSB standards in order to provide a comparable regulated environment for the Islamic financial sector. The standards are mandatory in some countries, such as Bahrain and Sudan, and are used as guidelines in others.

Answer reference: Section 1.4.2

4. What are the penalties for breach of the General Data Protection Regulation (GDPR)?

Breaches of the GDPR are subject to a tiered structure and subject to a maximum of 4% of the annual global turnover of the previous financial year or €20 million (or equivalent), whichever is greater.

Answer reference: Section 1.5.1

5. List the data subject rights.

The data subject rights are:

- Any data breach that is likely to *'result in a risk for the rights and freedoms of individuals'* must be reported within 72 hours of the data processor first having become aware of the breach. Customers and controllers must be notified *'without undue delay'* after first becoming aware of a data breach.
- Data subjects have the right to obtain from the data controller confirmation from the data controller as to whether or not their personal data is being processed, where, and for what purpose. Furthermore, the controller must provide a copy of the personal data, free of charge, in an electronic format on request.
- Data subjects have the right to be forgotten (also known as data erasure). On request, the data subject to have the data controller must erase their personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in Article 17, include the data no longer being relevant to the original purpose for

processing, or a data subject withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to *'the public interest in the availability of the data'* when considering such requests.

- Data subjects have the right to receive the personal data concerning them, which they have previously provided in a *'commonly used and machine-readable format'* and have the right to transmit that data to another controller.
- Privacy by design has become part of the GDPR legal requirement. Controllers must implement appropriate technical and organisational measures to meet the GDPR requirements. Only the data that is absolutely necessary for the completion of their duties should be held and processed.

Answer reference: Section 1.5.1

6. State the key policy goals of MiFID III.

- Extending the range of investment services for which a firm can obtain an EU 'passport' (ie, obtaining authorisation in one EU state – the home state – enabling a firm to provide investment services in another EU member state – the host state – without requiring any further local authorisations), and
- Removing a major hurdle to cross-border business by no longer applying 'host state' rules to incoming passported firms.
- MiFID III and MiFIR 2 extend the application to Alternative Investment Fund Managers and management companies, and extend the scope of derivatives subject to the clearing obligation.

Answer reference: Section 1.5.2

7. List how the Market Abuse Regulation (MAR) applies to financial instruments to increase market integrity and investor protection.

EU Regulation with the aim to increase market integrity and investor protection. The regulation establishes a common regulatory framework on insider dealing, the unlawful disclosure of inside information, market manipulation as well as measures to prevent market abuse. Applies to the following:

- a. Financial instruments admitted to trading on a regulated market or for which a request for admission to trading on a regulated market has been made.
- b. Financial instruments traded on a Multilateral Trading Facility (MTF), admitted to trading on an MTF, or for which a request for admission to trading on an MTF has been made.
- c. Financial instruments traded on an organised trading facility (OTF).
- d. Financial instruments not covered by points (a), (b) or (c), the price or value of which depends on or has an effect on the price or value of a financial instrument referred to in those points, including, but not limited to, credit default swaps and contracts for difference.

Answer reference: Section 1.5.2

8. What does Section 404 of the Sarbanes-Oxley (SOX) Act require publicly registered US companies to do?

Section 404 lays out the requirement for the management of a US public company to report annually on the operational effectiveness of the company's internal controls over financial reporting. Additionally, the company's auditors must attest to

and report on the management's assertion over the effectiveness of internal financial controls.

Answer reference: Section 1.5.2

9. What is the definition of payment services?

'Services enabling cash to be deposited in or withdrawn from, for example, a bank account, as well as all the operations required to operate the account. This can include transfers of funds, direct debits, credit transfers and card payments. Paper transactions are not covered by the directive.'

Answer reference: Section 1.5.2

10. What is the punishment for defrauding securities investors?

Up to 25 years in prison.

Answer reference: Section 1.5.2

11. How is AMLD best described?

A series of EU directives providing a risk-based approach that requires EU-wide risk assessments in combination with national and institutional risk assessments.

Answer reference: Section 1.5.3

12. What are the four forms of disciplinary action that exchange operators can take against any person registered by the exchange?

Disciplinary action and enforcement penalties are usually determined by a disciplinary committee and may take the form of:

- A reprimand.
- A fine (usually within limits laid down/agreed by the exchange).
- Suspension of the member.
- Expulsion of the member or trading representative.

Answer reference: Section 1.6.1

13. What is counterparty risk?

Counterparty risk is the risk that a counterparty may not honour its obligations under the contract when they become due.

Answer reference: Section 1.7

14. How do regulators approach Fintech?

Regulations do not focus on the technical details but on implementation. The regulatory sandbox allows the regulator to review the implementation and assess whether new regulations are required or whether existing rules contain sufficient flexibility for firms to use the new technology. Regulators are catching up with these developments and have been introducing new regulations such as the EU rules on cryptomarkets.

Answer reference: Section 1.8

15. What are the possible applications of artificial intelligence (AI)?

Artificial intelligence (AI) can be applied in financial services in the following ways:

- Enhance accuracy of credit scoring using algorithms and large volumes of data from a range of different sources. Due to the absence of bias and judgement, the decision-making process is more rational.
- Combatting and preventing fraud and ML by identifying irregular patterns in customer behaviour and suspicious transactions.
- Automated trading platforms making recommendations and predictions based on algorithms that assess large volumes of data. The use of AI reallocates time to customer interaction rather than data analysis and circumvents bias and judgement.
- Chatbots to interact with customers applying a combination of AI and big data, addressing the simple, rules-based queries with a transfer to a customer representative for complex queries.

Answer reference: Section 1.8.3

16. List the expectations of regulators in relation to Fintech and corporate governance.

Regulators expect firms to have appropriate corporate governance in place to manage the deployment of new systems, which includes the following:

- Sufficient involvement at board level.
- Engagement of risk and compliance functions.
- Training and development of staff in general, and board members, risk and compliance functions in particular.

Answer reference: Section 1.8.4

17. Which types of regulators typically cover insurance markets and investment services at a national level?

Self-regulatory organisations (SROs) typically cover insurance markets and investment services, such as financial advice, investment management and mortgages. Members are usually national and, accordingly, the focus of the SRO is essentially national in nature.

Answer reference: Section 2.1

18. What are the three objectives of securities regulation that the International Organization of Securities Commissions (IOSCO) aims to achieve?

The three objectives of securities regulation are:

- the protection of investors
- ensuring that markets are fair, efficient and transparent
- the reduction of systemic risk.

Answer reference: Section 2.2.3

19. Describe the main responsibility of the US Securities and Exchange Commission (SEC).

The SEC's main responsibility is to enforce federal securities laws, propose securities rules, and to regulate the securities industry. The mission of the SEC is to protect investors; to maintain fair, orderly, and efficient markets; and to facilitate capital formation. They strive to promote a market environment worthy of the public's trust.

Answer reference: Section 2.2.5

20. What are diagnostic tools used in thematic-based supervision?

- Diagnostic tools– designed to identify, assess and measure risk.
- Monitoring tools – to track the development of identified risk, wherever it arises.
- Preventative tools – to limit or reduce identified risks and so prevent them crystallising or increasing.
- Remedial tools – to respond to risks when they have crystallised.

Answer reference: Section 2.3.4

21. State IOSCO's eight Principles Relating to the Regulator.

The 8 principles relating to the regulator are:

1. The responsibilities of the regulator should be clear and objectively stated.
2. The regulator should be operationally independent and accountable in the exercise of its functions and powers.
3. The regulator should have adequate powers, proper resources and the capacity to perform its functions and exercise its powers.
4. The regulator should adopt clear and consistent regulatory processes.
5. The staff of the regulator should observe the highest professional standards including appropriate standards of confidentiality.
6. The regulator should have or contribute to a process to monitor, mitigate and manage systemic risk, appropriate to its mandate.
7. The regulator should have or contribute to a process to review the perimeter of regulation regularly.

8. The regulator should seek to ensure that conflicts of interest and misalignment of incentives are avoided, eliminated, disclosed or otherwise managed.

Answer reference: Section 2.4

22. What four categories can UK-regulated activities be split into?

In the UK, regulated activities can be split into four broad categories:

- banking activities
- investment activities
- insurance activities, and
- home finance activities.

Answer reference: Section 2.6

23. Why does regulation require that firms have adequate capital standards?

Capital adequacy standards foster confidence in the financial markets and are designed to allow a firm to absorb some losses, particularly in the event of large adverse market moves, and to achieve an environment in which a securities firm could wind down its business over a relatively short period without loss to its customers or the customers of other firms and without disrupting the orderly functioning of the financial markets.

Answer reference: Section 2.7.2

24. Explain the difference between home and host state regulations.

In general, matters relating to the firm's structure and organisation (such as regulatory capital and authorisation

processes) are a matter for the home supervisor. Matters relating to customer interaction tend to be addressed by the host supervisor(s).

In the EU, this approach is seen as beneficial for consumers, who should be similarly protected regardless of the EU domicile of the firm servicing them. For firms, the combination of home and host regulations requires additional effort, and any misalignment between the rules of the different jurisdictions can add complexity to the ability to effectively perform cross-border business

Answer reference: Section 2.8.1



Chapter Two

The Compliance Function

Section 1

International Best Practice

Section 2

Regulatory Compliance and the Risk of Non-Compliance

Section 3

Managing Regulatory Relationships

This syllabus area will provide
approximately 24 of the 100
examinations questions



1. International Best Practice

1.1 Systems and Controls



- 2.1.1 Understand the fundamental systems and controls a firm should implement in order to conduct its business in line with international regulatory standards

1.1.1 Organising Appropriate Systems and Controls to Ensure Compliance

Compliance is most effective in a corporate culture that emphasises standards of honesty and integrity and in which the board of directors and the senior management lead by example. In other words, compliance starts at the top. However, it does not stop there, and it is vital that compliance is a concern of everyone in an organisation and should be viewed as an integral part of the firm's everyday activities. This also means observing the spirit, as well as the letter, of the law.

A firm needs to establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm (covering its managers, employees, and representatives) with its obligations under the regulatory system in which it operates, and for countering the risk that the firm might be used to further financial crime (including money laundering (ML) and terrorist financing (TF)). **Compliance risk**, generally, is seen as the risk of legal or regulatory sanctions, material financial loss, or loss to reputation as a result of failure to comply with laws, regulations, rules, related self-regulatory organisation (SRO) standards, and codes of conduct applicable to the firm's business.

Compliance is not the responsibility of specialist compliance staff alone. It needs to be embedded within a firm and become part of its culture. Nevertheless, a firm will be able to manage its compliance risk more effectively if it has a compliance function in place, the organisation of which may vary between firms. In a small firm, it may be an individual person, it may be a separate department or it may form a discrete part of an overall risk management function. In particularly large and/or international firms, compliance staff may be located within business lines and have group and local compliance officers; separate units may also be established to deal with the prevention of money laundering and terrorist financing (ML/TF).

Irrespective of the organisational structure, an effective compliance function should operate independently, be sufficiently resourced, and have the following responsibilities:

1. To regularly assess and monitor the adequacy and effectiveness of the measures and procedures put in place, and the actions taken to address any deficiencies in the firm's compliance with its obligations.
2. To advise and assist the relevant persons responsible for carrying out regulated activities to comply with the firm's obligations under the regulatory system.

The Basel Committee on Banking Supervision (BCBS) has issued a set of ten principles relating to compliance and the compliance function. While these principles are aimed at banks, their general approach has a much wider application for firms across the financial sector subject to regulation. The BCBS principles can be found at <https://www.bis.org/publ/bcbs113.pdf>.

1.1.2 Responsibilities of the Board

The first of the BCBS principles is that the board of directors is responsible for overseeing the management of the firm's compliance risk. The board should approve the firm's compliance policy, including a formal document establishing a permanent and effective compliance function. At least once a year, the board or a committee of the board should assess the extent to which the firm is managing its compliance risk effectively.

A firm's compliance policy will not be effective unless the board of directors promotes the values of honesty and integrity throughout the organisation. Compliance with applicable laws, rules and standards should be viewed as an essential means to this end. As is the case with other categories of risk, the board is responsible for ensuring that an appropriate policy is in place to manage the firm's compliance risk. The board should oversee the implementation of the policy, including ensuring that compliance issues are resolved effectively and expeditiously by senior management with the assistance of the compliance function. The board may delegate these tasks to an appropriate board-level committee (eg, its audit committee).

1.1.3 Responsibilities of Senior Management

The BCBS principles also set out the responsibilities of senior management who are responsible for:

- the effective management of compliance risk, and

- establishing and communicating a compliance policy, ensuring that it is observed, and reporting to the board of directors on the management of the firm's compliance risk.

Therefore, senior managers are responsible for establishing a written compliance policy that contains the basic principles to be followed by management and staff, and explains the main processes by which compliance risks are to be identified and managed through all levels of the organisation. Clarity and transparency may be promoted by making a distinction between general standards for all staff members and rules that only apply to specific groups of staff.

Senior management are also responsible for ensuring that compliance policy is observed and that appropriate remedial or disciplinary action is taken if breaches are identified. They should also identify and assess the main compliance risk issues facing the firm (with the assistance of the compliance function, at least once a year) and the plans to manage them. Such plans should address:

- any shortfalls (policy, procedures, implementation or execution) related to how effectively existing compliance risks have been managed, and
- the need for any additional policies or procedures to deal with new compliance risks identified as a result of the annual compliance risk assessment.

Senior management should:

- at least once a year, report to the board of directors or a committee of the board on the firm's management of its compliance risk, in such a manner as to assist board members to make an informed judgement on whether the firm is managing its compliance risk effectively, and
- report promptly to the board of directors, or a committee of the board, on any material compliance failures (eg, failures

that may attract a significant risk of legal or regulatory sanctions, material financial loss, or loss to reputation).

1.2 Adequate Resources



2.1.2 Understand BIS Principle 6 and the requirement for adequate resources

Principle 6 of the BCBS principles on 'compliance and the compliance function in banks' states:

'The bank's compliance function should have the resources to carry out its responsibilities effectively.'

The resources should be both sufficient and appropriate for effective management of the firm's compliance risk.

In particular, compliance function staff should have:

- the necessary qualifications, experience, and professional and personal qualities to enable them to carry out their specific duties, and
- a sound understanding of compliance laws, rules and standards, and their practical impact on the firm's operations.

The professional skills of compliance function staff, especially with respect to keeping up to date with developments in compliance laws, rules and standards, should be maintained through regular and systematic education and training.

1.3 Compliance Manual and Policies



2.1.3 Understand the practical applications of a formalised document of compliance policies and procedures: compliance manual

1.3.1 Purpose of the Compliance Manual

The purpose of the compliance manual is to formally document the standards to be followed by all employees in their personal conduct and in conducting business with customers and counterparties. It also serves to expand upon compliance-related content of the company's corporate governance manual in relation to:

- the legal and regulatory obligations of employees and contracted agents, and
- the policies and procedures that apply to the business and personal conduct of employees and agents to ensure that they comply with the laws, regulations, rules and codes that govern the firm's conduct of business as a regulated firm.

All managers and directors of the company are responsible for ensuring that the members of their teams read, understand and are fully conversant with the contents. It should be remembered that this manual is not a procedures manual, but rather provides policy and guidance. Detailed procedures are normally produced by the various operational business areas and overseen by managers or directors who will be responsible for ensuring that their staff know where to find such information.

1.3.2 Scope of the Compliance Manual

The compliance manual endeavours to give a high-level overview of the rules and regulations of the regulatory bodies governing the firm's business. For firms operating internationally, it is important to clearly document how differing or overlapping regulatory

requirements will affect operations and staff. The compliance manual provides employees with the information required to comply with the rules and regulations applicable to their activities. These may include relevant laws of the countries in which the firm directly operates, or in which its clients are situated. Ignorance of the law or relevant rules and regulations will not protect the company or its employees.

The compliance function normally seeks feedback from staff with a view to regular updating of the compliance manual. It is important that it is a 'living' document, and is regularly reviewed and, if necessary, updated based on changes in circumstances, experience, and feedback from staff members. The compliance function needs to keep everyone informed of significant developments arising from regulatory changes and experience throughout the company. Many firms use an online compliance manual with search facilities and links to online learning modules and relevant regulatory websites.

See [Appendix 1](#) for an example of the contents page of a compliance manual.

1.3.3 Communicating the Formal Status of the Compliance Function

The compliance function must have a formal status within the firm to give it the appropriate standing, authority and independence. This may be set out in the firm's compliance policy or in any other formal document. The document should be communicated to all staff, either electronically via an intranet site or other means. The compliance policy needs to be included in induction and other relevant training.

The compliance manual will contain the following with respect to the compliance function:

- Its role and responsibilities.
- Measures to ensure its independence.

- Its relationship with other risk management functions within the firm and with the internal audit function.
- In cases where compliance responsibilities are carried out by staff in different departments, how these responsibilities are to be allocated among the departments.
- Its right to obtain access to information necessary to carry out its responsibilities, and the corresponding duty of staff to cooperate in supplying this information.
- Its right to conduct investigations of possible breaches of the compliance policy and to appoint outside experts to perform this task if appropriate.
- Its right to be able to freely express and disclose its findings to senior management, and if necessary, the board of directors or a committee of the board.
- Its formal reporting obligations to senior management.
- Its right of direct access to the board of directors or a committee of the board.

1.4 An Effective Compliance Function



2.1.4 Understand how an effective compliance function can add value to a business

2.1.5 Know how to produce and implement an effective compliance programme

As mentioned in section 1.1.1, the way in which a compliance function is organised varies between firms. In smaller firms there may be a single compliance officer, or the compliance function may be part of risk management. Larger companies may have decentralised compliance functions in business units as well as a central compliance function.

To be effective, the compliance function needs to operate independently, be sufficiently resourced, and responsible for:

1. Regular assessment and monitoring of the adequacy and effectiveness of measures and procedures in place, and action any deficiencies.
2. Advise and assist relevant staff of the firm's obligations under the regulatory requirements.

The compliance function may include specific statutory roles (eg, an officer fulfilling the role of **money laundering reporting officer (MLRO)**), and may liaise with relevant external bodies, including regulators, standard setters and external experts. They may also be responsible for ensuring that relevant regulatory returns and filings are made, for example, working with a corporate finance department and signing off the adequacy of capital calculations, or arranging for regular reporting of transactions, complaints, **client assets** and money.

An effective compliance function will add value to the business. It will keep it on a compliance path, and its involvement and advice will be sought by all levels of staff in the business. Such a function will contribute to innovation, business development and other projects. It will be seen as a business enabler rather than a stereotypical business-prevention unit.

The compliance function needs to take a proactive approach to its dual responsibilities of monitoring the business and providing advice to senior management. A well-run compliance function can add competitive advantage to a firm, helping to build a strong reputation and attract business. Their key purposes are to:

- provide reassurance to the board and senior management that the business is operating in a compliant manner, through regular reports, ad hoc reports and other management information

- provide advice, information, education, and guidance to the board of directors, senior management and staff on compliance laws, rules and standards and to assist them to meet their compliance responsibilities – especially during times of substantial regulatory change or when the firm is expanding into new product areas
- identify and record good and bad practice
- provide feedback on failures in controls and compliance and provide recommendations for improvements and, where necessary, remedial action
- provide analysis and early warning of regulatory change which may impact the business, and to ensure that such change is communicated to the board and management
- build a good and open relationship with the firm's regulators to ensure they have a good understanding of the business, the risks involved and how those risks are controlled, and to facilitate business development where new permissions or licences are required and, where necessary, resolve issues
- support operational areas when preparing/reviewing their procedures and policies, to ensure that underlying regulatory requirements are correctly incorporated into the material to ensure the first line of defence (see section 2.1.3) is better equipped to prevent problems arising, and the compliance team builds valuable engagement ahead of future monitoring activity
- coordinate application to the regulator for approval of new directors and senior managers, as well as advise on applications of a change in permissions of the firm, and
- where relevant, respond and coordinate responses to proposed legislation or regulations with a view to achieving regulations that, while meeting the objectives, take into account the practical implications for businesses; such responses may be direct with regulators or through trade associations.

While these matters can be of great value when successfully deployed, it is important that the compliance function continues to provide a thorough monitoring programme and ensure that compliance risk is understood. The compliance officer must, therefore, be able to secure the resources needed to deliver these goals.

1.4.1 Identification, Measurement and Assessment of Compliance Risk

The compliance function proactively identifies, documents and assesses the compliance risks associated with the firm's business activities, including the development of new products and business practices, the proposed establishment of new types of business or customer relationships, or material changes in the nature of such relationships. If the firm has, for example, a new products committee, operations committee or risk management committee, compliance function staff should be represented on such committees.

The compliance function needs to measure compliance risk (eg, by using performance indicators) and use such measurements to enhance compliance risk assessment. Technology can be used as a tool in developing performance indicators by aggregating or filtering data that may be indicative of potential compliance problems (eg, an increasing number of customer complaints, breach trends, or irregular trading or payments activity).

The compliance function must assess the appropriateness of the firm's compliance procedures and guidelines, promptly follow up any identified deficiencies, and, where necessary, formulate proposals for amendments.

1.4.2 Monitoring, Testing and Reporting

The compliance function needs to monitor and test compliance by performing sufficient and representative compliance testing. The results of the compliance testing are reported to the head of compliance in accordance with the firm's internal risk management procedures. Determining what needs to be monitored is part of developing the compliance programme.

On a regular basis, the head of compliance reports to senior management on compliance matters. The reports include the compliance risk assessment during the reporting period, including any changes in the compliance risk profile based on relevant measurements, such as performance indicators, a summary of any identified breaches and/or deficiencies and the corrective measures recommended to address them, and a report on corrective measures already taken. The reporting format will be commensurate with the firm's compliance risk profile and activities.

1.5 Compliance Monitoring Programme



- 2.2.10 Understand the purpose of a compliance monitoring programme: risk-based; reporting; planned
- 2.2.11 Understand the key considerations in developing a compliance monitoring programme
- 2.2.12 Understand how to conduct an effective compliance monitoring programme: working papers; meetings with senior management; management responses; risk mitigation plans

The compliance programme sets out the responsibilities of the compliance function and its planned activities such as, the implementation and review of specific policies and procedures, compliance risk assessment, compliance testing, and educating staff

on compliance matters. It is the responsibility of the head of compliance or equivalent, to ensure appropriate coverage across businesses and coordination among risk management functions.

The purpose of the compliance monitoring programme is to provide an independent review of the operational work performed by the firm, with a focus on two elements:

1. To confirm whether operational tasks are being performed in line with operational procedures.
2. To confirm whether operational procedures continue to reflect current regulatory requirements.

It is impractical for the compliance function to review every item of processed work – the cost of supporting such oversight would be uneconomical – and so the compliance function must establish a method for performing sufficient oversight to be confident that the underlying risks have been appropriately controlled. Hence, the compliance monitoring programme must be risk based. The programme involves the review and testing of documentation and completed work items, to identify findings and recommendations for improvements. Specific working papers are generally used, detailing the parameters of the testing to be performed, in order to ensure that the scope of each monitoring review is achieved. The completed working papers also provide a clear evidential record of the review work performed and the specific items that gave rise to findings. Reviews are typically thematic in nature, looking to identify patterns and issues in qualitative data.

While such compliance efforts should be independent of operations, it is important that senior management of the operational area concerned understand the findings and agree on the remedial action to be taken. Formal reporting to senior managers in the business is a common step to ensure that all business areas are aware of the types of issues being identified and the actions being taken to rectify problems. In larger programmes, the compliance function produces a risk mitigation plan to provide

the board with an overall view of how compliance engagement with the operational areas is improving the risk position of the business.

While firms establish their programmes in different ways, there are essentially three key stages:

Stage 1 – Information Gathering

Information is gathered on potential adverse events – such as errors that may arise in the activities undertaken by the firm in delivering its products and services. These may include:

- payments not made on time
- suspicious activity not reported
- failure to complete reconciliations (assets or money)
- late execution of client instructions
- late handling or mishandling of complaints or breaches, and
- unsuitable investment advice.

Stage 2 – Scoring

The events identified as part of Stage 1 are scored for financial impact, exposure and probability. In designing the scoring method, it is necessary to decide whether each metric will be scored using discrete values (eg, a cash value in sterling or a frequency in days) or using relative values.

Financial Impact

Financial impact reflects the magnitude of financial cost were the adverse event to crystallise, and is usually scored according to a set of relative impact measures (eg, a scale from high to low). This has benefits because actual or estimated costs vary according to:

- the precise nature of the event (versus its high-level definition as per Stage 1)
- the particular area or element of activity that gives rise to it, and
- precise values, if the event relates to investment transactions.

Similarly, the potential financial impact of a regulatory transgression is difficult to reliably forecast. Factors to be considered should include:

- investigation costs (potentially including third-party review)
- compensation costs to affected customers
- legal costs in defending the company against regulatory action, and
- potential regulatory fines.

A final consideration is the requirement to include the future financial impact of loss of goodwill and/or reputation caused by the event, but the near impossibility of attributing any particular value or amount.

The head of financial management, for example, the finance director or financial controller, will often assist by scoring individual events per area, providing experience of the level of past costs, and offering an informed assessment of likely impact were an event to occur.

Exposure Frequency Score

Exposure means how often the activity occurs that could give rise to the adverse event. This can be implemented in several ways. For example, using a conversion table that provides a value approximating to the number of occurrences expected/evidenced in a single year. Given the number of business days in a year, a value of 250 might be adopted as indicating a 'daily' event, whereas a value of 50 may indicate weekly, 1 annually, and 0.1 rarely.

When deciding these values, the firm should ensure that the scoring model is appropriately balanced (to prevent certain types of events being given disproportionate attention, while other types of concerns do not sufficiently emerge). For example, the 'real-time' score needs to balance the following:

- Certain activities may occur twice in the working day (eg, work item batching or the receipt of postal deliveries), matching a score of 500.
- Setting a number greater than 500 increases the potential that the model could exaggerate the effect of an event.

While these scores are largely a matter of fact, care must be taken to ensure the scoring system does not incorrectly exaggerate or underplay events such as 'infrequent, with extreme financial impact' and 'real-time events having little financial impact'. Use of an 'additional probability weight field' may be appropriate, or the use of 'number of events' rather than 'frequency' might be preferable for some activities.

Probability Weight

The probability of the adverse event actually occurring must then be determined, taking into account the strength of procedures and controls within the area. This may be expressed as the 'probability of the risk crystallising', (PORC) factor, which reflects the annualised likelihood of an event occurring given the management controls that are in place. For example:

Low – <30%
 Medium – 30% to 70%
 High – >70%

Care must be taken when considering scores of 0% (an impossible event) or 100% (an inevitable event). Some scoring systems are designed not to recognise such scores, while others will permit them in certain circumstances. The initial assessment is based on consideration by compliance, audit and operations management of the findings from past and recent examinations or assessments, the incidence of breaches and complaints, and the extent of manual processes. Trends and proportions are more important considerations than absolute numbers, which, in any event, must be reviewed regularly.

Stage 3 – Weightings

The above variables represent the risk identified by the business. However, the compliance function may need to use additional variables in order to determine the priority subjects for inclusion in the monitoring programme. Such weighting of priorities can be affected by the following variables:

- **Anxiety weighting** – what is currently worrying the compliance officer about industry/regulator- expressed concerns: is the regulator undertaking a thematic review on market timing or the care and protection given to client assets and money?
- **Perspective** – whereas the gathering of information has been largely based on past experience of adverse events, here it is appropriate to consider future volumes of business, propose new areas and the implications for existing operations.
- **Days since last tested** – activities may be considered low risk, perhaps because of low value impact, or because the controls are considered so strong that it is unlikely that the activity would naturally come to the top as a result of the risk factors considered so far. In such cases, using a weighting based on the time elapsed since the activity was last reviewed, ie, that increases as the time-span gets longer, means that eventually the activity will come to the top of the list and be included in the monitoring schedule.

Some firms prefer using a plan which is fixed at one point in the year, and then follow that plan for 12 months. A more dynamic approach is to aim to complete the review of all activities over, for example, an 18-month period, but run the risk assessment on a quarterly basis to focus each quarter's work on the most pressing activities; this also allows for any incidents or regulator concerns to be proactively incorporated into the programme.

1.6 Integration of Regulatory Requirements



2.1.6 Understand how regulatory requirements should be integrated into operating systems, policies and procedures

It is important for a firm to ensure that the operational processes and procedures it employs deliver the outcomes required by regulation. It is also important that the firm establishes controls to ensure that implementation of new processes and procedures – including changes to associated IT systems – are performed based on a sound understanding of those regulatory requirements. The regulatory requirements must be integrated within the firm's processes.

Successful integration of regulatory requirements and the maintenance of compliant systems, procedures and controls require the concerted effort of the whole business and the people who make up the board of directors, management and staff of the firm.

As with most compliance-related issues, integration starts from the top and depends heavily on the culture of the firm. The board and individual directors must consider whether they have the appropriate organisation and controls to ensure that regulatory requirements are integrated and compliance is embedded in the ethos of the firm. They should periodically review their high-level governance policies and procedures.

To ensure the organisation's controls are appropriate, the following factors may be considered:

- **People** – the requirement is to establish an appropriate recruitment programme and hire staff with the right skills, knowledge and experience relating to the business. This includes setting out the required competencies, qualifications, experience expected and testing of candidates

to ensure they have the appropriate skills and knowledge required.

- **Allocation of responsibilities** – written job descriptions are a useful guide for individuals and should include, at a high level, their regulatory responsibilities. This might include a responsibility for managers to train their staff in financial crime prevention, information security and fair treatment of customers.
- **Training** – comprehensive training programmes should be in place including induction courses, on-the-job training, specialist sessions on regulatory areas and a requirement to undertake continuing professional development (CPD), appropriate professional examinations, and access to regulatory updates or bulletins produced by the compliance function and industry updates. A minimum number of CPD hours should be set. Periodic training assessments and needs analysis should be undertaken using information from regular staff appraisals or Personal Development Review (PDRs)
- **Procedures** – written procedures need to be in place for all areas of the business to provide guidance for staff on how to perform activities and incorporate compliance processes. In some firms, the procedures and processes are mapped to the relevant regulations and rulebooks. The procedures should be reviewed and signed off periodically by local management as compliant. The compliance function must check samples of these procedures as part of their monitoring assignments to ensure the validation process is being followed. The compliance function will have procedures for its own activities.
- **Systems** – the design of operational systems should incorporate all the relevant regulatory requirements. These should be documented in business requirements, system requirements or specification documents and be included as part of a robust system and user testing scripts. While the business areas should specify their requirements, the

compliance function will often be called upon to provide advice and guidance on new procedures and significant changes to regulations. Again, the regulatory effectiveness of systems and controls will be included in the sample checks performed by compliance staff during their monitoring assignments.

1.7 Regulations, Internal Policies and Procedures



2.1.7 Know the difference between regulations, internal policies, and procedures

Regulations, and internal policies and procedures, are all important to a firm's governance, although each has a distinct purpose and origin. Regulations are provided by governments and regulatory bodies to give clear minimum rules by which businesses can operate. Regulations might be rules-based or principles-based. Internal policies are created within each firm to guide staff and management in respect of the core principles by which the firm will achieve compliance and explain the main processes to be followed. Policies go further than regulations and, for example, set internal codes of conduct with requirements that go beyond what is required by regulation. Procedures provide the detailed guidance on the action to be taken by management and staff.

Internal policies and procedures reflect the firm's interpretation of the regulations. The regulations may offer flexibility and, therefore, different firms may adopt different approaches. Once again, it is important that the compliance function is involved in reviewing policies to ensure the interpretation is valid. In some cases, an opinion from external consultants or legal experts may be beneficial.

While regulations, and internal policies and procedures serve distinct purposes, conflicts between these items can arise – particularly in respect of international businesses. Conflicts may arise between the local regulations in one jurisdiction and the corporate internal policies and procedures handed down from head office. It is important to identify any such conflicts that arise, and to ensure that regulatory requirements are satisfied in the resolution.

1.8 Regulatory Implications of Business Strategies



2.1.8 Understand the potential regulatory implications of business strategies: outsourcing and oversight; capital requirements; variation of permissions; control framework

1.8.1 Outsourcing and Oversight

Many firms take a strategic decision to concentrate on certain core activities and to outsource other activities and support functions to specialist suppliers. For example, a global asset manager operating collective investment funds may decide that it wants to concentrate on management of the investment portfolios, but outsource all the activities to do with fund accounting, pricing and investor record-keeping.

Generally, regulations permit firms to outsource the tasks associated with regulated activities – although the firm retains regulatory responsibility for those tasks outsourced. This means that supervisory or enforcement action could be taken against the firm if the outsource service provider fails to deliver a compliant operation. Typically, when outsourcing a material task, the firm needs to advise its regulator in advance. In some countries, regulatory approval is

required before outsourcing and, in some cases, outsourcing of specific tasks may not be permitted, or a geographic limitation may be applied with a view to protecting investors.

When outsourcing, a regulator will expect the firm to:

- undertake appropriate due diligence of the service provider
- retain sufficient expertise to undertake oversight of the outsource service provider, to ensure the service is compliant and ensure that access to relevant information is provided to both the firm and the regulator
- have a written contract with the service provider together with a clear service level agreement (SLA) and establish key performance indicators, and
- have agreed with the service provider plans for business continuity and disaster recovery, including periodic testing of any applicable back-up facilities.

A more detailed checklist for outsourcing is provided in [Appendix 2](#) at the end of the workbook.

The European Banking Authority (EBA) has issued guidelines on outsourcing, which came into force on 30 September 2019. They contain specific provisions for the governance frameworks in relation to outsourced activities of financial institutions, as well as the related supervisory expectations and processes. The guidelines specifically state that the financial institution's management remains responsible for all of their activities including those that are outsourced. In 2025, the EU introduced the Digital Operational Resilience Act (DORA) to strengthen the digital resilience of financial entities. It entered into application on 17 Jan 2025 and ensures that banks, insurance companies, investment firms and other financial entities can withstand, respond to, and recover from any IT disruptions, including cyberattacks or system failures. DORA harmonises the rules relating to operational resilience for the financial sector, and is applicable to 20 different types of financial entities and third-party IT service providers.

In response to DORA, the EBA has proposed to update their guidelines to de-scope activities subject to DORA from the outsourcing guidelines, and to extend the scope to include more types of investment firms, authorised issuers of asset-referenced tokens, and non-bank creditors under the Mortgage Credit Directive. The Mortgage Credit Directive regulates first and second charge mortgages and consumer buy-to-let lending.

The institution must have sufficient resources available to appropriately support and ensure the performance of their responsibilities, including overseeing all risk and management of the outsourcing arrangements. Outsourcing must not lead to a situation in which an institution becomes an 'empty shell' that lacks the substance to remain authorised. When the service provider to which operations have been outsourced is based outside of the EU, they still need to comply with EU rules and regulations if they provide services to financial institutions based in the EU.

This is similar in other jurisdictions such as Singapore, Switzerland, Hong Kong, and Australia.

1.8.2 Capital Requirements

The global financial crisis has led to a strengthening of capital requirements and standards by regulators in many parts of the world. Models for firms to use in calculating capital adequacy (ie, the appropriate amount of capital a firm should maintain) have become increasingly complex. Examples of international capital adequacy approaches include the Bank for International Settlements (BIS) Basel II and III Accords for banks, and the EU's Solvency II Directive aimed at harmonising capital requirements across the insurance industry in the EU.

Typically, the regulations and standards set out how to determine the appropriate levels of capital adequacy given the types of

business and levels of risk the business or assets held may represent. Two approaches are commonly used:

- The use of a standard formula for calculating the minimum capital requirements. Depending on the risk-weighted assets of the firm, the minimum capital requirement may fluctuate. In simple terms, this means the higher the risk, the greater the capital requirement.
- The use of internal models to determine the risk reflecting the firm's own risk and solvency assessment. These internal models should better reflect the firm's risk profile than the adoption of a standard formula. It may be lower than the capital adequacy requirement based on a standard formula but equally, it may be higher. The models will need to be approved by the regulator, and are subject to robust governance.

It is important that the business incorporates its regulatory reporting requirements for capital within its overall strategy and operations. Retail banking will have a different risk profile to investment banking, for example. The mix of business chosen and the risk appetite of the institution as set by the board will have significant implications for capital adequacy and overall regulatory requirements.

Any plans to change the business strategy of the firm should, therefore, take into consideration any implications for the firm's capital requirements. A business expansion that might appear profitable could be undermined if it would require the firm to substantially increase its level of regulatory capital.

1.8.3 Variation of Permission (VOP)

One of the ways in which a regulator controls the risks to its objectives is to limit the regulated activities a firm may undertake. A firm must ensure it holds the relevant permissions for the business it

undertakes, and will also want to ensure it does not hold excess authorisations. The broader its permissions, the greater the regulatory obligations.

However, forward planning is essential for business development purposes and the regulatory implications. Early involvement of the compliance function will be required if the firm plans to move into new areas of business, either in terms of an extension of current activities or to diversify into entirely new activities. In many jurisdictions, the process to amend authorisation is known as a variation of permission (VOP).

The firm typically advises the regulator at an early stage of the firm's plans and confirms the requirements for varying the firm's authorised permissions. For a minor variation, application for approval typically requires minimal documentation to be submitted. In this case, the approval process usually takes only a limited amount of time, and can be as little as two to eight weeks.

For major variations, such as an entirely new area of activity, more evidence will need to be provided, including a detailed overview of the firm's expertise in the new activity, the risk assessments undertaken and the detailed business plan. In such cases, the lead time for obtaining regulatory approval can be lengthy and take up to a year.

Regulators may provide a service level target for processing such applications which are designed to give the regulator ample time to consider the application.

1.8.4 Control Framework

A key part of the business strategy is understanding the key risks the business will face and how those risks will be managed. Risks can be mitigated, eliminated, or accepted. Assessment of the risks associated with any change in business strategy, together with an understanding of the need to control those risks, is vital to ensuring

that the firm is prepared to expand its business activities or adopt some other change in overall strategy. While change can be positive in realising growth for a company, the compliance officer must ensure that the regulatory consequences of change have been understood and appropriate plans put in place.

1.8.5 Preparing Compliance Reports



2.1.9 Know how to prepare an effective compliance report for management

2.1.10 Know what basic information compliance officers should have access to

There is no prescribed layout for compliance reports, and firms will take differing approaches. Some firms prefer narrative styles, while others might use a recognisable corporate template to ensure consistency across the various reviews performed (such as the example shown at the end of the workbook).

Regardless of the format, the following needs to be taken into consideration:

- **Initial steps:**
 - The title page and meeting corporate style/standards.
 - Designing a template that meets your needs.
 - The introduction and contents pages.
- **Report scope, parameters and people:**
 - The purpose of the review and report.
 - Compliance project reports – summary and objectives.
 - Acknowledging key personnel.

- Any points to be noted.
- **Significant pages:**
 - Contents: subject areas considered and reviewed.
 - The executive summary.
 - Report findings and recommendations.
- **The right of reply:**
 - Incorporating management responses.
- **Issuing the report and document version control:**
 - Recording, retention and revisiting.

Access to Information and Personnel

The compliance function needs to be able to communicate with any staff member and obtain access to any records or files necessary to enable them to carry out their responsibilities. They need to be able to independently carry out their responsibilities in all departments of the firm in which compliance risk exists. They should also have the right to conduct investigations of possible breaches of the compliance policy, and to request assistance from specialists within the firm (eg, legal or internal audit) or engage outside specialists to perform this task if appropriate.

The compliance function should be free to report any irregularities or possible breaches disclosed by its investigations to senior management, without fear of retaliation or disfavour from management or other staff members. Although its normal reporting line should be to senior management, the compliance function needs to have direct access to the board of directors or a board committee, bypassing normal reporting lines when necessary. Further, it may be useful for the board or a committee of the board to meet with the head of compliance at least annually, as this will help the board or board committee to assess the extent to which the firm is managing its compliance risk effectively. In larger firms,

the compliance function will be directly represented on the board with the appointment of a compliance director who may serve as the chief compliance officer for the company and its subsidiaries.

Examples of the types of records compliance typically access for monitoring purposes fall into three main categories. They are:

- basic
- periodic, and
- non-essential.

Basic Records

- Customer applications/instructions.
- Suitability/appropriateness test records.
- Contract notes.
- Transaction records.
- Telephone recordings.
- Customer correspondence (written and electronic).
- Accounts – customer, bank.
- Customer asset and money reconciliations, trust letters.
- Marketing materials.
- Complaints and breach of regulation records.
- Suspicious activity reports (SARs).
- Court of Protection orders.
- Court orders.
- Marriage certificates.
- Probate documents.
- Powers of attorney (POAs).
- Death certificates.
- Anti-money laundering (AML) documents.
- Scanning.
- Tax vouchers.
- Tax-related reports/returns.

- Policies.
- Procedures.
- Distribution records.
- Cheque processing.
- Risk assessments.
- Control reports..

Periodic Records

- Prospectus and instruments of constitution.
- Staff records for recruitment, fit and proper tests, references, credit checks.
- Training and CPD.
- Statements issued to customers.
- Report and accounts.
- Websites.

Non-Essential

- Supplier invoices.
- Management accounts – forecasts/projections.
- Adviser/client agreements.



2. Regulatory Compliance and the Risk of Non- Compliance

2.1 Regulatory Compliance and the Risk Responsibilities and Accountabilities of Management and Staff



2.2.1 Understand the responsibilities and accountabilities of management and staff for compliance with regulations

Regulators expect the executive management of a firm to ensure that their responsibility for the running of the firm is clear. When it comes to daily 'business as usual' activity, all staff and management of a firm must, together, ensure that it remains compliant with the regulations.

Operational processes must follow the prescribed procedures to ensure that the right outcomes are achieved. Any concerns staff might have regarding the accuracy of those procedures should be escalated for consideration by management. Staff and management

must ensure that the training provided to each person remains current and suited to their role, and that any regulatory training obligations are satisfied (such as obligations for AML training). While firms will often make such matters part of the firm's code of conduct, enabling it to take disciplinary action against staff where relevant, it is important to recognise that failings in these areas could give rise to regulatory concerns as well as HR issues. The code of conduct is the firm's documented expectations of how its staff and management will act in respect of share dealing, engagement with clients and suppliers, and various other matters.

2.1.1 Understand How to Monitor whether a Business is in Compliance with Regulations and Internal Policies and Procedures



2.2.2 Understand how to monitor whether a business is in compliance with regulations and internal policies and procedures

The common methods used to monitor compliance are:

- interviewing relevant staff, management and directors, particularly when an issue has been raised or escalated
- observing the processes in action and seeing evidence of the controls being operated
- testing statistically-based samples of transactions, either in situ or by desk-based review. It is particularly helpful if compliance staff have direct read-only access to relevant systems such that they can take their own samples and do not have to rely on operational staff for providing the material
- reviewing previous reports, audit reports and other key management information such as key performance indicators, breach and complaint trends, and

- reviewing specific system-produced transaction reports for the compliance function, for example, checking exception reports and any follow-up actions.

For example, in the event the compliance function observes a trend in specific types of money laundering transactions, they could start a project to check similar transactions. At first, to establish whether this pattern may be an anomaly or an indication of a wider trend they start with checking a sample of transactions from a similar business unit in detail. In the event the pattern is confirmed within a sub-set of the sample, the compliance function will extend their compliance checks to a larger number of transactions and include observing processes and interviewing staff and management.

2.1.2 Risks of Non-Compliance



2.2.3 Understand the risks associated with non-compliance for firms and the financial services industry

It is generally accepted that no firm can at all times remain fully compliant with all regulatory requirements. Manual processes are open to error; human beings will make mistakes; fully automated processes can be vulnerable if system problems arise. While any firm may, at times, experience a breach of regulation, it is important that the firm appreciates the significance of such breaches and the potential consequences that could follow. Ultimately, in the case of severe breaches, a regulator will have the power to sanction a firm as well as its executive management in the event that the firm fails to uphold the standards expected. It is, therefore, important for the firm to distinguish between isolated failings and situations indicating that a systemic problem exists.

One example of an isolated breach would be where a transaction is misfiled through human error, such that the transaction is delayed

and the investor may receive a worse price on their deal. It is important that the firm rectifies such cases. Root cause investigations are a valuable control to confirm that the human error was not caused by a poorly designed process or badly written procedure. Any root cause identified by the firm should be promptly addressed to prevent continued breaches bearing in mind that some breaches are worse than others, and not all breaches are the same in terms of risk and impact. For example, a breach of ML regulations or fair treatment of customers principles has a higher impact than an isolated case of misfiling a transaction.

The chief risk faced by a firm is that its regulator will take action if it becomes concerned by the level, type, or frequency of breaches arising, or that the firm is failing to address the fundamental causes of problems. Where the regulator believes the firm's clients are being put at risk, or where it considers the firm is not responding appropriately to the regulator's expectations, the regulator may impose a fine on the firm. Such fines are often made public, which could undermine client confidence in the firm. In some cases, the regulator might also take action against the senior management of the business; those individuals who were personally responsible to the regulator for ensuring the business would be well run.

Aside from the specific cost of any regulatory action taken, the firm is likely to incur substantial additional expense in managing a period of regulatory investigation. Firms under regulatory investigation will often retain external support to help their investigations and build a defensive case – all of which has implications for the firm's profitability.

In extreme cases, the regulator has the power to revoke authorisation, effectively preventing the firm or individual from continuing in business. The regulator must seek to ensure that overall confidence in the financial sector as a whole is maintained, and doing so requires strong action to be taken against those who have failed to operate at the required standards. Revoking of authorisation of firms is rare. For example, in January 2024, the PRA

imposed a penalty of £118,808 on Mr Hunter, the CEO of Wyelands Bank, as an individual for breaching three conduct rules. In addition, Mr Hunter is no longer permitted to work in financial services in the UK. In December 2000, the Federal Reserve Board in the US issued a termination notice against the US operations of Bancomer S.A. as a result of the bank's conviction for a money laundering offence in the US.

2.1.3 Independence of the Compliance Function



2.2.4 Understand BIS Principle 5 relating to the independence of the Compliance Function and senior management accountability

2.2.5 Understand the relationship between compliance and other departments, including 'three lines of defence'

Principle 5 of the BCBS' principles for compliance and the compliance function in banks states that the compliance function should be independent.

The concept of independence does not mean that the compliance function cannot work closely with management and staff in the various business units. Indeed, a cooperative working relationship between compliance function and business units should help to identify and manage compliance risks at an early stage.

The concept of independence involves four related elements:



Compliance should have a formal status within the firm



There should be a group compliance officer or head of compliance



Their responsibilities within the firm should not lead to conflicts of interest



They should have access to information and personnel

The independence of the head of compliance and any other staff having compliance responsibilities may be undermined if they are placed in a position where there is a real or potential conflict between their compliance responsibilities and their other responsibilities. It is the preference of the BCBS that compliance function staff perform only compliance responsibilities. The BCBS recognises, however, that this may not be practicable in smaller banks, smaller business units or in local subsidiaries. In these cases, therefore, compliance function staff may perform non-compliance tasks, providing that potential conflicts of interest are avoided. The independence of compliance function staff may also be undermined if their remuneration is related to the financial performance of the business line for which they exercise compliance responsibilities. However, remuneration related to the financial performance of the bank as a whole should generally be acceptable.

Most firms apply the three lines of defence approach or a recognisable variation of it.

- First line of defence is operational controls – such as a ‘quality check’ performed on transactions inputted on the firm’s systems to reduce the risk of a processing error. Given the nature of operational activities, such first line checks are usually performed only a short period after the initial operational activity so that problem scenarios can be avoided. First line is business and process owners.
- Second line supports management to help ensure risk and controls are effectively managed. This is usually provided by the compliance function. The compliance monitoring programme discussed above enables sample-based review of the operational tasks performed to validate the specific performance achieved and to reflect upon whether any improvements might be made to better secure the operational processes against risk.
- Third line of defence provides assurance to senior management and the board that the first and second lines’ efforts are consistent with expectations and is generally the role of the firm’s internal audit function.

The three lines of defence are complementary, each performing its control responsibilities independent of the other lines. The frequency of review may reduce as you progress through the lines of defence, but the depth of critical analysis increases in order to ensure the firm’s processes are mitigating risks to the optimal level (given budgets and other organisational limits).

The three lines of defence are a clear and consistent organisational and operational structure, including decision-making powers, reporting and functional links and segregation of duties which are clearly defined, transparent, consistent, complete and free from conflicts of interest.

2.1.4 Compliance Role in Training and Competence



- 2.2.6 Understand the role compliance has in training and maintaining competence and awareness: educating staff on compliance issues; acting as a contact point for compliance queries from staff members; providing written guidance to staff
-

The role of compliance in training largely covers in three main areas:

1. Educating staff on compliance issues.
2. Acting as a point of contact for compliance queries from staff members.
3. Providing written guidance to staff.

Educating Staff on Compliance Issues

Education of staff on compliance matters may be completed in a number of different ways, depending on the size and approach of the firm.

If there is a learning and development department responsible for delivering training, then they are likely to be responsible for induction courses and periodic regulatory courses such as those relating to financial crime prevention. The role of compliance is to review the training material and provide advice on updating it to reflect any changes in regulations.

Special workshops or training sessions may be required to be prepared and possibly delivered by compliance staff on specific areas of regulation, such as anti-bribery legislation or new product regulation. They may also provide sessions in groups or individually for directors and senior management who are approved by the regulator; this would be to cover the senior management responsibilities so far as compliance is concerned.

Acting as a Point of Contact

Providing a compliance helpdesk/helpline can be a valuable educational tool. This would deal with day- to-day queries arising

from the business where line managers have not been able to answer the query. This can then highlight any areas of the firm and activities where there may be a lack of knowledge and the need for more formal training or guidance to be given. The provision of online facilities with the compliance function producing a frequently asked questions (FAQ) guide can be useful.

Providing Written Guidance to Staff

The compliance department must understand the specific regulations applicable to the business, though most areas of the business simply need to ensure that the work they undertake remains in line with the regulatory requirements. As such, the compliance team will need to provide a range of updates and documentation to support the business areas in maintaining the necessary standards and ensuring that any projects to implement regulatory changes are accurately defined.

There will always be a need for compliance to respond to queries that arise from business-as-usual (BAU) events. In order to remain efficient, and to avoid any systemic concerns from developing, the compliance team should periodically consider whether the BAU questions it has received indicate any underlying concern in a given part of the business. Again, maintaining open and supportive relationships with the business is important for giving compliance visibility of potential concerns.

Depending on the specific activities of the firm, the compliance function may maintain a formal 'house view' of how certain regulations are to be interpreted or applied. Any change to those rules will require the compliance function to update its material and communicate any consequences with the business areas affected. The compliance function might provide periodic internal updates to summarise regulatory themes or specific matters of interest, providing a 'call to action' for the firm to ensure that it is strongly positioned on a matter of regulatory interest.

For firms with a smaller compliance department, these materials might be obtained from participation in industry events or trade association discussions. The key point is that the compliance function must ensure it provides guidance to staff in respect of regulatory obligations.

As part of their monitoring programme, the compliance function will review the training and competence policies of the firm and test the record-keeping relating to those staff in approved or supervisory roles. This is to ensure that the training plans and CPD have been completed and, where relevant, that the supervisor or senior manager has assessed the individuals as competent to undertake their role.

2.1.5 Non-Compliance by Individuals



2.2.7 Understand how to monitor an individual's compliance with regulations and internal policies and procedures

2.2.8 Understand the range of potential outcomes to remedy non-compliance by an individual within a firm: training and development activities; internal disciplinary measures; external regulatory sanction; legal avenues

The directors and management of a firm have responsibility for the day-to-day managing of staff and providing feedback on any issues arising from an individual's performance. Quality checking and assurance processes should be designed to identify non-compliance. If the matter is serious, then it may be necessary for management to involve HR or the personnel department and, if there is a regulatory issue, the compliance function too.

The following list provides examples of methods for the monitoring of an individual's compliance with regulations and internal policies

and procedures:

- **Regular appraisal of performance by senior staff** – this may range from daily contact and support/ advice provided by those in supervisor, manager or executive roles through to more formal periodic reviews. Periodic reviews may be monthly, quarterly, half-yearly or annual. Appraisals normally are interview-based with written records of areas discussed.
- **Quality checking and assurance processes** – this may take the form of manual checks by a second experienced person. This may range from checking each activity and item of work (ie, checking 100% of the individual's work) through to checking a sample, for example, 10%.
- **Exception and error reports** – automated system reports may be used to identify where non-compliance may occur. For example, if an investment manager fails to observe investment and borrowing limits, an automated report may be used to warn when a breach occurs.
- **Testing on a periodic basis** – for example, the firm may provide regular (eg, annual) training and refresher training on regulatory subjects and internal policies. These sessions will often involve testing of the individuals to ensure their compliance knowledge is satisfactory.
- **Self-certification by the individual** – a firm may require individuals to sign a declaration periodically (eg, annually) that they have read and understood the firm's policies and procedures, for example, a declaration that the individual has read and understood the policies and procedures relating to client data protection or privacy.
- **Audit trails** – ensuring that the firm maintains adequate records to demonstrate compliance is important. Such records, whether paper- or system-based, may be used to demonstrate an individual's compliance, as well as the firm's. In the event that criminal activity is suspected, then a formal audit of the records may be necessary.

The potential outcomes could involve the following:

- **Training and development activities** – this may involve some coaching by an experienced member of staff or it may require the individual being temporarily removed from their role while they are retrained in processes which are compliant.
- **Internal disciplinary measures** – where the individual has acted negligently or repeatedly been non-compliant, then appropriate internal disciplinary measures may be necessary. This may include the giving of a verbal or written warning and a record made on their personal file. Where the behaviour persists, suspension and/or dismissal may be necessary.
- **External regulatory sanction** – in certain cases, it may be necessary for the compliance function to notify the regulator. Remember the principle of an open relationship with your regulator. It is possible that the individual may be subject to action, particularly if the breach amounted to serious market abuse; and the firm is at risk too if it failed to have appropriate controls in place or monitor what was going on. A ban and fine for the individual may be levied, quite separate from any action against the firm.
- **Legal avenues** – if the breach is related to ML, insider dealing or bribery, for example, then the regulator may take legal action for any offences committed. Clearly, if convicted of a criminal offence, the individual may face quite severe penalties; not just a fine, but a potential custodial sentence.

2.1.6 Business Development



2.2.9 Understand the role compliance plays in new business development: due diligence; risk assessment; scope of regulation and approval; highlighting material changes in the nature of existing relationships; assessing and reporting potential reputational risks

There are five key aspects to the role compliance plays in the development of new business. These aspects are:

- due diligence
- risk assessment
- scope of regulation
- highlighting material changes in the nature of existing relationships, and
- assessing and reporting potential reputational risks.

Where there is an independent compliance department, there tends to be an emphasis on advising the business. In particular, the role of compliance in approving new products has increased significantly over the years and is recognised as vital to the product development process. This is an area where compliance can add value at an early stage in the product approval process and thereby help to avoid problems such as potentially breaching regulations later on. It is common at larger firms for there to be written guidelines for new product initiatives, integrating compliance into the process.

Depending on the relationship between the firm's compliance and risk management functions, compliance will either perform or participate in a due diligence review of any new product or service that the firm wishes to introduce. The focus for compliance is to ensure that the regulatory aspects of the new service have been correctly understood and determine any impact of the new service upon the firm's regulatory permissions or capital requirements. At a later point, compliance will need to verify marketing communications and regulatory submissions relating to the new service and may review operational readiness and system test output where the change is substantial.

The wider risk assessment performed in the firm will look at the operational risks of delivering an accurate and timely service in respect of the new product and consider any potential reputational damage that the firm may suffer if problems arise. The firm will also

need to ensure that the correct external relationships (eg, partners, clients and suppliers) are in place and ready to support the expanded business in terms of volumes, capacity and complexity.



3. Managing Regulatory Relationships

3.1 Regulator Relationship



- 2.3.1 Understand the relationship between the firm and regulator
- 2.3.2 Understand how an effective regulatory relationship can be of strategic importance to a firm: advocating opinion; involvement in consultation; drafting regulatory responses; making representations and applications; obtaining effective guidance

3.1.1 How Regulators Manage the Relationship with Authorised Firms

As a general principle, regulators supervise firms according to the risks they present to the regulator's objectives. Regulators assess risks in terms of their impact (the scale of the effect these risks will

have on consumers and the market if they were to happen) and probability (the likelihood of the particular issue occurring).

As noted by the International Organization of Securities Commissions (IOSCO), supervision of market intermediaries' conduct through inspection and surveillance helps to ensure the maintenance of high standards and the protection of investors. These preventative programmes are a necessary complement to investigation and enforcement programmes. The nature and extent of the supervisory relationship with an individual firm depends on how much of a risk the regulator considers the firm could pose. It also may take into account the risks across several firms in the sector (to provide a benchmark) or indeed the market as a whole. Different methods or frameworks may be used to assess that risk, but generally the focus will be either on the firm alone or as part of a sector/industry.

The base level of supervisory intensity depends on impact and probability scores assigned to a firm (or group of firms) which, in turn, help to determine the nature of the relationship that the regulator has with a particular firm.

Medium- and High-Impact Firms

In medium- and high-impact firms, the firm may coordinate work through a relationship manager, who carries out a regular risk assessment and determines a risk mitigation programme proportionate to the risks identified. The precise volume and type of work undertaken will depend on the size and risk rating of the firm concerned.

On a regular basis, the regulator will analyse a firm's financial and other returns and check compliance with notification requirements. Breaches and other indicators of risk may be followed up by the supervisory team with the firm's compliance function.

For high-impact firms, the regulator is likely to apply a closer monitoring regime. This is essentially a planned ongoing schedule

of visits to the firm to meet the firm's directors and senior management regularly. In addition, for high-impact firms which are systemic in nature, the regulator may design specific programmes of core work to assess the biggest risks on the prudential and conduct side of the business.

Where possible, the regulator may centralise supervision of all associated firms within a group in a single team and, when appropriate (for example, if it believes the group has an integrated management and/or control structure), produce a combined risk assessment and risk mitigation programme covering all the firms in a group.

Low-Impact Firms

If a firm is assessed as low impact, it may not have a specific risk assessment or risk mitigation programme. These firms are monitored by a combination of base-line monitoring of financial and other returns, action in response to risks identified by this information, thematic exercises to monitor compliance standards in a sector and work as part of sector-wide reviews.

Individually, most small firms pose a low risk to a regulator's objectives. In practice this means that unlike the larger firms, they do not have regular risk assessments and are usually required to send regulatory reports less frequently. Small firms are unlikely to have an individual relationship manager.

However, collectively, small firms pose a risk to a regulator's objectives. The regulator may collect information from a variety of sources, analyse the data to identify collective risks and, where necessary, investigate the matter further (eg, using questionnaires or targeted firm visits), and then communicate the results of the research to the industry. The aim is to change the behaviour of small firms in a way that improves standards across the industry.

3.1.2 Building the Relationship

Building a good relationship with the regulator is a key role for compliance staff. An effective relationship is one that is built on mutual trust and enables open and constructive discussion to take place. Indeed, a commonly accepted principle is that a firm must deal with its regulator in an open and cooperative way and must appropriately disclose to the regulator anything of which it would reasonably expect notice. One of the valuable aspects of a good relationship is the ability of the firm's compliance function to seek an opinion on issues that arise and discuss resolution, or perhaps seek an opinion on a planned business development. Similarly, the regulator may wish to seek firms' opinions on a formal, or informal, basis about a regulatory issue that may be affecting the sector or industry.

Obtaining effective guidance at an early stage can clearly be of strategic importance to the firm and save a great deal of time and effort. A constructive relationship with the regulator enhances the opportunity for such dialogue.

Responding to consultation papers issued by the regulator allows a firm the opportunity to formally express their opinion on forthcoming regulations. It allows the firm to provide the regulator with information about the practical implications of the proposals being made. It is common for regulators to be accountable for ensuring they understand the business impact and, in some cases, carry out cost benefit analysis to ensure the proposals are proportionate.

Such responses to consultations may be collated by trade associations, and the balance of industry opinion can be analysed and provided to the regulator. This route also allows firms to comment anonymously. However, firms may decide to respond directly as well as through any relevant trade association. When drafting such responses, it is usual to set out details of the firm, its position in the industry and its interest in the consultation being undertaken before going on to respond to the specific points raised in the consultation paper issued by the regulator.

3.1.3 Applications

Obtaining authorisation usually requires a formal application to be made to the regulator. The following are examples of the various types of information required; in this case, for a retail financial intermediary firm:

- Staff organisational chart.
- Business plan information.
- Compliance procedures.
- Details of the firm's professional advisers.
- An opening statement of financial position (also known as balance sheet).
- A forecast closing balance sheet after 12 months' trading or first year's trading.
- A monthly income statement (also known as profit and loss account) for the first years of trading.
- A monthly cash flow forecast.
- A copy of the latest annual accounts (if previously traded).
- A professional indemnity insurance quotation.

3.1.4 Representations

Where a regulator has made a formal decision to refuse an application or proceed with enforcement, it will normally offer an appeals process for firms. The representation may be in writing, or it may be an oral representation, and will, in the normal course, be put to persons who may be independent but are appointed by the regulator for the purpose of hearing such representations.

3.1.5 Regulatory Visits



2.3.3 Understand what to do if your firm is the subject of a regulatory or law enforcement visit: scheduled;

Visits from the regulator are an important tool of regulatory supervision. These visits ensure that firms are complying with the requirements and standards under the regulatory system at all times. They can be scheduled or unscheduled and involve regulators coming onsite, interviewing senior management, and reviewing files. Visits typically last for a few days.

Scheduled Visit

Medium-sized, as well as selected other businesses, can expect to have scheduled visits from their regulator:

- periodically to undertake risk assessments, and/or
- as part of thematic research and investigation, perhaps involving a number of firms across the industry or sector.

Larger firms can expect to receive visits for the same reasons, but they may also attend regular meetings to discuss specific areas of their business, and to maintain contact with senior management to discuss the firm's strategy and corporate plans. In all the above routine-type visits, the firm will normally receive prior notice of the visit and may well receive a request for information to allow the regulator to carry out some desk-based analysis and prepare for the visit. Firms may also, as part of relationship- building, proactively invite the regulator to their premises to update them on business developments, organisation structure or to present a corporate update and plans for the business over a period.

In all these cases, it is helpful to obtain the cooperation of all relevant areas of the firm who may be involved in the visit. Planning will enable such a visit to run smoothly: prepare the agenda beforehand, book meeting rooms, arrange for relevant directors or managers to be available at the times arranged, arrange refreshments, and organise someone to take notes of the meeting(s).

Unscheduled Visit ('Dawn Raid')

Regulators may undertake unscheduled visits where they have an ongoing investigation, which may involve a criminal offence such as insider dealing or ML. Countries around the world are adding challenges in the form of new laws or the renewed enforcement of existing laws. As national laws are strengthened, and international regulators cooperate on significant investigations, so the likelihood of dawn raids increases.

Unscheduled Visit Procedure

Raids may be carried out at dawn but are usually commenced at the start of the working day. They often take place simultaneously at various offices and homes of key individuals.

A regulator seeking to enter the premises to search for evidence will usually hold a legal search warrant authorising its action. The raid will, therefore, usually be accompanied by police officers. The firm should check that the warrant is in order and ensure that the search team does not exceed the authority granted by the warrant.

The warrant should specify:

- the date on which it was issued
- the legal authority by which it was issued
- the regulatory authority to whom it was granted
- each set of premises to be searched, and
- the type of articles, materials, or persons sought.

However, the exact nature of warrants will differ between jurisdictions and on the legal basis by which they are issued.

Once inside, the investigators will search through documents, records, and computers.

They are likely to have at least one specialist computer forensics expert in the team. The investigators are entitled to take copies of any relevant information. If information is not readily available, then the investigators can ask for it to be compiled. They may also be in

possession of a search and seizure order, in which case they can also take possession of hard drives and original documents. Information or documents that fall within the terms of the warrant may be seized; however, the police may be able to seize other material (eg, incriminating material giving direct evidence of a criminal offence) even if not specified in the warrant.

Legally privileged documents and those that may lead to self-incrimination do not need to be provided. Legal advice should be sought to ensure there are reasonable grounds to believe that privilege exists. The investigators must keep a record of all documents they copy and they will ask someone to sign it before they leave and, at that time, a copy should be taken for the records of the firm.

The warrant also entitles the investigators to interview individuals. Failure to cooperate with any aspect of the raid could be a criminal offence punishable by a prison sentence.

Investigators may be willing to wait for legal representatives to arrive before they commence their search, but they are not obliged to do so.

Advance Preparation

It is good practice for firms to advise their employees about the possibility of dawn raids occurring and brief them on the procedure. It is important for staff to understand the scope of the information they should provide. In particular, they should be aware of the legal consequences of a failure to cooperate and of **tipping off** any other persons who may be involved. Firms should have in place procedures for key staff to follow in the event of a raid, including who should be notified.

Consideration should also be given as to how information is stored and whether legal advice and communications should be filed separately. This is advisable in any event and in the event of a raid, it will avoid the inadvertent disclosure of privileged information. In

addition, firms are advised to consider lodging copies of sensitive information with their lawyers. If asked for copies, the firm can advise the investigators that they are in safekeeping and that the solicitors will undertake to hold them pursuant to a court order.

Firms should also consider whether the seizing of individual hard drives would inhibit the operation of the company or if all essential information is held on a central server. Consideration should also be given as to how the company would respond to any media interest and in relation to advising investors as to what has occurred. There should be clear internal policies as to how the company would respond if the activities of an employee or director are the focus of any investigation.

General Checklist in the Event of a Raid

If there is a raid on your property, whether business or residential, it is important that you do the following:

- Check that the warrant has been granted against your premises/abode and that it is signed, dated and sealed and that it is still in date – there will be a window of time for the investigators to make the raid. Ensure that all investigators present are named on the warrant. Exclude entry to anyone attempting to enter who is not named.
- Advise the investigators that you are contacting your legal adviser and will ask them to be present.
- Check the terms of the warrant and the scope of the information which must be provided. Brief employees as to the scope of the warrant and remember that you do not have to provide privileged legal advice and that you have the right to redact documents which have information in them which is not relevant.
- Cooperate by allowing access to relevant documents and information and advise anyone else involved to cooperate.
- Do not tip off people who may not be present that there is a raid, particularly if you believe that they may also be involved

and advise other employees of the same risk. Ask investigators before you notify other offices or directors.

- Keep a list of all the documents copied/supplied/asked for and also any questions which are asked and the answers given. The investigators must provide a list of what they are taking. The two lists should be checked against one another before you accept and sign the investigation record of documents copied/taken.
- Compile a report on the raid.

3.1.6 Breaches



2.3.4 Understand what to do if a regulatory breach occurs

2.3.5 Know what types of information must be disseminated to whom in the event of a regulatory breach

When a regulatory breach occurs, the firm needs to first assess the severity of the breach. The severity will dictate what they need to do. Every breach needs to be assessed and actions need to be taken to ensure they do not re-occur. However, not every breach requires immediate reporting to the regulator.

Minor regulatory breaches need to be recorded in a breaches log and a record needs to be kept of the resolution of the breach or other action taken. The breach should be reviewed by an appropriate manager to ensure that all relevant action has been taken, including where appropriate, that compensation has been paid or that the client has been restored to their correct position.

Analysis of breaches will be helpful to indicate trends and provide managers and senior managers with information to help control the business, identify any action required and consider any preventative

action for the future. Any client impacted by the breach should be notified and provided with an explanation of any action taken.

If the breach is a notifiable breach it needs to be reported to the regulator typically within 24 hours of identification of the breach. A notifiable breach is a type of breach which regulations state is reportable to the regulator. The regulator may request some form of incident report and an explanation of how the breach was discovered, whether investors were at risk, and what remedial action has been taken. It will also wish to understand whether the breach is a single event or evidence of a systemic problem. It is important that relevant directors and senior managers are aware of any breach that is reportable to the regulator and ensure that the information provided accurately reflects the issue, the action already taken to rectify the position (and prevent recurrence), and any ongoing areas of activity.

3.1.7 Confidential Information



2.3.6 Know what information may be disseminated and what should remain confidential if financial crime is suspected or detected

2.3.7 Know what types of information should remain confidential in the normal course of business

If financial crime is suspected or detected, the person discovering the information should report the matter to the firm's MLRO. If the MLRO based on their review believes it is suspicious, then they should make a suspicious activity report (SAR) to the appropriate law enforcement agency (LEA). Failing to report suspicions is a criminal offence.

If a client is being investigated, the LEA will not usually divulge the source of the initial report, although the client may have the right to see relevant papers/reports should they request them. When an

MLRO makes an SAR, individual staff names are not passed on as part of the process. Staff should not inform the client that a report is being made about them. This is regarded as tipping off. The staff member may be liable to imprisonment, a fine, or both if they were convicted of tipping off.

Staff may refer concerns about specific transactions or other activity to their line manager to obtain advice or guidance. However, the suspicion should still be logged and referred to the MLRO.

An example of suspicion raised by staff might include the following:

1. **Incident summary** – a high level summary of the case. For example, the client did not pass telephone security questions which may require the client to quote letters from a password, answer a pre-advised security question (eg, providing their mother's maiden name), or confirm their date of birth.
2. **Details of the incident** – details of the case, including reference to dates and amounts, as appropriate. For example:

'The client called on 27 October 2022, they answered the full name, address and date of birth questions successfully, but they sounded young and the account holder on the system is shown as a being in their 80s. The caller came through the automated valuation line and was querying the valuation; in addition the caller wanted confirmation of how to sell the investment quickly and send the proceeds to a third party. I informed the client that I could not locate an account with the information provided and that they should put their request in writing.'

3. **Reason for suspicion** – an explanation of what made the staff member suspicious regarding the case, eg, the voice did not sound like it belonged to a person in their 80s and the caller was clearly interested in selling the investment quickly and wished the proceeds to be sent to a third party.

The SAR will be made to the regulator and/or an appropriate arm of the police that deals with financial crime.

In the normal course of business, the authorised firm will have a duty of care to keep confidential all the client's information, including the details of their investments or bank account. Any personal data will also be subject to relevant data protection or privacy laws. Reporting suspicious activity, therefore, involves sharing confidential information, but does not constitute a breach of client confidentiality or data protection/privacy laws in such circumstances.

Such information may only be disclosed where it is necessary for a criminal investigation or in the event of tax evasion; release of the information may be subject to an appropriate court order being served on the firm.



End of Chapter Questions

1. State the two responsibilities of an effective compliance function, irrespective of the organisational structure.

An effective compliance function should operate independently, be sufficiently resourced, and have the following responsibilities:

1. To regularly assess and monitor the adequacy and effectiveness of the measures and procedures put in place and the actions taken to address any deficiencies in the firm's compliance with its obligations.
2. To advise and assist the relevant persons responsible for carrying out regulated activities to comply with the firm's obligations under the regulatory system.

Answer reference: Section 1.1.1

2. Who is responsible for establishing a written compliance policy containing the basic principles followed by management and

staff?

Senior managers are responsible for establishing a written compliance policy.

Answer reference: Section 1.1.3

3. What is the purpose of the compliance manual?

The purpose of the compliance manual is to formally document the standards to be followed by all employees in their personal conduct and in conducting business with customers and counterparties. The compliance manual may also expand upon compliance-related content of the company's corporate governance manual.

Answer reference: Section 1.3.1

4. What are the three key stages involved in a risk-based approach to a monitoring programme?

The three key stages involved in a risk-based approach are:

1. Information gathering (gathering information on potential adverse events)
2. Scoring (scoring each event for financial impact, exposure and probability), and
3. Weighting (using formulas to ensure that the most important factors have the largest influence when aggregating the overall score).

Answer reference: Section 1.5

5. What are the most common methods used to monitor whether a business is in compliance with regulations, internal policies and procedures?

The common methods used to monitor compliance are:

- interviewing the relevant staff, management and directors
- observing the processes in action and seeing evidence of the controls being operated
- testing statistically based samples of transactions, either in situ or by desk-based review
- reviews of previous reports, audit reports and other key management information
- reviewing specific system-produced transaction reports for the compliance function.

Answer reference: Section 2.1.1

6. To which types of people might compliance staff provide individual training?

Individual training may be provided to directors or senior management staff. Compliance staff might also provide training on new areas of regulation pertinent to the business.

Answer reference: Section 2.1.4

7. What role might compliance play in the development of new business?

There are five key aspects to the role compliance plays in the development of new business. These aspects are:

- due diligence
- risk assessment
- scope of regulation

- highlighting material changes in the nature of existing relationships
- assessing and reporting potential reputational risks.

Answer reference: Section 2.1.6

8. What two factors do regulators use to assess risks?

As a general principle, regulators assess risks in terms of their impact (the scale of the effect these risks will have on consumers and the market if they were to happen) and probability (the likelihood of the particular issue occurring).

Answer reference: Section 3.1.1

9. What type of information can be withheld when providing information?

Legally privileged documents and those that may lead to self-incrimination do not have to be provided.

Answer reference: Section 3.1.5

10. What is it called when staff informs a client a SAR is made about them?

When an MLRO makes an SAR, individual staff names are not passed on as part of the process. Staff should not inform the client that a report is being made about them. This is regarded as tipping off

Answer reference: Section 3.1.7



Chapter Three

Managing the Risk of Financial Crime

Section 1

**Money Laundering, Terrorist Financing
and the Standards Required of Firms**

Section 2

Practical Implications

Section 3

**Policies, Procedures and Controls
Required of Firms**

**This syllabus area will provide
approximately 20 of the 100
examinations questions**



1. Money Laundering, Terrorist Financing and the Standards Required of Firms

1.1 The Concept of Money Laundering and Terrorist Financing



3.1.1 Understand the concepts of money laundering and terrorist financing

Financial services firms must reduce the risk that their services are used for money laundering or terrorist financing purposes.

Although these two areas are related, the issues and risks faced by firms differ and so employees need to be aware of both aspects.

Money laundering is related to financial transactions aimed at turning money derived from criminal activities ('dirty money') into money which appears to have been legitimately acquired and which can, therefore, be more easily invested and spent ('clean money').

Money laundering can take many forms, including:



Handling the proceeds of crimes such as theft, fraud and tax evasion



Handling stolen goods



Being directly involved with, or facilitating, the laundering of any criminal property



Criminals investing the proceeds of their crimes in a whole range of financial products

Terrorist financing relates

to the financial support of organisations or groups that seek to perform terrorist acts and also to any financial transactions undertaken to move such money around the globe in order to enable terror attacks to be carried out.

There are similarities between money laundering and the movement of terrorist funds and, because terrorist groups can have links with other criminal activities, there is inevitably some overlap between anti-money laundering (AML) provisions and the rules designed to prevent the financing of terrorist acts. There are two main differences to note:

1. Although the overall funds required may be significant, terrorist financing usually involves small amounts of money, making identification and tracking more difficult.

2. In terrorist financing, the source of funds may be legitimate, thus, making it difficult to identify when the funds become terrorist funds.

The cross-border nature of money laundering and terrorist financing has led to international coordination to ensure that countries have legislation and regulatory processes in place to enable identification and prosecution of those involved.

Examples include:

- The Financial Action Task Force (FATF), which has issued recommendations aimed at setting minimum standards for action in different countries to ensure AML efforts are consistent internationally; it has also issued special recommendations on terrorist financing.
- **European Union (EU) directives** targeted at money laundering prevention.
- Standards issued by international bodies to encourage due diligence procedures to be followed for customer identification.
- Sanctions by the United Nations (UN), United States (US) and the EU to deny individuals and organisations from certain countries access to the financial services sector.
- Guidance issued by the private sector Wolfsberg Group of banks in relation to private banking, correspondent banking and other activities.



1.2 Stages of Money Laundering



3.1.2 Know the stages of the money laundering process: placement; layering; integration

There are three stages to the money laundering operation:

- **Placement** – introduction of dirty money into the financial system. Typically, this involves placing the criminally derived cash into a bank or building society account, a bureau de change or any other type of enterprise which can accept cash, such as a casino, or the conversion of currency into crypto currency.
- **Layering** – involves moving the money around in order to make it difficult for the authorities to link the placed funds with the ultimate beneficiary of the money. This might involve buying and selling foreign currencies, shares or bonds in rapid succession; investing in collective investment schemes; or insurance-based investment products; or moving the money from one country to another.
- **Integration** – at this final stage, the layering has been successful and the ultimate beneficiary appears to be holding legitimate funds (clean money rather than dirty money). The money is regarded as 'integrated' into the legitimate financial system.

Impact on Financial Services Firms

Each of these stages impact financial services firms. During the **placement** stage, the money launderer introduces cash into the financial system. This requires cash in hand to be replaced by some valuable claim on assets or benefits. In recent years, the use of electronic currency (eg, Bitcoin) has raised much interest regarding the disruptive impacts of technology, but should also be considered in the light of money laundering considerations. Any transaction by which someone converts actual currency for an electronic currency could be an example of placement.

For most financial services firms, layering represents the biggest risk – as any transaction that exchanges one asset for another, or changes the registered owners of an asset, could be a step of layering. Because the purpose of layering is to disguise the original source of the money and the eventual end recipient, layering processes will often be protracted and detailed – yet each individual

step will be designed to appear innocent, such as the usual activity of an investor managing their affairs. For this reason, the ability to assess behavioural trends in account activity has become increasingly important.

Where a firm processes many thousands of transactions – each of which seem ordinary – they are investing in systems and procedures that look for patterns or series within the transactional data, such as where an investor might change their bank details or address and shortly afterwards redeem their holding. In many cases, such transactions may still be genuine – but the firm must exercise due care.

Integration can be more difficult to demonstrate, because the cleaned money may not actually be removed from the financial system. The money launderer's purposes are satisfied provided the illegal source of the money can no longer be identified by firms or law enforcement. In some cases, the integration phase may see the criminal making withdrawals from a bank account, while in others, the money may remain invested in some long-term project or investment. The aim of firms is to ensure sufficient records make it more difficult for the criminal to achieve this stage of integration.

1.3 Role of International Agencies



- 3.1.3 Know the role of international agencies in combating money laundering and the financing of terrorism: United Nations Office on Drugs and Crime (UNODC); International Monetary Fund (IMF); World Bank

3.1.4 Know the role of the Financial Action Task Force (FATF) in combating money laundering and terrorist financing; jurisdictions with strategic deficiencies; the challenge of jurisdictional differences

Globally, a number of international agencies actively work to combat money laundering and terrorism financing, each of which has a specific focus dependent on their mandates.

1.3.1 United Nations Office on Drugs and Crime

The UNODC is mandated to assist UN member states in combating illicit drugs, crime and terrorism. In the Millennium Declaration (2000), member states also resolved to intensify efforts to fight transnational crime in all its dimensions, to redouble the efforts to implement the commitment to counter the world drug problem and to take concerted action against international terrorism. Their mandate is defined as follows:

'The Law Enforcement, Organized Crime and Anti-Money-Laundering Unit of UNODC is responsible for carrying out the Global Programme against Money-Laundering, Proceeds of Crime and the Financing of Terrorism, which was established in 1997 in response to the mandate given to UNODC through the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988. The Unit's mandate was strengthened in 1998 by the Political Declaration and the measures for countering money laundering adopted by the General Assembly at its 20th special session, which broadened the scope of the mandate to cover all serious crime, not just drug-related offences.

The broad objective of the Global Programme is to strengthen the ability of member states to implement measures against money laundering and the financing of terrorism and to assist them in

detecting, seizing and confiscating illicit proceeds, as required pursuant to UN instruments and other globally accepted standards, by providing relevant and appropriate technical assistance upon request.'

1.3.2 International Monetary Fund (IMF)

The IMF summarises their work in relation to AML and CFT as follows:

'As a collaborative institution with near-universal membership, the International Monetary Fund (IMF) is a natural forum for sharing information, developing common approaches to issues, and promoting desirable policies and standards – all of which are critical in the fight against money laundering and the financing of terrorism. In addition, the IMF's broad experience in conducting financial sector assessments, providing technical assistance in the financial sector, and exercising surveillance over members' economic systems has been particularly helpful in evaluating countries' compliance with the international anti-money laundering/countering the financing of terrorism (AML/CFT) standard and in developing programmes to help them address identified shortcomings.'

In 2006, the IMF executive board confirmed the general principle that every Financial Sector Assessment Program (FSAP) and Offshore Financial Center (OFC) assessment should incorporate a full AML/CFT assessment. The IMF has been a substantial contributor in this area, by cooperating with the FATF and the FATF-style regional bodies (FSRBs), conducting AML/CFT assessments alongside the FATF's and FSRBs' peer evaluations of their members' compliance with the FATF 40 Recommendations (see section 1.3.4), providing technical assistance, and contributing to policy development and research.

In 2009, a five-year donor-supported trust fund was launched to provide technical assistance in AML/ CFT, which was extended for a further five-year period in 2014. Over the 10-year period, in excess of USD 25 million was provided by a variety of countries including Canada, France, Japan, Korea, Kuwait, Luxembourg, the Netherlands, and the United Kingdom (UK). Many projects were successfully completed.

In 2018, the IMF adopted an AML/CFT strategy which included the identification of emerging areas in the AML/CFT space including FinTech, correspondent banking and transaction laundering. The increased demand for integrity advice and capacity development lead to the goal of at least one or two assessments per year going forward. As part of the strategy, since 2020, IMF staff participate in AML/CFT assessments carried out by other assessor bodies such as FATF-style regional bodies. In 2023, the IMF undertook a review of their AML/CFT strategy which found that since 2018, the coverage of financial integrity has increased across all their workstreams. A wide range of quantitative and qualitative data has been collected and is used to guide the IMF work with member countries. The benefits of incorporating AML/CFT strategy in their overall assessments has proven to be beneficial and will be continued until the next review in five years' time. Going forward, greater focus will be put on the assessment and mitigation of macroeconomic impacts, and a better understanding of the nature and severity of financial integrity risks. The next review of the AML/CFT strategy will be undertaken in 2028.

1.3.3 The World Bank

The World Bank consists of two main components: the International Bank for Reconstruction and Development (IBRD), and the International Development Association (IDA). Both the IBRD and the IDA are involved in supporting developing countries and in the case of the IDA making grants to the poorest countries.

As emerging markets open their markets and financial systems, they experience unpredictable movements of money in and out of their economy. This is attractive to money launderers since it makes it easy to hide any illicit activity[♦]. If left unchecked, this activity will eventually undermine the credibility of the formal financial sector. Although it is the case in any country, the damage to the financial sector and the overall economy is more significant in emerging and developing countries since it reduces trust in the country and thus hinders growth. In its financial sector operations, the World Bank promotes measures to counter the flow of illicit funds into the financial systems of countries and arranges for external assistance. In doing so, the World Bank recognises that measures to prevent and detect money laundering activities cannot focus only on banks. Effective measures must also address the securities, insurance, and money-changing sectors.

The Stolen Asset Recovery Initiative (StAR) is a partnership between the World Bank Group and UNODC that supports international efforts to end safe havens such as Bermuda and the Cayman Islands for corrupt funds. StAR works with developing countries and financial centres to prevent the laundering of the proceeds of corruption and to facilitate a more systematic and timely return of stolen assets to their country of origin. The cost of corruption to developing countries is estimated by the World Economic Forum to be around USD 1.26 trillion through bribery, misappropriation of funds, and other corrupt practices.

1.3.4 Financial Action Task Force (FATF)

The FATF is an intergovernmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The FATF is, therefore, a policy-making body that works to generate the political will necessary to bring about legislative and regulatory reforms in

these areas. Over 200 countries participate in the formulation and implementation of the 40 Recommendations. ♦

The FATF's 40 Recommendations on money laundering and combating terrorist financing set an international standard that can be implemented into national laws and regulations. The Recommendations are continuously reviewed and updated with the recent amendments dating October 2025.

The FATF monitors members' progress in implementing necessary measures, reviews money laundering and terrorist financing techniques and countermeasures, and promotes the adoption and implementation of appropriate measures globally. In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism.

In addition, the FATF:

- sets international standards to combat money laundering and terrorist financing, and provides best practice papers and guidance including implementing a risk-based approach
- assesses and monitors compliance with the FATF standards, and provides a list of non-cooperative countries for use by countries to help apply Recommendation 21 (see below)
- conducts studies of money laundering and terrorist financing methods, trends and techniques, and
- responds to new and emerging threats, such as proliferation financing.

Example: FATF Recommendation 21

Measures to be taken with respect to countries that do not or insufficiently comply with the FATF:

Financial institutions need to give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not, or

insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities. Where such a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate countermeasures.

FATF has published guidance on counter proliferation financing. Proliferation financing refers to the act of providing funds or financial services which are used, in whole or part, for the manufacture, acquisition, possession, development, export, transfer or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes).

The crime of proliferation financing does not require knowledge, intention or negligence. However, when a jurisdiction specifies the responsibilities of financial institutions or a possible criminal offence of proliferation financing, the legal principles governing these two regimes in that jurisdiction will apply, including the roles of knowledge, intention or negligence.

Combating money laundering and terrorist financing on a global scale requires addressing varying differences between jurisdictions' anti-money laundering regimes or frameworks. Criminals may exploit such differences, utilising jurisdictions with potentially weak anti-money laundering controls, for various reasons, including the movement of illicitly-derived funds. Therefore, on a global scale, any global money laundering and terrorist financing measures are 'only as strong as the jurisdiction with the weakest measures', as indicated by the [FATF](#). It is pertinent to note that the FATF categorises jurisdictions with strategic deficiencies into two, being the:

- **High-Risk Jurisdictions subject to a Call for Action (informally referred to as the 'Black List')**

These jurisdictions would have been identified as having substantial deficiencies in their regimes to tackle money laundering, terrorist financing, and proliferation financing. As indicated in this section, any financial association with such jurisdictions would need to be the subject of enhanced due diligence and other counter-measures as applicable.

- **Jurisdictions under Increased Monitoring (informally referred to as the 'Grey List')**

These jurisdictions, together with the FATF, would be working to address identified deficiencies to counter money laundering, terrorist financing, and proliferation financing.

The above jurisdictions would be indicated in statements published by the FATF, at the end of its plenary meetings typically held three times a year (February, June and October). Jurisdictions may be removed from such category lists, once they have addressed their deficiencies or action plans.

1.4 Predicate Offences in Financial Crime



3.1.5 Understand the role of predicate offences in financial crime: fraud; embezzlement; bribery; corruption

According to Article 23 of the United Nations Convention Against Crime (UNCAC), 'laundering of the proceeds of crime' constitutes a criminal offence, when committed intentionally.

Article 23 prohibits:

1.
 - a. 'the conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit

origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action

- b. the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime.

2. Subject to the basic concepts of its legal system:

- a. the acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime
- b. participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.'

A predicate offence is the underlying criminal offence that gives rise to criminal proceeds, which is then the subject of a money laundering charge. Fraud and embezzlement are examples of predicate offences in financial crime and are described in detail below.

Fraud

Fraud is the practice of obtaining value by deceptive means. That value might be obtained in the form of goods or services. This implies that fraud can cover a wide range of illegal activities, such as credit/ debit card fraud. In this type of fraud, criminals purchase goods or services using the stolen or cloned credit/debit card information. This can go unnoticed for long periods if the actual cardholder is not diligent in reviewing their transaction records.

Financial institutions analyse expenditure trends to be able to pick up on potential fraudulent transactions before they are completed.

Larger transactions can also be fraudulent – such as where one party misrepresents their part in a contract.

Securities fraud is a specific type of fraud, where investors are encouraged to enter into investment transactions based on untrue statements about the assets being traded.

Embezzlement

Embezzlement is the act of dishonestly appropriating or secreting assets by one or more individuals to whom such assets have been entrusted. Embezzlement is a kind of financial fraud. For instance, a clerk or cashier handling large sums of money could embezzle cash from their employer, a lawyer could embezzle funds from clients' trust accounts, a financial adviser could embezzle funds from investors, or a spouse/civil partner could embezzle funds from their partner. Embezzlement may range from the very minor in nature, involving only small amounts, to the immense, involving large sums and sophisticated schemes.

More often than not, embezzlement is performed in a manner that is premeditated, systematic and/or methodical, with the explicit intent to conceal the activities from other individuals, usually because it is being done without their knowledge or consent. Often it involves the trusted person embezzling only a small proportion or fraction of the funds received, in an attempt to minimise the risk of detection. If successful, embezzlements can continue for years (or even decades) without detection. It is often only when the funds are needed, or called upon for use, that the victims realise the funds or savings are missing and that they have been deceived by the embezzler.

Bribery

Bribery, a form of corruption, is the giving of money or something else of value, with the intention of influencing the behaviour of the

recipient. Bribery constitutes a crime and is defined by Black's Law Dictionary as:

'The offering, giving, receiving, or soliciting of any item of value to influence the actions of an official or other person in charge of a public or legal duty.'

The bribe is the benefit bestowed to influence the recipient's conduct. It may be any money, good, right in action, property, preferment, privilege, emolument, object of value, advantage, or merely a promise or undertaking to induce or influence the action, vote, or influence of a person in an official or public capacity.

Corruption

Corruption involves the abuse of power and may range from bribery of high foreign officials to secure some type of favourable action by a foreign government to so-called facilitating payments that allegedly were made to ensure that government functionaries discharged certain ministerial or clerical duties. Corruption can also take place within financial firms where, for example, senior officials or executives use their position to obtain bribes for awarding contracts.

1.5 Financial Firms and Crime



3.1.6 Understand how financial services firms may be utilised for financial crime: Ponzi schemes; boiler rooms; money laundering; offshore trusts; beneficial ownership; cybercrime

By choosing to invest in financial services products, an investor accepts certain risks. However, where the product or service has not been designed with the investor's best interests at heart, they will be exposed to greater risk of loss than they expect. In some cases, an unscrupulous firm or individual might set up a product designed

to further their own self-interest rather than to provide a transparent and honest opportunity for investment returns.

Ponzi Schemes

The term 'Ponzi scheme' is used to describe a financial services product that claims a level of investment return that is not supported by the investment activity undertaken. The shortfall between the returns generated and those claimed is made up by using the money of new investors, who have been attracted to the scheme by the high headline returns being publicised. One of the most well-known Ponzi schemes in recent history is the Madoff investment scandal discovered late 2008 in which new investments were used to pay out high returns to existing investors. The size of the fraud was estimated to be in excess of US\$65 billion. At the end of 2024, the Madoff Victim Fund, a US government initiative aimed at compensating the victims, made their final payment as a result of which the victims have recovered close to 94% of their losses.

For a short time period, Ponzi schemes can be sustained – provided sufficient new money is received to cover the returns being paid to older investors. However, as this new money is paid out to earlier investors it is not, therefore, put to any investment purpose; the scheme builds up a substantial unpayable debt to its clients.

At some point there will be insufficient new money to sustain the false profits, and the scheme will collapse – resulting in losses for those investors that unfortunately joined the scheme too late. Financial services practitioners – particularly those with successful, market-leading products – must, therefore, guard their motivations. A successful honest product may become a Ponzi scheme if those running it become dependent on the fame of their success, or the fees it provides, and sacrifice their integrity to sustain high performance rates regardless of current market conditions.

Financial services firms must, therefore, be aware of any products they offer which appear to be providing excessive returns and ensure that the firm has not become host to a Ponzi scheme.

Similarly, firms acting on behalf of their clients should ensure they perform solid due diligence reviews of any products recommended/supported to reduce the risk of their clients becoming victims of a Ponzi scheme. Warning signs might include an investment approach that the scheme cannot explain or guaranteed/high rates of return at little investment risk.

Boiler Rooms

'Boiler room' scams involve fraudsters selling customers overvalued, if not worthless, securities by means of an intensive selling campaign through numerous salespeople via the internet, messaging systems, telephone or direct mail. They do not consider the suitability or the needs of the customer, and the sales tactics used are designed to induce a hasty decision to buy the securities being offered, without disclosure of the material facts about the issuer (hence the name 'boiler room' because of the high-pressure selling tactics). Modern techniques include the use of internet bulletin boards to promote certain securities and entice buyers.

Money Laundering

As detailed in section 1.2, financial firms are likely to be used predominantly in the first two stages of money laundering. Banks are among the firms likely to be recipients of cash, ie, the placement stage. Other firms, such as fund managers or stockbrokers, may be used in the layering stage where the criminals are attempting to disguise the origins of the dirty money by placing layers of transactions between the original deposit and the ultimate receipt of 'clean' money from the redemption of any investments. This clean money will then be used to invest in legitimate businesses which may or may not include financial firms.

Fines that relate to money laundering include the following:

- **July 2023** – the US Federal Reserve fined Deutsche Bank \$186 million for failing to sufficiently address money laundering control problems and other shortcomings.

- **December 2021** – HSBC was fined £64 million by the Financial Conduct Authority (FCA) in the UK for failings in their AML process.
- **June 2020** – Commerzbank AG was fined £37 million by the UK FCA for failures in AML systems and controls.
- **April 2019** – Standard Chartered Bank was fined £102 million by the UK FCA for failures in AML controls in their wholesale correspondent banking business and branches in the UAE. In addition, the bank reached a settlement of \$1.1 billion with the US Treasury for various violations.

Money laundering and cyber crime (see below) are closely linked as rapid advances in technology used in the financial sector are used as opportunities by money launderers.

Offshore Trusts

A trust is an agreement whereby assets are donated by one person (the donor or settlor) for the benefit of another (the beneficiary) with a third party acting in the interests of the beneficiary until the assets completely become the property of the beneficiary. An offshore trust is such an arrangement located in a different jurisdiction – usually in order to benefit from the taxation regime there, or some other feature. The use of an offshore trust is not criminal or suggestive that any impropriety exists.

In most cases, the identities and relationships between the parties are clear, though in some cases, the trust might be established such that the identity of the beneficiaries is not stated. Such models are referred to as ‘orphan structures’, and the use of orphan models might be used to disguise the chain of ownership for certain assets – either because the assets have dubious origins or because the beneficiary is trying to evade tax.

Some offshore trusts, offshore companies, trusts and financial institutions situated in certain financial centres, are used by criminals to hide origins or owners of funds. However, with the greater international focus on fighting financial crime, beneficial

ownership regimes are being introduced that aim to improve transparency and remove anonymity. For example, the Trust Register is a UK initiative that requires offshore trusts with a UK tax liability, and certain non-UK trusts, to be registered. Any trustee who fails to register a trust within the required time frame, or registers late, can be personally liable for a penalty of £5,000 per offence.

For example, where it was previously easy for offshore trusts to be used in the layering process of money laundering by moving monies around different accounts; breaking the proceeds down into different amounts and utilising numbered accounts and/or offshore companies with ownership hidden by offshore trusts, **nominee** directors or bearer shares, the mandatory registration of trusts makes this significantly more difficult.

Although offshore trusts may be used by people for legitimate tax planning, ie, minimising an individual's or family's tax liability within the tax regulations relating to their country of residence and the offshore centre, such trusts may also be used for tax evasion. While tax avoidance is legal, tax evasion is a crime and any suspicion is reportable as with any financial crime. See section 1.3.7 on tax evasion and tax avoidance.

Beneficial Ownership

According to FATF, the beneficial owner is the natural person or persons who ultimately own or control an asset and/or on whose behalf a transaction is being conducted. Beneficial owners include those persons who have ultimate effective control over a legal person or arrangement. In order to ensure the firm is not subject to financial crime, it is important to know who the beneficial owner of a transaction is. Know your customer (KYC) processes play an important role in assessing the ownership structure of the client and the ultimate beneficial owner. Knowing beneficial owners is important to ensure the financial institutions are able to identify Politically Exposed Persons (PEP), whether a customer is subject to sanctions, or may in any way expose the institution to increased risk.

Not knowing the ultimate beneficial owner may enable perpetrators to hide their involvement and hence their activities and hence expose the financial institution to be used to enable criminal activity.

The Customer Due Diligence (CDD) Rule measures to identify and verify that customers are who they say they are include an expectation for financial institutions to establish and maintain written procedures that are reasonably designed to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions. These procedures must enable the institution to identify the beneficial owners of each customer at the time a new account is opened, unless the customer is otherwise excluded, or the account is exempted. In cases of high-risk clients and significant financial transactions Enhanced Due Diligence (EDD) has to be undertaken which requires a firm to obtain additional identifying information, using intelligence reports, verification of the source of cash or wealth, and to obtain additional information on the nature and purpose of the business relationship.

Cybercrime and Crypto Assets

Cybercrime refers to the use of computers for illegal means such as fraud, trafficking, identity theft and violating privacy. The increase in the use of computers has resulted in a global increase in cybercrime in which criminals seek to exploit human or security vulnerabilities to steal passwords, data or money. The most common forms of cybercrime are:

- **Hacking** – including social media and passwords.
- **Phishing** – fake emails asking for security information and personal details.
- **Vishing** – fraudulent callers try to extract identifying details to use in perpetrating another crime.
- **Malicious software** – including ransomware.
- **Distributed denial of service attacks (DDoS)** – ensuring a website becomes unreachable.

The scale and complexity is wide-ranging and can vary from a poorly executed email pretending to be from the bank hoping the recipient will click the link and leave their bank details to complex operations such as cryptomining malware attacking digital currencies. Cybercrime is becoming more and more sophisticated.

Cybercrime is global, and is for a large part, undertaken by email. The annual cost for 2019 was estimated to be in excess of USD 3.5 billion, which has risen to in excess of \$5 billion in 2023, and USD\$1.2 trillion in 2025[♦]. The rise between 2019 and 2023 was in part the result of the increased vulnerabilities associated with home working during the coronavirus (COVID-19) pandemic. The cost of cybercrime is not just related to the direct financial losses, but also includes business downtime, brand reputation, economic disruption, and insurance claims and increases in premium.

Although types of cybercrime have been added to laws in many countries, the criminal justice system in most countries is not yet up to date with the severity of the crimes. In the UK, for example, the conviction rate for hacking between 2008 and 2018 was close to 90% of prosecutions resulting in convictions. The penalty when convicted, however, is low with most convictions being given conditional discharges or community service[♦]. However, since then fraud and computer misuse offences have increased substantially[♦].

Cybercrime, in particular ransomware, often involves crypto assets. These assets are a digital representation of a value that can be transferred, stored, or traded electronically and include cryptocurrencies and non-fungible tokens. In the context of financial crime, it is worth noting that crypto assets are, because of their lack of regulation, often used for illegitimate purposes.



1.6 Misstatement of Financial Circumstances



3.1.7 Understand how a firm or its representatives may collude in the propagation of financial crime: misstatement of financial circumstances; corporate fraud

A misstatement is defined as a difference between the amount, classification, presentation, or disclosure of a reported financial statement item and what is required for the item to be in accordance with the applicable financial reporting framework.

Accordingly, a material misstatement of the financial statements may arise in relation to:

1. the appropriateness of the selected accounting policies
2. the application of the selected accounting policies, or
3. the appropriateness or adequacy of disclosures in the financial statements.

Misstatements in financial statements can arise from a fraud or error. The difference between them is that the former is intentional.

Errors may be detected by auditors, and fraud perpetrated by an employee can be detected – subject to relevant controls being in place.

Typical objectives for fraudulent misstatements are:

- **earnings management** – where there is pressure to meet market expectations, minimise tax or inflate earnings to secure bank finance
- **misappropriation of assets** – eg, embezzling receipts through collections accounts, diverting write-offs to personal bank accounts
- **payments for goods not received** – payments may be made to fictitious vendors, or kickbacks received, and

- **using entity's assets** – for personal use, eg, as collateral for a loan.

Where the firm or multiple individuals collude, it is more difficult to detect misstatements of financial positions. It is difficult to detect frauds where two or more employees collude, and even more so where management is involved.

Fraud is the use of deception to obtain goods or services, and is a criminal offence in many jurisdictions. As fraud is an illegal action, it follows that any money received as a result of fraud represents proceeds of financial crime.

Fraud can be both internal and external. Internal fraud is committed by someone within the organisation against the organisation. External fraud is committed by someone from outside the organisation.

Corporate Fraud

Corporate fraud arises when an organisation adopts such deceptive means as part of running its business. We have already seen that a firm running a Ponzi scheme (see section 1.3.5) will lie to its clients about the use to which their money has been put. However, there are other types of fraud that a company might commit.

The bookkeeping of the firm is often key to corporate fraud events. The money or assets of an investor might be misused (eg, transferred to the company to support its statement of financial position), or the money may be embezzled by an unscrupulous employee. The company's financial accounts might be misstated so that the company's share price remains higher based on the inaccurate information released to the market. This may include deceiving the external auditor, so the deception remains undetected.

This century has already witnessed some substantial corporate frauds, which have illustrated the need for all market participants to beware of any firm that seems to be generating unnatural profit

levels in comparison with similar organisations. Some examples of corporate fraud are summarised below:

- **Enron Energy** – the US energy company failed in 2001, in the light of multiple accounting irregularities which had maintained an artificially high share price. Two of Enron's chief executive officers (Kenneth Lay and Jeffrey Skilling) were each convicted of multiple charges – including conspiracy, securities fraud, false statements, and insider trading. They had each sold substantial shareholdings in the company in the period shortly before the accounting frauds became known. Audit firm Arthur Anderson faced much scrutiny for its role in the scandal. A corporate conviction for obstruction of justice (relating to the shredding of Enron-related documentation) effectively prevented the firm from practising and the firm was disbanded (even though the criminal conviction was overturned in 2005).
- **Lehman Brothers** – the fourth largest investment bank in the US filed for Chapter 11 bankruptcy on 15 September 2008. The company experienced substantial losses from the sub-prime mortgage crisis, owing to the level of gearing now understood as being built into such mortgage products. In the aftermath, executives faced challenges over the earnings they had made during the period in which the firm was failing. The company's auditors were charged by state prosecutors about the accuracy of the financial accounts they approved. No significant convictions followed.
- **Goldman Sachs** – in 2010, the Securities and Exchange Commission (SEC) charged Goldman Sachs with fraud in respect of some sub-prime mortgage-related securities. Goldman Sachs created a portfolio of mortgage-backed investments and sold an interest in that portfolio to a number of investors. However, what Goldman Sachs did not disclose to the investors is that the portfolio had been assembled in conjunction with a substantial client of the firm, John Paulson,

and that he would then trade in the expectation that the portfolio would reduce in value rather than grow. Effectively, Goldman Sachs enticed investors who would lose their money to Paulson, without disclosing that it had a corporate interest on both sides of the transaction.

- **Steinhoff International** – an international retail holding company in the furniture and household goods business overstated profits for eight years (2009–17) by a total amount of \$7.4 billion. The accounting fraud involved a small group of executives and outsiders entering into a transaction that substantially inflated the group's profit and asset values. Although Steinhoff first disclosed irregularities in 2017, the fraud was not revealed until 2019. Legal proceedings were instigated against four executives in Germany, and the assets of the CEO were seized. A number of civil suits were lodged against Steinhoff International in Germany, South Africa, and the Netherlands. Steinhoff International was liquidated on 13 October 2023.
- **Patisserie Valerie** – a UK-based patisserie reported significant and potentially fraudulent accounting irregularities requiring an immediate capital injection of £20 million. The firm's finance chief was suspended and arrested on suspicion of fraud having opened secret overdraft facilities totalling almost £10 million. Patisserie Valerie's market capitalisation dropped from £446 million to £68 million in a period of two weeks. Accounting firm Grant Thornton has been fined £2.3 million for failures in their audits of Patisserie Valerie. On 10 October 2023, the ex-CFO appeared in court on fraud charges. A trial date is set for spring 2026. Patisserie Valerie has restarted and as of mid 2026 had more than 90 outlets.
- **Wirecard AG** – a fully licensed German bank providing payment services filed for insolvency in June 2020 after disclosing that approximately €1.9 billion was missing. The missing funds are mainly attributed to balance sheet irregularities and inflated profits, a practice rumoured to have

started in 2008. In November 2020, the assets of the main business unit were sold to Santander.

These cases illustrate not only the potential scale of fraud that can arise, but also the way that discovery of such cases can impact other market participants. It is vital that firms ensure their governance structures are sufficiently robust to protect against becoming victims of fraudulent activity.

1.7 Tax Evasion and Tax Avoidance



3.1.8 Know the concepts of facilitation of tax evasion and tax avoidance

Tax avoidance is the use of legally permissible methods to reduce the amount of tax owed. This is generally achieved by claiming permissible deductions, credits and allowances. Tax avoidance is legal and includes aspects, such as transferring assets between spouses, or making pension contributions in order to reduce the level of income that remains subject to income tax. Tax avoidance is enabled by the complexity built into the taxation system, as such complexity can allow individuals to identify legal loopholes and exemptions by which certain monies do not give rise to tax liabilities.

Tax evasion, however, is an illegal practice where a person, organisation, or corporation intentionally avoids paying part or all of their tax liability. Examples might include not paying income tax or VAT when working for 'cash in hand'. Tax evasion would also arise if the capital gains made on investments were not correctly disclosed for taxation calculation. Although the difference between tax evasion and tax avoidance is clear, there is a grey area referred to as 'tax-aggressive strategies'. Most developed countries have what are known as general anti-avoidance rules (GAAR) prohibiting tax-

aggressive avoidance. The objective of these rules is to deter taxpayers from using arrangements for the purpose of tax avoidance and includes international tax arrangements. It does not prohibit the offering of specific products or services, but includes safeguards to ensure any reasonable choice of a course of action is not targeted.

1.8 Dual Criminality, Extradition and Mutual Legal Assistance



3.1.9 Know the concepts of dual criminality, extradition and mutual legal assistance

Extradition law is an amalgamation of international and domestic law that sets the structure for an individual living in one country to stand trial in another. Generally, extradition is only supported in conditions of dual criminality, which is also known as double criminality. In this case, the allegation relates to an action that constitutes a crime in both the country where a suspect is being held and the country asking for the suspect to be handed over or transferred to stand trial. In other words, a crime in one country has to also be a crime in the country extraditing the individual in question.

Cases of extradition can involve a combination of legal arguments and diplomacy, and can prove controversial. Consider the cases of 'The NatWest Three' (also known as the Enron Three) and Gary McKinnon. The NatWest Three were three businessmen extradited to Texas on counts of fraud as part of the Enron scandal. Gary McKinnon was a Scottish systems administrator accused of hacking thousands of government computers in 2002. Both cases raised questions of political balance within extradition arrangements between the UK and the US.

Under an OECD convention, each country has to provide prompt and effective legal assistance to other countries in criminal investigations and proceedings brought by a country. This mutual assistance is required for offences that fall within the scope of the convention, and for non-criminal proceedings within the scope of the convention brought by a country against a legal person. The country receiving the request shall inform the country making the request, of any additional information or documents needed to support the request for assistance without delay and if asked, of the status and outcome of the request for assistance.

Where a country makes mutual legal assistance conditional upon the existence of dual criminality, it shall be deemed to exist if the offence for which the assistance is sought is within the scope of this OECD convention. A country shall not decline mutual legal assistance for criminal matters within the scope of the convention on the grounds of bank secrecy.

2. Practical Implications



- 3.2.1 Understand how external financial crime issues may impact on a firm: reputational; systemically; counterparty risk; unreliable market valuations
 - 3.2.2 Understand how financial crime may directly impact a firm: theft of data; theft of assets
-

2.1 Impact of Financial Crime on Firms

Financial crime can impact a firm in various ways. If a specific crime becomes public knowledge, any firms directly connected with the crime face reputational damage. A previously respected company name can become synonymous with fraud or poor governance, reducing the potential for the firm to gain further clients and retain the business it already holds. The company's reputation will also be impacted if its regulator imposes a public penalty upon it – such as a regulatory fine or reprimand. For example, if a regulator fines a company for failing to satisfy AML rules, other clients may wish to move their affairs to a more respectable firm.

Firms can also be impacted by events taking place in other parts of the industry – even if they have no direct involvement in those events. Financial crime poses a systemic risk for the industry: the risk of collapse of an entire financial system or entire market, as opposed to risk associated with any one individual entity, group or component of a system. Such risks can lead to instability in the financial system with the outcome for one firm being potentially exacerbated by the action or inaction of other financial intermediaries. Because of interdependencies in a system or market, the failure of a single firm or group can cause a cascading failure, which could potentially bankrupt or bring down the entire system or market.

The Madoff Ponzi scheme is an example of such a crime which led to huge losses across the market. The malfeasance at Lehman Brothers prompted a global financial crisis with unprecedented support from governments being needed to prevent the banking system from collapsing. The impact of the global financial crisis on the reputation of, and trust in, financial institutions has been significant, and is still noticeable, even though there has been substantial regulatory reform.

The market requires participants to have trust in each other – even if that trust is built on regulatory obligations and a fear of sanction. The potential that a firm may be unable to deliver on its promises to another is known as counterparty risk or default risk. It is unusual for a firm not to honour its obligations on a financial transaction. However, the risk of such failure is increased significantly where financial crime may be a contributing factor. The inability of the counterparty to meet a claim may be the result of financial crime, including fraud, market abuse and misstatements.

Firms can also face unreliable market valuations which may lead to securities being over or undervalued as a result of market abuse and misstatements, for example, by giving out false information about an investment that makes the value seem higher or lower than it really is. In December 2022, the FCA published a decision notice

against three bond traders who were accused of placing large misleading orders for futures that they did not intend to execute thus giving a misleading impression as to the supply of and demand for these futures.

2.2 Impact of Financial Crime on Customers

One of the downsides to the rapid development of electronic communications is the portability of data in large quantities, using the internet or small storage devices. Increasingly sophisticated criminals are targeting financial service companies to steal the data they hold on customers, such as their personal details, names, addresses, bank details and passwords.

The data a firm holds about its customers are attractive to those attempting, for example, account takeover and credit card fraud.

There are many ways that criminals can target financial firms with a view to stealing data, including:

- infiltrating firms and placing people as employees who download data onto USB sticks
- theft of computers, laptops and data files on tape or disk
- hacking into systems, breaching firewalls and other security systems, using logger tools to gather data, and
- social engineering, deceiving call centre associates into providing information unwittingly.

Once criminals have a customer's personal details, including bank accounts and investments, they can attempt the theft of the customer's assets. They may take over the accounts of their victims, impersonating the customer to instruct a change of address or bank account details. Having usurped the original customer, the criminal will instruct the sale of assets, and have the proceeds sent to the address/bank account they control. This is often a fraudulently opened bank account, to ensure the account owner name will

match the name on the redemption cheque. The criminal then withdraws the cash and absconds with the proceeds. The financial firm may be left with an angry customer and, depending on the circumstances, may have to compensate its customer and reinstate their accounts.

Firms can be subject to asset thefts too. This may be as a result of account takeover, or other fraudulent activity which may be internal or external to the firm. For example, forged transfer of assets and forged sale instructions. This may involve proceeds being directed to bank accounts set up by the fraudsters specifically for the purpose of laundering the proceeds. In some cases, the amounts involved can be very significant.

The impact of such thefts can include:

- reduced profits and potential risks to the financial stability of the firm
- damage to the firm's reputation, which may arise from supervisory or other regulatory action, such as fines
- increased costs arising from investigation of theft, forensic work by expert or specialist firms and remediation where required such as new systems and controls, and
- increased insurance costs following revised premiums based on recent claim experience, or the need to take out additional insurance cover where perhaps the risk had not previously been identified.

2.3 Firms' Responsibilities for Financial Crime Prevention



3.2.3 Understand the responsibilities of directors and senior management in relation to anti-money laundering (AML), combating financial crime (CFC) and anti-corruption (AC) initiatives

The directors and senior management of an authorised financial firm are expected to:

- identify, and manage effectively, the risks in their businesses including ensuring appropriate action is taken in relation to CFT, AML, combating financial crime (CFC) and anti-corruption (AC)
- appoint a **nominated officer** to process disclosures
- appoint an MLRO with certain responsibilities
- ensure the MLRO has adequate resources devoted to AML/CFT, and
- understand the potential personal liability if legal obligations are not met.

Accordingly, the directors and senior management will ensure the policies and procedures established include systems and controls that:

1. enable the firm to identify, assess, monitor and manage money laundering risk, and
2. are comprehensive and proportionate to the nature, scale and complexity of its activities.

2.3.1 Anti-Money Laundering (AML)

In many respects, compliance with AML is an integral part of the overall compliance requirements of the regulated sector. The expectation is that senior management are aware of and take responsibility for all compliance activity within their institution. This

is embodied through senior management being able to provide evidence of having adequate systems and control procedures in place, which should be tested to prove effectiveness. These general compliance requirements obviously also apply to AML and related initiatives. Indeed, there is plenty of evidence of banks having been fined by regulators for failure to meet these requirements.

It is generally expected that senior management establishes the AML policy, setting out how the organisation will comply with the legal and regulatory AML regime; it will set out the reporting framework with the various responsibilities and accountabilities of the employees and management. The internal information systems will set out the application of the risk-based approach and how it is interpreted together with the client and transaction monitoring, record-keeping and reporting criteria.

2.3.2 Combating Financial Crime (CFC)

International efforts to combat financial crime have focused on a number of objectives to:

- reduce financial crime and deter the use of financial systems to commit financial crime
- ensure that firms have in place policies and procedures designed to minimise the risk that the firms' businesses may be used as a vehicle for money laundering and other financial crime
- raise consumer awareness of financial crime issues
- contribute to an effective wider fight against crime through international cooperation
- encourage a balanced, joined-up approach to AML and fraud through standards and guidance
- improve the effective use of regulator resources through risk assessment processes, and
- improve coordination with partner agencies.

The expectation is that businesses are aware of the risk, have appropriate measures to prevent, detect and monitor financial crime, and provide adequate resources to do so – and that:

- trade associations work together closely and provide leadership over fraud management
- senior managers accept that fraud is a significant threat that needs managing strategically and effectively
- more work is done on the risks and scale of fraud and better ways of tackling it, and
- improved organisational cultures and information sharing are developed.

This means that, using a risk-based approach, regulators will be looking for evidence of:

- a strong anti-fraud culture, with the lead being given from the top
- a clear allocation of responsibility for the day-to-day management of the risk
- satisfactory staff training
- robust **Know Your Customer (KYC)** procedures, and how the firm identifies potential criminal behaviour, and
- what management information on fraud is captured and how it is used.

Regulators will be looking for 'reasonable steps' to be aware of, and tackle fraud risks by being able to identify and report on the following:

- Who is responsible for managing fraud risks?
- How many frauds has the firm suffered recently?
- What are fraud losses?
- What **whistleblowing** arrangements are in place and how successful are they?
- How much is spent on preventing and detecting fraud?

- How does the firm monitor the effectiveness of fraud systems and controls?
- What information on fraud goes to the board or senior management?

Regulators have an important role as gatekeeper of those working in regulated businesses (granting authorisation to firms and those individuals seeking to perform **controlled functions**), and another role ensuring that the expected standards of behaviour and practice are met.

Regulators monitor firms and individuals to ensure risks are appropriately managed and fraudulent activity reported, confirming that businesses have the systems and controls to meet various legislative requirements in place. This will include looking at IT and manual systems, separation of duties within a firm, the role of internal audit, risk assessment, mitigation and monitoring programmes, documented policies and procedures, organisational cultures, collection and use of internal information, and reforms following frauds.

2.3.3 Anti-Corruption Initiatives

Corruption and bribery are harmful for business and form important barriers to investment growth. The development of anti-corruption systems, policies and procedures can help prevent corruption. In order to be effective, organisations must commit to an anti-corruption programme from the board down to senior management and lower levels of the organisations. Policies must be put in place and acted upon, with regular monitoring being an integral part of the plan. The UN launched a call for action in 2014, urging governments to introduce anti-corruption measures and good governance as fundamental pillars of a sustainable and inclusive global economy, and that included anti-corruption initiatives in the UN Sustainable Development Goals (SDGs). The overarching goal behind the SDGs is to 'leave no one behind'. To this

end, 17 goals have been defined which include no poverty, zero hunger, reduced inequalities, and peace, justice, and strong institutions. Anti-corruption activities cut across many of the goals.

2.4 Identifying Money Laundering



3.2.5 Understand the implications of using a risk-based approach to identifying money laundering

Many types of transactions can potentially conceal money laundering activity – particularly as the layering stage may feature multiple normal transactions in order to obscure the audit trail. To perform a full set of AML checks on every transaction undertaken would impose a significant cost upon the industry. Given the importance of trust to the financial services sector, it is important that firms also appear to trust their clients – rather than performing intrusive identity checks on transactions of trivial value. To help balance this difficulty, the FATF Recommendations note that a risk-based approach to the identification of money laundering is acceptable.

When adopting a risk-based approach, competent authorities and financial institutions must first determine which activities are most likely to conceal money laundering efforts, and also determine how the suspicious nature of such transactions might be revealed.

For example, firms that accept physical cash from clients will generally be considered as higher-risk, as these businesses offer a means for ‘dirty money’ to find its way into the financial system. In other cases, a minimum value threshold might be applied, below which the firm need only perform limited scrutiny.

Some types of savings and investment products may be determined as being intrinsically lower-risk in terms of potential money laundering activity (eg, a pension scheme, if an investor’s money

cannot be withdrawn in the short term without incurring a tax charge). In some cases, the firm might be able to accept a certificate from another regulated firm – confirming that the earlier firm has already completed full client identification checks on a mutual client.

The rules recognise the potential that such mechanisms could mean that some cases of abuse are not identified, but that major abuses should still be captured, and that each firm must still ensure that its staff are sufficiently trained to identify any suspicious activity taking place.

2.5 Prevention of Money Laundering



3.2.4 Understand the role of the Money Laundering Reporting Officer (or equivalent) in relation to financial crime

3.2.6 Know the measures firms can adopt to inhibit the likelihood of financial crime

Firms must develop and implement a set of measures that are relevant to the type of business it performs, and sufficient to deliver a risk-based control over potential financial crime activity impacting its business. Some of these measures will be structural (eg, ensuring all relevant staff are sufficiently trained to understand the ways in which financial crime could affect the company), while other measures will apply when processing specific transactions.

A firm must carry out a regular assessment of the adequacy of the systems and controls to ensure that it continues to comply with relevant regulations and relevant legal requirements. In identifying its money laundering risk and establishing the nature of these systems and controls, a firm should consider a range of factors, including:

- its customers, products and activity profiles
- its distribution channels
- the complexity and volume of its transactions
- its processes and systems, and
- its operating environment.

Systems and controls must include:

- appropriate training for its employees in relation to money laundering with frequent updated training depending on the risk level of the institution. Typically, firms at high risk of money laundering will require its employees to undertake refresher training at least annually, and firms with low risk typically every two years
- appropriate provision of information to its governing body and senior management, including a report at least annually by that firm's MLRO, or another responsible senior executive, on the operation and effectiveness of those systems and controls
- appropriate documentation of its risk management policies and risk profile in relation to money laundering and other financial crime, including documentation of its application of those policies
- appropriate measures to ensure that procedures for identification of new customers do not unreasonably deny access to its services to potential customers who cannot reasonably be expected to produce detailed evidence of identity, and
- appropriate measures to ensure that money laundering and other financial crime risk is taken into account in its day-to-day operations, including in relation to:
 - the development of new products
 - the taking on of new customers
 - changes in its business profile.

A firm should allocate to a director or senior manager (who may also be the MLRO) overall responsibility within the firm for the establishment and maintenance of effective AML systems and controls.

2.5.1 Money Laundering Reporting Officer (MLRO)

The MLRO is responsible for oversight of the firm's compliance with the regulator's rules on systems and controls against money laundering. It is the MLRO's role to be aware of any suspicious activity in the business that might be linked to money laundering or terrorist financing, and if necessary, to report it. The firm should ensure that its MLRO has a level of authority and independence within the firm, and access to resources and information sufficient to enable them to carry out that responsibility. It is a senior role, sometimes referred to as a 'nominated officer', and the incumbent should report at a senior level and be able to take precedence over business lines operating, for example, in an international context. MLROs are usually responsible for:

- receiving reports of suspicious activity from any employee in the business
- considering all reports and evaluating whether there is – or seems to be – any evidence of money laundering or terrorist financing
- reporting any suspicious activity or transaction to the appropriate law enforcement agency (LEA) by completing and submitting a suspicious activity report (SAR), and
- asking the LEA for consent to continue with any transactions that they have reported and making sure that no transactions are continued illegally.

The firm might decide to make the MLRO responsible for other tasks that need to be done to make sure the business complies with

money laundering regulations. For example, they could be made responsible for:

- putting in place and operating AML controls and procedures
- carrying out money laundering risk assessments
- record-keeping, and
- training staff in preventing money laundering.

2.6 How Individuals Can Protect Themselves



3.2.7 Know the measures individuals can adopt to inhibit the likelihood of financial crime

Individuals can do a number of things themselves to reduce the likelihood that they would be a victim of financial crime. They should:

- keep personal information secure and if disposing of financial/bank statements, use a shredder to shred the statements before disposal
- keep payment cards in a secure place
- keep documents safe
- keep passwords and PIN secure
- check the qualification and authorised status of any financial adviser
- be aware of scams such as phishing, call and text schemes, and
- remember that if an investment sounds too good to be true, it probably is.

Email scams, for example, tend to come from known institutions such as the tax authority or a bank stating the recipient needs to urgently verify their personal details via a link provided. This link

goes to a fraudulent website via which criminals obtain all information needed to access the accounts of the target.

2.7 Sanctions Checking and Politically Exposed Persons (PEPs)



3.2.8 Understand the rationale behind sanctions screening

2.7.1 Sanctions Checking

Where an individual, company, organisation, or even government is considered to have acted illegally, it is possible for the rest of the global community to take action against that abuse. One mechanism by which such action might be taken is the use of financial sanctions. The range of sanctions can vary from comprehensive financial and trade sanctions to more targeted measures, such as arms embargoes, travel bans, financial or diplomatic restrictions.

Financial sanctions prevent the use and movement of monies relating to certain individuals or organisations considered by the international community to be unfit (usually because of an association with criminal or terrorist activity). In this way, those committing illegal actions should not be able to benefit financially from those actions – which should, in theory, reduce the motivation to commit those abuses.

Organisations such as the UN as well as governments maintain sanctions lists, and financial services firms should seek to minimise the risk that they are servicing customers who are subject to financial sanctions. In some countries (such as the UK, EU and US), legal sanctions are imposed on firms or individuals found to have breached financial sanctions. Aside from any legal penalties, failure

to recognise such cases exposes the firm to reputational risk. For example, if a firm is found to have indirectly supported terrorism, this may result in other people not doing business with that firm.

Firms should have processes to manage the risk of conducting business with, or on behalf of, individuals and entities on the sanctions lists. Some countries provide a consolidated list, which typically includes all the names of sanctioned persons and entities under the UN and, for example, EU sanctions regimes which have effect in the country concerned. Firms should consider screening their customers and transactions on a periodic and/or ongoing basis because names of countries, individuals and groups on a sanctions list may change over time with names added to and removed from the list.

The international frameworks for financial sanctions do not prescribe the processes which firms have to adopt to achieve compliance with their legal obligations. The guidance below is intended to provide an indication of the types of controls and processes that firms might adopt in order to enable them to comply with sanctions obligations in an effective and proportionate manner.

The scope and complexity of the screening process will be influenced by the firm's business activities, and according to the profile of the firm. An effective screening process should include the following elements:

- it should flag up potential name matches against the consolidated list and names against which measures have been issued, for example, in the UK under the Counter-Terrorism Act
- potential matches should be reviewed by appropriately trained staff
- where matches are confirmed as true, appropriate action should be taken to freeze the account

- true matches should be reported as soon as is practicable to the relevant LEA or government department, and
- the firm should maintain an audit trail of actions around potential and true matches.

Many firms use automated customer screening software provided by a commercial provider; other firms rely on manual screening. Firms may consider whether and what type of screening software to use in line with the nature, size and risk profile of their business. A key element of a screening system is that it will flag potential matches clearly and prominently. Firms should document the reasons for choosing the screening method they decide to use.

Where commercially available automated screening software is implemented, firms should understand its capabilities and limits, and make sure it is tailored to their business requirements, data requirements and risk profile. Firms should also monitor the ongoing effectiveness of automated systems. Where automated screening software is used, firms should be satisfied that they have adequate contingency arrangements should the software fail and should periodically check the software is working as they expect it to.

It is important to consider 'fuzzy matching', which is a term used to describe partial or potential matches. Some software solutions identify possible matches where data – in official lists or in firms' internal records – is misspelled, incomplete, or missing. They are often tolerant of multinational and linguistic differences in spelling, formats for dates of birth, and similar data. A sophisticated system will have a variety of settings, enabling greater or less fuzziness in the matching process, as appropriate to the risk profile of the business. In March 2015, PayPal was fined \$7.7 million after the US Treasury Department found it had failed to adequately screen and prevent transactions to users in the sanctioned countries (Iran, Cuba and Sudan).

The generation and resolution of an undue number of false positives may have a negative impact on the efficacy of the resolution process. Firms should, therefore, consider the level of appropriate human intervention to assess which results may be false positives.

All customers should be screened during the establishment of a business relationship or as soon as possible after the business relationship has commenced. Firms should be aware of the risks associated with screening customers after a business relationship has been established and/or services have been provided, ie, that they may transact with a sanctioned party in breach of sanctions prohibitions. Firms must be aware of the absolute restrictions embedded in the financial sanctions regime. Where there is any delay in screening, firms risk breaching the legislation.

As noted in section 1.3.5, firm must apply enhanced due diligence (EDD) measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. As part of this, a firm may conclude, under its risk-based approach, that the standard evidence of identity is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer. EDD applies, for example, in the event the customer is not physically present or is a **politically exposed person (PEP)**.

As part of a risk-based approach, therefore, firms may need to hold sufficient information about the circumstances and business of their customers for two principal reasons:

- To inform their risk assessment process, and thus manage their ML/TF risks effectively.
- To provide a basis for monitoring customer activity and transactions, thus increasing the likelihood that they will detect the use of their products and services for ML and TF.

2.7.2 OFAC Sanctions

The Office of Foreign Asset Control (OFAC) is part of the US Department of the Treasury and acts under presidential national emergency powers, as well as the authority granted to it by specific legislation. OFAC has the right to impose controls on transactions and to freeze assets under US law. OFAC is responsible for the administration of the specially designated nationals (SDN) list which contains individuals and organisations with whom US citizens and permanent residents, regardless of where they are based in the world, are prohibited from transacting and doing business with. In addition, OFAC administers and enforces economic and trade sanctions, many of which are based on the United Nations Security Council (UNSC)♦ resolutions and other international mandates.

Under Chapter VII of the UN charter♦, the sanctions process of the UN typically starts with a matter of concern taken up by the Security Council. At an early stage, knowing the Security Council may impose sanctions can be sufficient to prevent escalation or outbreak of conflict. Sanctions are a last resort imposed in a variety of instances, including in the combating of terrorist financing and proliferation finance.

The sanctions process can be depicted as follows♦:



Sanctions are imposed by means of a UNSC resolution establishing a sanctions regime and a sanctions list. Sanctions committees are subsidiary organs of the Council and are composed of all 15 of the Council's members. The role of the sanctions committees is to implement, monitor and provide recommendations to the Council on particular sanction regimes.

Committees meet regularly to consider reports from expert panels and to meet with Member states, UN actors and international organisations. Sanctions need to be implemented with due regard for human rights.



2.7.3 Politically Exposed Persons (PEPs)



3.2.9 Understand the purpose behind screening individuals: risk-based approach; politically exposed persons (PEPs)

PEPs are individuals with a high political profile. Such persons can pose a higher money laundering risk to firms as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status itself does not incriminate individuals or entities. It does, however, put the customer, or the beneficial owner, into a higher risk category. A PEP is defined as:

‘an individual who is or has, at any time in the preceding year, been entrusted with prominent public functions and an immediate family member, or a known close associate, of such a person’

EU Directive 2006/70/EC sets out the implementing measures for defining PEPs, and so provides a definition of positions that constitute prominent public functions. That definition includes the following categories:

1. heads of state, heads of government, ministers and deputy or assistant ministers
2. members of parliaments
3. members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances
4. members of courts of auditors or of the boards of central banks
5. ambassadors, *chargés d'affaires* and high-ranking officers in the armed forces, and
6. members of the administrative, management or supervisory boards of state-owned enterprises.

This definition was reinforced in the EU's Fourth Money Laundering Directive (MLD) and maintained in subsequent editions of MLD, and extended to include members of the governing bodies of political parties; as well as directors, deputy directors and members of the board or equivalent function of an international organisation. In addition, the definition of a PEP extends to direct family (spouse or equivalent, children and their spouses (or equivalent), and parents) as well as close associates. In this context, close associates are:

- natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a PEP, and
- natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a PEP.

In all six categories of PEP mentioned above, the definition excludes middle- and junior-ranking officials. The governmental legislative/judicial positions noted in the first five categories may relate to posts at national or community (ie, EU) level.

Firms are required to take a risk-based approach to PEPs and need to:

- have appropriate risk-based procedures to determine whether a customer is a PEP
- obtain appropriate senior management approval for establishing a business relationship with such a customer
- take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction, and
- conduct enhanced ongoing monitoring of the business relationship.



3. Policies, Procedures and Controls Required of Firms



3.3.1 Understand the risks to a firm posed by its clients, products and delivery systems

3.1 The Risks Posed to a Firm

Similar to individuals, firms are also exposed to financial crime risks when they perform financial services for clients.

Some of these risks arise because of the firm's clients: are they honest, or seeking to deceive the firm to achieve criminal outcomes? Other risks arise in respect of the different products that the firm may offer: products such as individual savings accounts (ISAs) or pensions allow certain tax benefits, and the firm should be alert to the risks associated with tax evasion. The delivery systems chosen by the firm to provide its services can also affect the financial crime risks that the firm is managing; for example, it is important that the firm is confident that any instructions it receives are made by the actual customer (rather than a criminal seeking to

impersonate the customer in order to take over the account and acquire the assets). The mechanisms that the firm can use to validate a person's identity will vary for different communication channels: telephone calls enable ID questions to be asked; written material must contain all necessary information; and electronic communications are usually protected by some form of username and password.

The firm must be able to recognise such areas of risk and understand how these different elements apply to its own business model. In this respect, senior management should ask themselves a number of questions.

For example:

- What risk is posed by the firm's customers?
 - Does the client satisfy the definition of a PEP, and is the firm able to give such an account the extra care required?
 - Is a customer based in, or conducting business through, a high-risk jurisdiction – and is the firm equipped to perform the additional due diligence that may be required?
 - Is the customer's own business within a sector that places them at a higher risk of exposure to financial crime or corruption? A firm would not want to be associated with a customer who could be exposed as committing or facilitating financial crime – both from a public relations perspective, and because of the practical implications of 'dirty money' being found to have passed through the firm's financial products as market transactions.
- What risk is posed by a customer's behaviour?

- Has the firm established relevant controls over dealing patterns and trends, to identify whether a customer is performing unusual deals that could be suspicious?
 - How would the firm react if a customer asks questions about the levels of secrecy regarding a transaction – or requests additional secrecy measures?
 - Is a customer seeking to transfer assets or money to the firm in such a way that the origin of wealth or the source of funds cannot easily be verified?
 - If the customer is not a private individual, is the operator of the account willing to provide relevant information about the underlying owners and controllers?
- What risk is posed by the way the customer became a customer?
 - Was the firm able to complete the necessary due diligence review of the customer?
 - Where the customer came to the firm via a financial intermediary, is the firm confident in the due diligence material provided by that intermediary?
 - Was the customer accepted after distance communication only, or was a face-to-face meeting held?
- What risk is posed by the products/services the customer is using?
 - Does the product allow payments to third parties?
 - Could the product be used to enable inappropriate assets to pass through the firm?
 - Does the product include features that could enable money laundering or terrorist financing?

The firm must, of course, consider all these factors against its normal expectations for the type of business it performs and the clients it intends to service.

3.2 Understanding the Controls



3.3.2 Understand the controls a firm should have in place to minimise its risk to fraud, money laundering and terrorist financing, including a training programme

Firms are exposed to the risk that its business will become a victim of fraud or will be used by someone performing money laundering or seeking to support terrorist organisations. The firm must, therefore, assess where such risks primarily reside: what processes, products, and client types pose the greatest risk of being abused in this way. Having assessed the risk, senior management must then ensure that appropriate controls are designed and implemented to mitigate this risk.

In respect of fraud, firms must recognise the potential for both internal and external fraud. Internal fraud relates to the actions taken within the company: an employee misusing their position to enrich themselves at the expense of the company or its employees. Quality control checks (to ensure accuracy of processing) and segregation of duties (to ensure that work must pass through separate departments before payment is released) are examples of controls that can reduce the risk of internal fraud occurring.

As regards money laundering and terrorist financing, managing and mitigating the risks will involve:

- measures to verify the customer's identity
- collecting additional information about the customer, and

- monitoring transactions and activity, to determine whether there are reasonable grounds for knowing or suspecting that money laundering or terrorist financing may be taking place.

Part of the control framework will involve decisions as to whether verification should take place electronically, and the extent to which the firm can use customer verification procedures carried out by other firms. Firms must determine the extent of their CDD measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction.

To decide on the most appropriate and relevant controls for the firm, senior management should ask themselves what measures the firm can adopt, and to what extent, to manage and mitigate these threats/risks most cost effectively, and in line with the firm's risk appetite.

Examples of control procedures include:

- introducing a customer identification programme that varies the procedures in respect of customers appropriate to their assessed money laundering/terrorist financing risk
- requiring the quality of evidence – documentary/electronic/third-party assurance – to be of a certain standard
- obtaining additional customer information, where this is appropriate to their assessed money laundering/terrorist financing risk, and
- monitoring customer transactions/activities.

Risk management is generally a continuous process, carried out on a dynamic basis. A money laundering/terrorist financing risk assessment is not a one-time exercise. Firms must, therefore, ensure that their risk management processes for managing money laundering and terrorist financing risks are kept under regular review. A firm should, therefore, keep its risk assessment(s) up to date. An annual, formal reassessment might be too often in most

cases, but still appropriate for a dynamic, growing business. It is recommended that a firm revisits its assessment at least annually, even if it decides that there is no case for revision. Firms should include details of the assessment, and any resulting changes, in the MLRO's annual report.

3.3 Effective Training



3.3.2 Understand the controls a firm should have in place to minimise its risk to fraud, money laundering and terrorist financing including a training programme

It is essential that the firms train their employees in respect of fraud, money laundering controls, and the prevention of terrorist financing in order that staff will be able to recognise suspicious events, and will know how to escalate any such suspicions.

Key criteria for a training programme include:

- understanding the internal controls established, and the risks they are intended to mitigate (eg, controls intended to prevent internal fraud)
- staff responsibilities under the firm's arrangements for the prevention of money laundering and terrorist financing, including those for:
 - obtaining sufficient evidence of identity
 - recognising and reporting knowledge or suspicion of money laundering or terrorist financing
- the identity and responsibilities of the nominated officer and the MLRO
- the potential effect on the firm, on its employees personally and on its clients, of any breach of that law

- the content and frequency of training reflecting the risk assessment of the products and services of the firm and the specific role of the individual, and
- appropriate assessment at the end of a training session to ensure it has been effective.

In addition, selected or relevant employees should be given regular appropriate training in order to be aware of:

- potential fraudulent activity
- the criminal law relating to money laundering and terrorist financing, and
- the regulations or guidance issued by the regulator.

Staff will find it helpful to have illustrations of the type of situation that may be unusual, and which in certain circumstances might give rise to reasonable grounds for suspicion.

Training programmes may also include:

- examples of fraudulent activity – whether previously identified within the firm itself, or relevant cases from similar firms
- the nature of terrorism funding and terrorist activity, in order that staff are alert to customer transactions or activities that might be terrorist-related, and
- trends and the changing behaviour and practices among those involved in money laundering and financing terrorism.

3.4 Effective Suspicious Activity or Transaction Reporting



3.3.3 Know the criteria for an effective suspicious transaction reporting system

An appropriate system of reporting must be in place whereupon:

- All staff must raise an internal report where they have knowledge or suspicion, or where there are reasonable grounds for having knowledge or suspicion, that another person is engaged in money laundering, or that terrorist property exists.
- The firm's nominated officer must consider all internal reports.
- The firm's nominated officer must make an external report to the relevant LEA as soon as is practicable if they consider that there is knowledge, suspicion, or reasonable grounds for knowledge or suspicion, that another person is engaged in money laundering, or that terrorist property exists.
- The firm must seek consent from the LEA before proceeding with a suspicious transaction or entering into arrangements.
- The firm must freeze funds if a customer is identified as being on the sanctions list on the government website of suspected terrorists or sanctioned individuals and entities and make an external report to the relevant authority in its home state.

Firms need to ensure that detailed records are maintained, relating to any suspicious transaction activity – whether as part of the reporting system or as separate records. Such record-keeping should include:

- Details of any disclosures made regarding enquiries on a case.
- The reasons why a SAR/suspicious transaction report (STR) was, or was not, submitted.
- Any communications made with or received from the authorities, including the LEA, in relation to the SAR/STR.
- Where relevant, details of the need for prior consent to be received from the LEA before releasing the proceeds of a transaction – together with details of any such consent received.

The firm's nominated officer must report suspicious approaches, even if no transaction takes place. Any actions required should be kept under regular review.

It is a criminal offence for anyone, following a disclosure to a nominated officer or to the LEA, to do or say anything that might either tip off another person that a disclosure has been made or prejudice an investigation.



End of Chapter Questions

1. What are the three stages of money laundering?

The three stages of money laundering are:

1. Placement (criminal money being fed into the financial system)
2. Layering (performance of multiple transactions to obscure the history/origin of the criminal proceeds), and
3. Integration (removal of the disguised criminal proceeds, so that its origin cannot be determined).

Answer reference: Section 1.2

2. What is the purpose of the Financial Action Task Force (FATF)?

The FATF is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The FATF is therefore a policy-making body that works to generate the necessary political will to

bring about legislative and regulatory reforms in these areas.

Answer reference: Section 1.3.4

3. Give two examples of predicate offences in financial crime.

A predicate offence is the underlying criminal offence that gives rise to criminal proceeds, which is then the subject of a money laundering charge. The following crimes are examples of predicate offences in financial crime: securities fraud, embezzlement, bribery, corruption.

Answer reference: Section 1.4

4. How does a Ponzi scheme work?

The term 'Ponzi scheme' is used to describe a financial services product that claims a level of investment return that is not supported by the investment activity undertaken. The shortfall between the returns generated and those claimed is made up by using the money of new investors, who have been attracted to the scheme by the high headline returns being publicised.

Answer reference: Section 1.5

5. What are typical cybercrime activities?

The most common forms of cyber crime are:

- Hacking – including social media and passwords.
- Phishing – fake emails asking for security information and personal details.

- Vishing – callers try to extract identifying details to use in perpetuating another crime
- Malicious software – including ransom ware.
- Distributed denial of service attacks (DDoS) – ensuring a website becomes unreachable.

Answer reference: Section 1.5

6. Describe how a material misstatement of financial statements may arise.

A material misstatement of the financial statements may arise from fraud or error, in relation to:

- a. the appropriateness of the selected accounting policies
- b. the application of the selected accounting policies, or
- c. the appropriateness or adequacy of disclosures in the financial statements.

Answer reference: Section 1.6

7. What is the difference between tax avoidance and tax evasion?

Tax avoidance is the use of legally permissible methods to reduce the amount of tax owed. This is generally achieved by claiming permissible deductions, credits and allowances. Tax avoidance is legal and includes aspects such as transferring assets between spouses or making pension contributions in order to reduce the level of income that remains subject to income tax. Tax evasion, on the other hand, is an illegal practice where a person, organisation, or corporation intentionally avoids paying part or all of their tax liability. Examples might include not

paying income tax or VAT when working for 'cash in hand'. Tax evasion would also arise if the capital gains made on investments were not correctly disclosed for taxation calculation.

Answer reference: Section 1.7

8. Explain the concept of dual criminality.

Dual criminality (also known as 'double criminality') describes the situation where an action constitutes a crime in both the country where a suspect is being held and the country asking for the suspect to be handed over or transferred to stand trial, ie, the action represents a crime in both jurisdictions.

Answer reference: Section 1.8

9. What are the direct impacts of financial crime?

Financial crime has different direct impacts on different participants. The financial firm may be left with an angry customer and, depending on the circumstances, may have to compensate its customer and reinstate their accounts

The impact of such thefts can include:

- reduced profits and potential risks to the financial stability of the firm
- damage to the firm's reputation, which may arise from supervisory or other regulatory action, such as fines
- increased costs arising from investigation of theft, forensic work by expert or specialist firms and remediation where required such as new systems and controls, and

- increased insurance costs following revised premiums based on recent claim experience, or the need to take out additional insurance cover where perhaps the risk had not previously been identified.

Answer reference: Section 2.2

10. Name three responsibilities of senior management in relation to financial crime.

The directors and senior management of an authorised financial firm are expected to:

- identify, and manage effectively, the risks in their businesses and this will include ensuring appropriate action is taken in relation to combating the financing of terrorism (CFT), AML, CFC and AC
- appoint a nominated officer to process disclosures
- appoint an MLRO with certain responsibilities
- ensure the MLRO has adequate resources devoted to AML/CFT
- understand the potential personal liability if legal obligations are not met.

Answer reference: Section 2.3

11. What factors should a firm consider when assessing the adequacy of its financial crime prevention systems and controls?

A firm should ensure that the systems and controls include:

- appropriate training for its employees in relation to money laundering

- appropriate provision of information to its governing body and senior management, including a report at least annually by that firm's MLRO, or other responsible senior executive, on the operation and effectiveness of those systems and controls
- appropriate documentation of its risk management policies and risk profile in relation to money laundering and other financial crime, including documentation of its application of those policies
- appropriate measures to ensure that money laundering and other financial crime risk is taken into account in its day-to-day operation, including in relation to:
 - the development of new products
 - the taking-on of new customers
 - changes in its business profile, and
- appropriate measures to ensure that procedures for identification of new customers do not unreasonably deny access to its services to potential customers who cannot reasonably be expected to produce detailed evidence of identity.

Answer reference: Section 2.5

12. How can individuals protect themselves from financial crime?

Individuals can do a number of things to reduce the likelihood that they would be a victim of financial crime. They should:

- keep personal information secure and if disposing of financial statements/bank statements use a shredder to shred the statements before disposal
- keep plastic cards in a secure place

- keep documents safe
- keep passwords and PIN numbers secure
- check the qualification and authorised status of any financial adviser
- be aware of scams such as phishing, call and text schemes, and
- remember that if an investment sounds too good to be true it probably is.

Answer reference: Section 2.6

13. When should a firm apply enhanced due diligence?

A firm must apply enhanced due diligence measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing.

Answer reference: Section 2.7.1

14. List the range of the United Nations (UN) sanctions.

UN sanctions measures include:

- travel bans
- assets freeze
- arms embargoes
- bans on export of luxury goods
- commodity bans, like diamonds
- bans on items, material, equipment, goods and technology related to nuclear ballistic missiles and other weapons of mass destruction programmes.

Answer reference: Section 2.7.2

15. Where do the Office of Foreign Assets Control (OFAC) powers originate from?

The Office of Foreign Assets Control (OFAC) is part of the US Department of the Treasury and acts under presidential national emergency, as well as the authority granted to it by specific legislation.

Answer reference: Section 2.7.2

16. What is included on the specially designated nationals (SDN) list?

The specially designated nationals (SDN) list contains individuals and organisations with whom US citizens and permanent residents are prohibited from transacting and doing business with.

Answer reference: Section 2.7.2

17. In applying a risk-based approach to identifying money laundering, what factors should a firm consider?

A risk-based approach starts with the identification and assessment of the risk that has to be managed.

In identifying its money laundering risk, a firm should consider a range of factors, including its:

- customer, product and activity profiles
- distribution channels
- complexity and volume of its transactions
- processes and systems, and
- operating environment.

Answer reference: Section 2.5

18. What controls should be put in place to mitigate the risk a firm faces in respect of money laundering?

Managing and mitigating the risks of money laundering will involve:

- measures to verify the customer's identity
- collecting additional information about the customer, and
- monitoring transactions and activity, to determine whether there are reasonable grounds for knowing or suspecting that money laundering or terrorist financing may be taking place.

Answer reference: Section 3.2

19. Give three examples of the content of a training programme relating to the detection and prevention of fraud, money laundering and terrorist financing.

Key criteria for training programmes are likely to include:

- understanding the internal controls established, and the risks they are intended to mitigate (eg, controls intended to prevent internal fraud)
- staff responsibilities under the firm's arrangements for the prevention of money laundering and terrorist financing (including the need for evidence of identity, and reporting knowledge or suspicion of money laundering or terrorist financing)
- the identity and responsibilities of the nominated officer and the MLRO
- the potential effect on the firm, on its employees personally and on its clients, of any breach of that law
- the content and frequency of training reflects the risk assessment of the products and services of the firm

and the specific role of the individual, and

- appropriate assessment at the end of a training session to ensure it has been effective.

Answer reference: Section 3.3

20. What action should be taken if a customer is identified as being on the sanctions list?

The firm must freeze funds if a customer is identified as being on the sanctions list on the government website of suspected terrorists or sanctioned individuals and entities and make an external report to the relevant authority in its home state.

Answer reference: Section 3.4



Chapter Four

Ethics, Integrity and Fairness

Section 1

Ethics

Section 2

Market Integrity

Section 3

Fair Conduct

Section 4

Fair Dealing

Section 5

Environmental, Social and Governance (ESG)

This syllabus area will provide
approximately 19 of the 100
examinations questions



1. Ethics



- 4.1.1 Understand how ethical principles relate to the financial services industry: regulatory standards; professional codes of conduct; internal codes of conduct
-

1.1 Relating Ethical Standards to the Financial Sector

Regulators believe that they have an obligation to consider and make judgements about the ethics and values of the firms they regulate. Making judgements about behaviours is more than just setting regulations and expecting firms to comply; having a compliance culture is simply not enough. What is needed is an ethical culture in the firm which embodies the values underlying the whole regulatory structure – values which lead to proper protection for consumers of financial services, to proper information for customers, and behaviour in the markets which maintains public confidence in them, and which enables financial crime to be fought effectively.

History shows that many British firms across various industries were originally established as a reflection of the beliefs of their founders; Cadbury and Quaker Oats being two commonly cited examples from the industrial era. Equally, there are examples in the financial sector. Lloyds and Barclays grew from the Quaker movement; and Halifax Building Society was created to help the working classes achieve the benefits of home ownership. Over time, others entered these markets – many simply keen to provide a good service and earn a reasonable capital return, rather than directly following ideological purposes – and the original founders of a company will be replaced. As a market evolves and competition matures, the initial motivations of participants may, therefore, become less visible – particularly if the market begins to display examples of abuse.

While the Western financial sector has arguably moved some way from the ideological roots of some founding firms, they do adhere to voluntary codes of ethics which typically incorporates business ethics, a code of professional practice, and an employee code of conduct.

1.2 Regulatory Standards

Most regulators set out standards and principles which they expect businesses and key individuals to observe. These may include:

- **Integrity** – a firm must conduct its business with integrity.
- **Customers' interests** – a firm must pay due regard to the interests of its customers and treat them fairly; and provide them with information which is clear, fair and not misleading; and advice which is suitable.
- **Market conduct** – a firm must observe proper standards of market conduct.
- **Client assets** – a firm must arrange adequate protection for clients' assets when it is responsible for them.

By setting such standards and principles for firms and key individuals, regulators aim to ensure that the culture and operation of a firm meets the spirit, as well as the letter, of the regulations.

1.3 Professional Codes of Conduct

For any industry in which trust is a central feature, demonstrable standards of practice and the means to enforce them are a key requirement. Hence, the proliferation of professional bodies in the fields of health and wealth. In other words, areas in which consumers are more sensitive to performance and have higher expectations than in many other fields.

The terms 'code of ethics' and 'code of conduct' are often used interchangeably. However, using the term 'ethics' implies conformity with standards of behaviour and personal morality and does not imply compliance with rules and guidance relating to professional dealings. The latter is more appropriately described as a code of conduct. Where it is considered that more specific guidance on standards of professional practice would be beneficial, such standards might be set out in an appropriately entitled document, or in regulatory standards. Examples of professional codes follow.

The Financial Conduct Authority (FCA), for example, has identified six customer outcomes. See section 3.1.

1.3.1 The Chartered Institute for Securities & Investment (CISI) Code of Conduct

Professionals within the securities and investment industry owe important duties to their clients, the market, the industry and society at large. Where these duties are set out in law, or in regulation, the professional must always comply with the requirements in an open and transparent manner. Members of the

CISI are required to meet the standards set out within the CISI's Principles.

These Principles impose an obligation on members to act in a way beyond mere compliance, and to support the underlying values of the CISI.

The Principles are shown in the following table, with a column indicating the main stakeholders in connection with application of the relevant Principle. However, members should be aware that the list is not exclusive and, in some instances, the Principles are applicable to more than one stakeholder.

The Principles	Stakeholder
Personal Accountability – to strive to uphold the highest levels of personal and professional standards at all times, acting with integrity, honesty, due skill, care and diligence to avoid any acts, either in person, in a remote working environment or digitally which may damage the reputation of your organisation, your professional body or the financial services profession.	Self, clients, regulators, colleagues, market participants, firm, profession, society
Client Focus – to put the interests of clients and customers first by treating them fairly, being a good steward of their interests, never seeking personal advantage from confidential information	Clients

received and utilising client data only for a defined purpose.	
Conflict of Interest – being alert to and actively manage fairly and effectively any personal or other conflicts of interest, obeying legislation and complying with regulations to the best of your ability, ensuring you are open and cooperative with all your regulators, challenging and reporting unlawful or unethical behaviour.	Clients, market participants, regulators
Respect for Market Participants – to treat all counterparties and business partners with respect, to observe proper standards of market integrity, good practice, conduct and confidentiality required to maintain the highest level of mutual trust.	Clients, market participants
Professional Development – to strive continually for professional excellence, committing to Continuous Professional Development (CPD) and promoting and supporting the development of others.	Profession, clients, colleagues
Aware of Capabilities – to decline to act on any matter about which you are not competent or qualified unless	Clients, profession, market participants

you have access to such advice or assistance to carry out the work in a professional manner, taking into account the nature of the individual mandates given by your customers and counterparties.	
Respect Others and the Environment – to treat everyone fairly and with respect, supporting opportunity for all, embracing diversity and inclusion and ensuring that the environmental impact of your work is considered.	Society, colleagues, clients, regulators, market participants, profession, professional body
Speak Up & Listen Up – to be active in speaking up and encouraging others to do so by listening up, promoting a safe environment for all and recognising the responsibilities you have to the communities in which you operate.	Society, colleagues

The CISI has also added some guidance on digital ethics to be used by members as a supplementary reference alongside the CISI Code of Conduct. It specifically focuses on the ethical principles for consideration within digitalisation and changing technologies.

Technologies offer significant opportunities to make our lives easier, safer, more comfortable, efficient, and fun. They also present a range of risks that may impact people's privacy and their trust in these technologies, if they are not addressed as the technology

develops. The guidance is structured into two parts: one focusing on ethical considerations for technology developers, and the other tailored for users.

Material breach of the Code of Conduct would be incompatible with continuing membership of the CISI and may result in disciplinary action. Members who find themselves in a position which might require them to act in a manner contrary to the Principles are encouraged to:



Discuss their concerns with their line manager



Seek advice from their internal compliance department



Approach their firm's non-executive directors or audit committee



If unable to resolve their concerns and, having exhausted all internal avenues, contact the CISI for advice (email: principles@cisi)

1.3.2 The Chartered Financial Analyst (CFA) Institute – Code of Ethics and Standards of Professional Conduct

One of the professional institutes with a global reach is the CFA Institute whose members follow a code of ethics and standards of professional conduct which were created in the 1960s and are continuously reviewed and updated as required. The code and standards have promoted the integrity of CFA Institute members and have served as a model for measuring the ethics of investment professionals globally, regardless of job function, cultural differences or local laws and regulations.

The CFA Institute Code of Ethics includes the requirements that members and candidates must:

- act with integrity, competence, diligence, respect and in an ethical manner with all stakeholders, such as clients and others in the profession
- place the profession above their own interests
- exercise independent professional judgement
- encourage others to act in a professional and ethical manner
- uphold the rules governing capital markets, and
- exercise continuing professional development.

Full details of the code and standards can be obtained from the Institute's website [♦](#).

1.4 Internal Codes of Conduct

Many firms in financial services have adopted their own internal codes of conduct and ethics which they communicate to staff and customers. Such codes may reflect the aim of good ethical behaviour as well as regulatory compliance. Internal codes of conduct are typically published on a financial services' intranet site.

Example

Code of Conduct

As an industry leader, we want to set an example in the marketplace when it comes to ethical values and professional standards. Our Code of Conduct provides a clear approach for how we expect all members of the Board of Directors and employees to conduct themselves. Only by operating within this framework can we maintain and strengthen our reputation for integrity, fair dealing and measured risk-taking. Our vision is to become the world's most admired bank. Our client-focused, capital- efficient strategy is designed to help realise this ambition and is reinforced by our principles of being a proactive, principled partner to our clients.

Our Ethical Values

- **Integrity** – A reputation for integrity is essential for our long-term success.
- **Responsibility** – We take responsibility for our actions and honour our commitments to our stakeholders.
- **Respect** – We treat our employees with respect and fairness.
- **Compliance** – We strive to maintain an exemplary control and compliance culture.
- **Confidentiality** – We treat confidential information as such and do not disclose any non-public information unless required to do so by law.
- **Trust** – We are committed to behaving in an ethical and professional manner.

Our Professional Standards

- **Service and Excellence** – We are committed to being a proactive, principled partner to our clients.
- **Risk Culture** – Our business is based on disciplined and intelligent risk-taking.
- **Transparency** – We seek constructive, transparent and open dialogue with our stakeholders.
- **Adherence to Laws and Regulations** – Members of the Board of

Directors and employees are expected to comply with all applicable laws, regulations and policies.

- **Sustainability** – We conduct our business with a long-term view to support environmental and social sustainability.
- **Commitment** – We value the efforts of our employees and strive to create a work environment that is designed to attract, develop and retain talent.

1.5 Applying an Ethical Approach



- 4.1.2 Understand the impact of the following when applying an ethical approach within an organisational or team environment: self-interest; fiduciary responsibilities; the role of the agent; the role of stakeholders; the role of the group or team
- 4.1.3 Understand the advantage of ethical behaviours and decision-making over rule-based compliance

1.5.1 Self-Interest

Self-interest refers to a focus on the needs or desires (interests) of oneself. By extension, it can mean:

- individualism, a philosophy stressing the worth of individual selves
- psychological egoism, the view that humans are always motivated by self-interest
- ethical egoism, the ethical position that moral agents ought to do what is in their own self-interest
- hedonism, the school of ethics which argues that pleasure is the only intrinsic good

- Epicureanism, a philosophical system related to hedonism
- enlightened self-interest, a philosophy which states that acting to further the interests of others also serves one's own self-interest, or
- indirect self-interest, any situation in which the interests of others match one's own, so that serving one will lead to serving the other.

When an ethical approach is to do the right thing and to ensure customers are treated fairly, the needs of the customer may be placed before the self-interest of the individual or the interest of the team or firm. A firm's corporate culture and attitude to ethics are set by the behaviour of the board and the executive. Therefore, if a senior member of management is seen to bend the regulations to favour the firm or themselves, junior staff are likely to follow their example.

1.5.2 Fiduciary Responsibilities

The term 'fiduciary duty' originates from the Latin *fiduciarus*, meaning '(holding) in trust'; from *fides*, meaning 'faith' and fiducia, meaning 'trust'. It is a legal or ethical relationship of confidence or trust regarding the management of money or property between two or more parties, most commonly a fiduciary and a principal. The fiduciary (for example, a corporate trust company or the trust department of a bank) holds a fiduciary relation or acts in a fiduciary capacity to the principal (for example, a person whose funds are entrusted to it for investment).

In a fiduciary relation, the principal places confidence, good faith, reliance and trust in the fiduciary whose aid, advice or protection is sought in some matter. The fiduciary should always act in the sole benefit and interests of the principal. The recruitment and training of the firm's staff who undertake these services will feature an ethical competency requirement.

1.5.3 The Role of the Agent

Investors will often seek the advice of agents such as financial advisers, when purchasing financial products and services. The agent may be:

- an **independent financial advisor** – completely independent of any bank, fund manager or insurance company in order to give the client unbiased advice. They typically charge a fee or commission for such advice, agreed to by the client, or
- a **tied agent** who sells only the products from one provider.

The agent will often arrange the purchase on the client's behalf either through an exchange or direct from the product provider. The client is relying on the trustworthiness of the agent to provide them with good advice and to ensure the suitability of any investment recommended.

Even after the United Kingdom (UK) regulator's Retail Distribution Review (RDR) banned many types of commission payments, some product providers offer agents a commission when they sell their products to the agent's clients. From an ethical perspective, there is a risk that the agent may be tempted to prioritise the products from a provider who pays the highest commission rather than the product most suitable for their client. Regulators have sought to prevent such outcomes, requiring transparency and disclosure of the commission received. The [Markets in Financial Instruments Directive \(MiFID\) II](#) introduced similar bans on the payment of commission within the European Union (EU). Another potential adverse impact of commission payments is that unless the rates are fixed, product providers may compete by offering increasing levels of commission.

Tied agents can be salaried and/or in receipt of commission or bonuses for sales. In these cases, the agent is clearly the agent of the product provider rather than the investor. To ensure they are fair, clear and not misleading, they should inform the investor of their

tied status and that their advice is limited to the range of products and services offered by the product provider they act for, and not the full range of products available from the market.

1.5.4 The Role of Stakeholders, Groups and Teams

A firm is a combination of groups and teams working to achieve outcomes, supported by, and accountable to, a range of stakeholders. Some of those stakeholders represent the executive leadership of the firm; others are non-executive (such as shareholders). The role of stakeholders will vary, as does the application of codes of conduct. The CISI Code of Conduct, for example, is intended to provide direction to members regarding their behavioural obligations when dealing with all stakeholders involved in the activity of financial services.

At the corporate and institutional level, this means operating in accordance with the rules of market conduct, dealing fairly and honestly with other market participants and not seeking to take unfair advantage of either. Competition should be fostered, but the rules and standards of behaviour enable markets to function smoothly, alongside the actual regulations which provide direction for the technical elements of market operation. Firms have an ethical responsibility to their clients over and above complying with the regulatory framework and legal responsibilities.

External stakeholders (eg, shareholders of the firm, creditors, local and national governments) have a role in holding the executive leadership to account for their implementation of the firm's ethical stance. Groups and teams within the organisation will, in most cases, own that implementation and must recognise their responsibility to the firm for ensuring their daily work reflects the ethical position of the firm.

1.5.5 The Advantage of Ethical Behaviours and Decision-Making

The main criticisms of rules-based compliance are that the rules become outdated as the market evolves, they become too complex and detailed, and those gaps in the rules become loopholes which unscrupulous firms will exploit.

In addition to the shift towards principles-based regulation (setting the required outcomes, rather than the means of achieving them), there has been renewed focus on professional integrity as shown, for example, by the inclusion of ethics in the continuing professional development (CPD) requirements of the CISI and the CFA. If those in the industry act in an ethical manner, the motivation for abuse will be reduced, resulting in various advantages.

Clients will have increased trust in firms and practitioners if they are confident that ethical standards are being applied. Firms may be able to change the way in which they oversee certain tasks, reducing the costs associated with monitoring activity and increasing the value of their findings. If firms can show that they can act in line with such ethical standards, over time, it should enable the regulators to reduce the prescriptive aspects of the rulebook, confident that firms will not seek to exploit such additional freedoms.

1.5.6 Senior Management and Ethical Standards



4.1.4 Understand the importance of senior management leadership in developing and maintaining ethical standards

Culture can be described, but not easily defined. It cannot be imposed on an organisation by just putting in a programme; it must

be recognised by those inside who are employed, and those outside who come into contact with the business.

At its most basic, corporate culture expresses itself in the behaviour of individuals and in the way a business is run. Staff members are sensitive to management style. When faced with a business problem, a manager has to balance the legitimate requirements of attaining business objectives and the ethical requirements of honesty and integrity in the way this is achieved.

If staff see from their managers' decisions that the prevailing culture is one of trust, integrity and openness, they generally will feel comfortable at work and be proud of the organisation. This is likely to be reflected in their own dealings with others.

For an ethical culture to be successful, it must have regard for all of those people and organisations who are affected by it.

An ethical approach helps minimise the negative effects of employee behaviour while ensuring a firm and its industry sustain healthy competition as well as socially responsible behaviour in the long run. Put simply, ethics control costs that cannot be controlled directly or may not be known. Setting up an ethics policy and instilling a sense of ethics into all employees is, however, a substantial task. Determining what can actually be considered ethical is challenging and it is tempting to shape an ethics policy to be self-serving.

Maintaining ethical standards is a necessity and requires management to build a culture of ethics. An organisation can only maintain ethical standards if senior management considers setting ethics as a top priority. Accordingly, management needs to embrace strong ethics while enforcing tough standards for all employees from the board and senior managers down to the most junior employee. An ethical organisation can strengthen its resolve to behave responsibly only by developing its ranks into ethical professionals, so that current and future leaders will follow solid ethics and help their firm succeed in the long term. Training

programmes, a clear code of ethics, and reinforcement of positive behaviour will assist in creating and maintaining an ethical environment.

As ethics attempt to address unknowns, it is difficult for management to isolate unethical behaviour by an individual until the fallout of those decisions occurs. This is further hindered by the fact that unethical behaviour typically occurs without the company's knowledge; thus, ethics rely on trust. To build trust, employees can be tested by management setting them up for ethical successes. Creating an ethical professional relies on management shaping the behaviour of employees where leaders can easily identify and guide individuals who may find it difficult to understand the real benefits of pursuing an ethical approach.

Maintaining ethical standards is a continuous effort that requires professional and workplace development. Ethical violations can be minimised by instilling a strong sense of ethics in employees when business leaders have influence over their subordinates' behaviour. Management can maintain strong ethical standards in their organisations by making it a requirement that all employees take ethical considerations into account when making decisions, but a strong ethics culture must be built over time.

The role of senior management in developing and maintaining strong ethical standards is important. In some countries, it has become the standard for firms to appoint chief ethics officers to assist in the delivery and maintenance of ethical programmes designed to raise the ethical standards employed by financial firms.

1.5.7 Ethical Decision-Making and Training



4.1.5 Know how training programmes can be used to promote ethical decision-making

IOSCO Recommendations for Developing an Effective Ethics Training Programme

An effective ethics training programme needs to do more than communicate a code of conduct; it needs to give employees an increased level of confidence and comfort when making business decisions that address ethical challenges. Guiding principles, practical decision-making models and training must be accompanied by company leadership dedicated to ethical decision-making. With these building blocks in place, financial services professionals will be able to develop a culture centred on ethical conduct that should become one of their greatest assets.

Effective ethics training contains the following components:

1. Basic Approach to Successful Ethics Training

- a. Help employees understand ethical judgement.
- b. Give employees ethical expectations and rules.
- c. Identify specific industry/profession areas of concern.
- d. Help employees understand their own ethical tendencies.
- e. Offer a realistic and practical view of the challenges in ethical decisions.
- f. Practise and return with questions.

2. Strategy Designed to Follow the Creation of a Code of Ethics

- a. Help employees understand the code and its usefulness.
- b. Review the code's provisions with a focus on how these provisions apply to job responsibilities.
- c. Learn what behaviours and decision-making processes the organisation wants employees to apply when confronting ethics challenges.

- d. Raise questions about ambiguities or uncertainties resulting from the code's language and examples.
- e. Practice applying the standards communicated by the code to 'typical' ethics challenges faced by employees.
- f. Learn what the organisation wants employees to do when:
 - i. facing ethical uncertainties
 - ii. observing ethical misconduct, or
 - iii. perceiving pressures being applied (to oneself or others) to commit ethical misconduct.

3. **Practical Advice for Developing a Comprehensive Ethics Training Programme**

- a. Start with company values and an ethics code of conduct.
- b. Involve executive management and secure adequate funding.
- c. Develop a range of materials.
- d. Consider innovative delivery strategies.
- e. Know when not to use technology.
- f. Tailor to the firm's operations.
- g. Integrate key ethical concepts into training courses.
- h. Make training programmes both global and local.
- i. Evaluate the programme.
- j. Consider using case studies from both inside and outside the industry.
- k. Consider a train-the-trainer/cascading process.
- l. Consider outside trainers.

Finally, there must be a mechanism for periodic review of the code of ethics programmes.

Creating an Ethical Culture

Experts emphasise that the goal of ethics training should not be to simply convey knowledge of the standards or the law, but rather to create an ethical culture in which employees are guided by a shared ethical compass that incorporates the principles behind the standards and the law.

In order to achieve this, an organisation has several options, the most effective being a 'values-based cultural approach'. This approach seeks to motivate employees to aspire to ethical conduct, encourage them to question authority where ethics are at stake, and to hold them accountable for ethics violations. Furthermore, this values-based approach requires the sincere commitment of leadership at all levels, including paying ongoing attention to key issues such as fair treatment of employees, rewards for ethical conduct, concern for external stakeholders, and consistency between words and actions.

An organisation would need to do the following:

- Instil the basics. An ethics or compliance function and articulated professional ethics standards are the foundations on which the other parts are built.
- Develop a well-known policy of 'programme follow through' which not only tries to detect violators but also follows up on the ethical concerns raised by employees. This is key, as it helps to demonstrate that the company and, specifically, the company leadership are committed to an ethical culture.
- Recognise that ethical and effective leadership creates 'an ethical tone' in companies, which employees detect and to which they respond. This ethical leadership should not be overlooked or understated as employees look to their leaders and managers for their own ethical tone. Thus, employees will have a more serious view of ethics if they perceive that their

leaders and managers pay attention to, and promote, ethical behaviour.

- Make ethics discussions a part of normal day-to-day activities. Ethics discussions should be woven into the corporate culture by making ethics concerns part of the norm.
- Implement a simple rewards system for ethical conduct that demonstrates the company's endorsement of an ethical culture and gives additional public examples of the company's focus on ethical actions.
- Reinforce ethical standards on a regular, repeating basis.
- Monitor and keep in touch with employee concerns about ethics. This provides valuable insight both into where, and how, real ethics violations are going to occur, and how employees perceive the ethical culture within the company.



2. Market Integrity

2.1 Fair and Orderly Markets



4.2.1 Understand the benefits of a fair and orderly market

4.2.2 Understand the implications of false and misleading statements, behaviours and practices

The benefits of fair and orderly markets broadly mirror the objectives and benefits of regulation (see chapter 1, section 1.1).

The benefits include:

- Investors will have the confidence to invest in securities issued by businesses which need to raise capital.
- They help to establish the environment to encourage economic development and wealth creation.
- They allow the transfer of capital between enterprises at fair prices for minimal cost.
- They successfully provide liquidity through the speed and ease with which capital transfers can be affected, and buyers

and sellers are able to locate counterparties willing to trade a wide range of securities at acceptable prices quickly and efficiently.

- Investors can be reassured that settlement and delivery of stock will take place.
- Information will be readily available to ensure transparency.
- The way in which securities trades are handled and cleared will be controlled and rules adopted aimed at limiting the volatility of security prices.
- Significant resources will be applied to the identification and prevention of market abuse.

Orderly markets depend upon the availability of accurate information. The integrity of the market can be affected when a party provides false or **misleading statements** regarding financial or other matters (see chapter 3, section 1.6). Publication of misleading financial statements might result in asset values being over or understated, which may in turn affect share prices and potential takeover and merger activity.

It is, therefore, important that a firm's behaviours and practices uphold market integrity. Where a firm provides false information, or acts improperly in some similar manner, market operations are impacted. Where such behaviour is then identified and made public, confidence in the market and its participants can be severely shaken. Regulators will, therefore, impose significant penalties on firms that release false or misleading information to the markets.



2.2 Price-Sensitive Information



4.2.3 Understand what type of information may be deemed to be price-sensitive non-public information

4.2.5 Know what activities can constitute 'insider dealing'

Directors and other senior staff members of a company have access to several types of corporate information relating to company performance (eg, budgeting and forecasting material, corporate accounts, or details of new contracts being entered into). In the event the company is listed on a stock market, this information may have an impact on the share price and is referred to as 'price-sensitive information'. It would not be ethical for those inside the company to benefit from their knowledge of such information.

As such, listed companies must establish controls and protocols to limit the ability of those with access to price-sensitive information (including their immediate family members and other close relations) to trade shares in the company during key periods of the business cycle such as, for example, in the months before publication of the company accounts). The company will also require that its senior management maintain the confidentiality of price-sensitive information, so that the individual does not share the information with anyone who can deal in the company's shares in the light of the information obtained from the company insider.

If an individual trades on the basis of **inside information**, or passes that information to another person in order that they may benefit from it, this would constitute a criminal offence in most jurisdictions and are punishable by a prison sentence and/or a fine.

Inside information is information that:

- relates to particular securities or to one or more particular issuer (ie, it is not so wide as to apply to securities or issuers of securities generally); it could, however, include information about the particular market or sector the issuer is active in
- is specific or precise
- has not been made public, and

- is price sensitive (ie, if it were made public, it would be likely to have a significant effect on the price of any securities).

Some of these criteria may seem quite subjective; for example, what is specific or precise? Legislation generally gives some assistance in interpretation; for example, it may include a (non-exhaustive) list of what 'made public' means. For example, information becomes public when it is:

- published in accordance with the rules of a regulated market to inform investors (eg, a UK-listed company making an announcement through a regulated information service (RIS)), or
- contained within records open to the public (eg, a new shareholding that is reflected in the company's register of shareholders).

An individual commits the offence of **insider dealing** if they:

- deal in price-affected securities when in possession of inside information
- encourage someone else to deal in price-affected securities when in possession of inside information, or
- disclose inside information, otherwise than in the proper performance of their employment, office or profession.

For a transaction (ie, an acquisition or a disposal of price-affected securities) to fall under the insider dealing legislation, it must take place in a regulated market, or through a professional intermediary – otherwise, the legislation does not apply.

Insider trading can only be committed by an individual holding inside information as an insider; it cannot be committed by a company. However, by arranging for a company to deal, an individual could commit the offence of encouraging it to do so. The offence of encouraging someone to deal need not result in an actual deal for the offence to have been committed (though it may be unlikely that the offence will come to light, if no deal results).

2.3 Ways in which Individuals Legally Possess Price-Sensitive Non-Public Information



4.2.4 Understand how individuals may legally possess price-sensitive, non-public information

Being in the possession of price sensitive, non-public information is not in itself illegal. There are a number of instances in which an individual will have access to price sensitive non-public information.

2.3.1 Market Makers

As long as a market maker can show that they acted in good faith in the course of their business as a market maker, they will not be deemed guilty of insider dealing. Hence, a market maker (or their employees) could hold unpublished price-sensitive information as an insider and continue to make a market in that security.

2.3.2 Market Information

An insider is not guilty of dealing or encouraging others to deal if they can prove that the information they held was 'market information', and that it was reasonable for them to act as they did despite having the information at the time. Market information includes information such as the fact that the sale of a block of securities is under consideration, or the price at which such a transaction is likely to be done.

2.3.3 Price Stabilisation

Rules generally permit the market price of a security to be 'stabilised' in connection with a new issue in order to manage volatility. These are known as the 'price **stabilisation** rules'; and as long as these rules are being followed, then the participants are not deemed to be insider dealing.

2.4 Market Integrity Controls (including Information Barriers)



- 4.2.6 Understand how systems and controls can minimise exposure to strategies and behaviours that might impair market integrity: information barriers; insider lists (including watch and restricted lists); personal account dealing; gifts and entertainment; conflicts of interest policies
 - 4.2.7 Understand the importance of whistleblowing for market integrity
-

2.4.1 Information Barriers

An information barrier, also known as a **Chinese wall**, is the term given to arrangements made by a firm to manage conflicts of interest where information held by an employee in one part of the business must be withheld from (or, if this is not possible, at least not used by) the people working in another part of the business.

There is no requirement for a firm to have information barriers in place; they are just one example of how to manage conflicts of interest. However, the regulator normally requires that if a firm establishes and maintains an information barrier, it must:

- withhold or not use the information held, and

- for that purpose, permit its employees in one part of the business to withhold the information from those employed in another part of the business.

A firm only needs to do so if at least one of those parts of its business is carrying out regulated activities, or another activity carried on in connection with a regulated activity.

Where a firm adopts information barriers, they must be correctly maintained – including taking reasonable steps to ensure that these arrangements remain effective and are adequately monitored.

Example of an Information Barrier in Operation

When a firm establishes and maintains an information barrier, it allows the persons on one side of the wall, eg, corporate finance, to withhold information from persons on the other side of the wall, eg, the equity research/market-making arm, but only to the extent that one of the parts involves carrying on regulated activities, ancillary activities or MiFID ancillary services.

The effect of the information barrier rule is that the corporate finance department may have plans for a company that will change the valuation of that company's shares. The equity research/market-making arm on the other side of the wall should have no knowledge of these plans; consequently, the inability to pass this knowledge on to clients is not seen as a failure of duty to their clients.

A firm will not be guilty of the offences of market manipulation, market abuse or be liable to a lawsuit when the failure arises from the operation of an information barrier.

To manage conflicts of interest and ensure the fair treatment of clients, firms need to have policies and procedures in place such as information barriers (reporting lines); remuneration structures; segregation of duties; policy of independence. The EU and UK regulations state that procedures and measures provided for must:

- be appropriate to the size and activities of the firm and the group to which it belongs, as well as the materiality of the risk of damage to the interests of clients, and
- ensure the firm maintains the requisite degree of independence including:
 - effective procedures to prevent or control the exchange of information if the exchange of that information may harm the interests of one or more clients
 - ensuring departments whose principal function is to work on behalf of clients where a conflict of interest may occur are separate from other departments
 - remuneration should be designed to ensure it cannot be unduly influenced by activities that may cause potential conflicts of interest
 - measures to prevent or limit any person from exercising inappropriate influence over the way in which a relevant person carries out services or activities, and
 - measures to prevent or control the simultaneous or sequential involvement of an individual in separate services that could impair the proper management of conflicts of interest.

If the adoption or the practice of one or more of those measures and procedures does not ensure the requisite level of independence, a firm must adopt such alternative or additional measures and procedures as are necessary and appropriate.

2.4.2 Insider Lists (including Watch and Restricted Lists)

Regulated/unregulated firms and issuers who handle inside information must have strong systems and controls to ensure

confidentiality and prevent the risk that the inside information they hold is improperly disclosed contrary to any regulatory market abuse regime. It is equally important that senior management at regulated/unregulated firms and issuers establish (and are seen to establish) a robust anti-leaking culture within their organisations. Some principles, policies and procedures for handling inside information are shown in Appendix 6.

An issuer, usually an investment bank or stockbroker, must ensure that it and persons acting on its behalf or on its account, draw up a list of those persons working for them, under a contract of employment or otherwise, who have access to inside information relating directly or indirectly to the issuer, whether on a regular or occasional basis.

As part of developing the Market Abuse Regulation (MAR), the European Commission (EC) published two templates for maintaining an insider list (one template to record permanent insiders, the other to record those who are insiders only in respect of a particular event or period of time).

Both templates require the following information to be recorded for each insider identified by the issuer:

- first name
- surname
- birth surname (if different)
- date of birth
- national identification number (if applicable)
- personal telephone numbers
- personal full home address
- company name and address (ie, any company associated with the insider)
- professional telephone number
- the person's function and reason for being an insider, and
- the date and time the individual was added to the list.

In addition, for a temporary insider, the date and time from which the individual ceased to be classed as an insider should also be recorded. Standard layouts of insider lists in other jurisdictions may vary. An insider list needs to be updated promptly and should clearly state the date and time it was created and last updated. In case the issuer is not able to ensure the confidentiality of the relevant inside information, they must have measures in place which enable public disclosure to be made via an RIS as soon as possible.

Before the details are made public, information in relation to a merger, acquisition or a corporate action such as, for example, a rights issue is clearly sensitive. During the sensitive period, the risk of insider dealing and market manipulation greatly increases. The perception that participants in an offering exploit material information and/or trade with a view to influencing the offer price and/or change their proprietary positions is potentially damaging to the fair and efficient operation and integrity of regulated markets.

During the sensitive period, participants in an offering should implement trade review and surveillance procedures usually known as watch lists (sometimes referred to as grey lists), which permit trading in the securities on the list, subject under close scrutiny by the firm's compliance department, and restricted lists, which restrict or prohibit trading in the securities on the list.

A restricted list is a mechanism established within a financial services firm to identify any securities that the firm's staff are (at that time) not permitted to trade. The firm will add security to its restricted list during any period when the firm is in possession of sensitive information about that security or its issuer. An example is when the firm is involved in a material transaction of the issuer, the details of which are confidential and may also be price sensitive. As inclusion on a restricted list will often mean that the firm and the issuer are engaged in some business/transaction, it is important that the restricted list (or details of the securities included) should

not be communicated to anyone outside the trading areas of the firm or to anyone external to the firm.

The compliance department plays an important role during the sensitive period. When an employee becomes aware of material information regarding security, they should immediately inform the compliance officer. The compliance officer must then decide on the trading restrictions, if any, that are appropriate in the circumstances. In particular, the compliance officer must decide whether to place the security on the firm's watch list or restricted list. The compliance officer must also consider the appropriateness of any trading restrictions in the context of the firm being a member of a financial group.

Participants in an offering should establish adequate internal controls over the trades carried out by their managers, employees and other related persons. Examples of issues the compliance function should be alert to in relation to inside information and which may give regulators cause for concern may include the following:

- The distribution of restricted lists to all staff working in the firm, regardless of function. Distribution should be restricted to those with a need to know.
- A failure by senior management/compliance to understand what information had been made available at 'private side' conferences that were subject to non-disclosure agreements (NDAs). While it is positive that such NDAs are signed off by compliance or senior management, knowledge of the firms and information discussed at such conferences is vital for proactive monitoring of subsequent trading.
- A general failure by firms to adopt clear desk policies. This leaves firms vulnerable to a leakage of inside information both to staff who are not insiders and to outside contractors who may have access to the firms' offices, particularly outside normal office hours. It is expected that firms adopt

appropriate controls in order to protect the security of inside information.

- While IT controls may be in place involving system passwords and file protections, it is necessary to consider extending the full range of market abuse controls to contractors and employees alike. Some external contractors may have access to sensitive information, but not be subject to personal account trading restrictions or market abuse training.

2.4.3 Personal Account Dealing

Besides from the mechanisms described above, which tend to affect certain employees or managers in certain situations or in respect of certain investments, financial services firms will have arrangements in place to minimise the risk of a conflict of interest when their employees deal in investments on their own account. Under MiFID, these rules regarding 'personal account dealing' are applicable to individuals defined as 'relevant persons'. In simple terms, a 'relevant person' means anyone working for the firm from directors of the firm or any of its **appointed representatives**, to any natural person involved in providing services to the firm – such as an outsourced services provider. In addition, it may include the employee's close relatives or cohabitants.

Conflicts of interest can be subjective, depending on the specific role an individual fulfils, and the specific information they possess. Therefore, each firm will design its PA dealing policy according to its own business context and activity. In some cases, all members of staff will be expected to apply the policy in a common manner; in some companies the personal account dealing policy will apply differently as the individual progresses up the corporate hierarchy. The intention is to protect staff against the suggestion that they acted improperly under a conflict of interest. Therefore, the policy may restrict the following types of activity:

1. entering into a personal transaction that is contrary to the MAR; involves misuse or improper disclosure of confidential information, or conflicts with the firm's duties to a customer
2. improperly advising or procuring that anyone else enters into a transaction that (if it had been done by the employee themselves) would have fallen foul of the above or of a 'relevant provision', or
3. improperly disclosing information or opinion, if they know or should know that the person to whom they have disclosed it is likely to enter into a transaction that (if it had been done by the employee themselves) would have fallen foul of the above or of a relevant provision or encouraging someone else to do so.

Clear PA dealing policies should be in place and all PA dealing requests should be signed off by an appropriately empowered individual. It is not appropriate for senior managers to be able to sign off their own PA dealing. Firms must keep records of all personal transactions notified to them, and of any authorisation or prohibition made in connection with them.

The arrangements must ensure that the affected employees are aware of the restrictions on personal transactions and of the firm's procedures in this regard. The arrangements must be such that the firm is informed promptly of any such personal transaction, either by notification of the transaction, or by some other procedure enabling the firm to identify it.

When outsourcing takes place, the arrangements must be such that the outsource service provider maintains a record of personal transactions undertaken by any relevant person and provides it to the firm promptly on request.

The rules on personal account dealing do not apply to:

- deals under a discretionary management service, if there is no prior communication between the portfolio manager and the

relevant person (or any other person for whose account the transaction is being executed) about the deal, or

- deals in units/shares in certain classes of a fund, if the relevant person (and any other person for whom the deals are affected) is not involved in the management of the fund.

The compliance function should ensure that:

- Staff are reminded periodically of the firm's PA dealing rules which should be readily available to them via a compliance manual or staff handbook, eg, a reminder via a regular email.
- Induction and refresher training, as part of the regulatory suite of training sessions or online e-learning modules, should be provided on an annual basis. Attendance or completion of such training should be recorded by the human resources department.

2.4.4 Gifts, Benefits in Kind and Entertainment

The firm needs to be sure that none of their board members, managers or staff are induced to act improperly.

Gifts and benefits in kind must never be accepted if they might give rise to the suspicion that the recipient's judgement is likely to be influenced. Staff must report all gifts and benefits offered to them in the course of business to the compliance function, for example, by means of a Gifts and Benefits Form.

Failure to report a gift or benefit in kind is often deemed a disciplinary offence and may constitute grounds for dismissal. Employees should be asked to familiarise themselves with the firm's policy. Firms should keep a record of gifts and benefits received; it is quite normal to set a minimum level for this and to require prior approval of compliance where the amount is over a set level.

While entertainment, such as lunch or attending a sporting event (eg, golf days), has been quite normal practice, and broadly

acceptable, a number of UK firms have in recent years been less willing for their staff to accept such invitations. Lavish gifts, such as holidays, should never be accepted. The compliance officer will also need to consider the employee's position and level. A junior member of staff may be influenced by a gift of a much lower value than that for, say, the chief executive.

2.4.5 Conflicts of Interest Policies

As far as market integrity is concerned, one of the key areas where conflicts of interest may arise, is in relation to the production and dissemination of investment research on listed companies and their securities.

In general, firms must seek to:

- take all reasonable steps to prevent conflicts of interest from giving rise to a material risk of damage to the interests of clients
- implement and operate an effective written policy for identifying and managing conflicts of interest
- specify in the conflicts policy, certain procedures and measures to ensure appropriate independence and further steps if these prove inadequate
- disclose the conflict to the client, if the arrangements under the firm's policy are not adequate to prevent material risks of damage to a client, and
- in considering their own policy in respect of their duties to their clients, take account of any circumstances, of which the firm is, or should be aware, which may give rise to a conflict of interest arising as a result of the structure and business activities of other members of the group.

Firms must also ensure that they have arrangements designed to satisfy the following conditions in place:

- Financial analysts and other relevant persons who know the likely timing/content of investment research which is not yet publicly available or available to clients and which cannot be inferred from information that is available, cannot undertake personal transactions, or trade for others, until the recipient of the investment research has had a reasonable opportunity to act on it. Certain exceptions may apply, such as the receipt of an instruction from an execution-only client and a market maker acting in good faith.
- In cases not covered by the above, firms cannot undertake personal account transactions without prior approval from the firm's compliance or legal department and then only in exceptional circumstances.
- The firm and any person involved in the production of research must not accept inducements from those with a material interest in the subject matter of the research.
- Firms may not promise issuers favourable research coverage.
- Issuers, relevant persons other than financial analysts, or anyone else must not be allowed to review draft investment research which includes a recommendation or target price, other than to verify compliance with the firm's legal obligations.

A key control for dealing with conflicts of interest is ensuring that appropriate disclosures are made including the following:

- Disclosure by the firm of any relationships and circumstances that may reasonably be expected to impair the objectivity of the research recommendation.
- When the disclosure would be disproportionate in relation to the length of the research recommendation, the firm must make clear and prominent reference to such a place where disclosures can be directly and easily accessed by the public.
- Disclosure of any significant shareholder relationship between the firm (or any affiliated company) and the relevant

issuer (the company which is the subject of the investment research recommendations), including at least:

- shareholdings exceeding 5% of the total issued share capital held by the firm or affiliated company
 - shareholdings exceeding 5% of the total issued share capital of the firm or any affiliated company held by the relevant issuer.
- Any other financial interests held by the firm or any affiliated company in relation to the relevant issuer which are significant in relation to the research recommendation.
- If applicable, a statement that the firm or any affiliated company is party to any other agreement with the relevant issues relating to the provision of investment banking services.
- In general terms, the effective organisational and administrative arrangements set up within the firm for the prevention of avoidance of conflicts of interest with respect to research recommendations, including information barriers.

2.4.6 Whistleblowing

Increasingly, regulators rely on whistleblowers in their battle against market abuse. A whistleblower is a person (typically an employee) who exposes any kind of information, behaviour, or activity deemed illegal, unethical, or incorrect within a private or public organisation. Regulators and companies encourage staff to speak up, and through legislation, regulation, and internal procedures, protection for these individuals is improving.

In the US, for example, whistleblowers involved with the securities markets are provided incentives and protection by the Dodd–Frank Wall Street Reform and Consumer Protection Act (2010).

In the UK, the Public Interest Disclosure Act 1998 provides a framework of legal protection for individuals who disclose information, so as to expose malpractice and matters of similar concern. It protects whistleblowers from victimisation and dismissal.

Firms need to put in place appropriate arrangements that allow staff to raise concerns about any malpractice with their manager, a senior executive or an independent function like compliance. If they feel uncomfortable raising the matter internally, the firm should also provide details of an external body such as private or charitable services. In some cases, regulators themselves provide a telephone hotline or an email address for staff to contact.

Firms need to have a written policy and procedures in place which are communicated to staff on induction and periodically.

Effective whistleblowing arrangements are key to good governance and anti-corruption. Equally, they reflect sound corporate culture. If not addressed, unethical or illegal conduct can lead to significant corporate failure and loss of value. In addition, effective whistleblowing arrangements will help with the detection and prevention of bribery and corruption, tax avoidance, money laundering, and other governance-related issues. In turn, this can result in better performance and will assist in meeting the Sustainable Development Goals (SDGs) because of the increase in transparency and fairness.



3. Fair Conduct



- 4.3.1 Understand expected compliant standards of behaviour for firms and individuals: honesty and fair treatment; acting in the client's best interest
-

3.1 Honesty and Fair Treatment

The key attributes of a successful industry are a good reputation and the trust of the public. A vital part of maintaining a strong reputation and trust is dealing with investors and customers honestly and fairly.

A firm must pay due regard to the interests of its customers and treat them fairly. Firms should conduct business with due skill, care and diligence; take reasonable care to organise and control affairs responsibly and effectively with adequate risk management systems; provide clear, fair and not misleading information to meet client needs; and ensure the suitability of their advice and discretionary decisions for customers. The principle that a financial firm must act in the best interest of their retail client, and have a

duty to protect them from financial harm are applied universally in different formats but with the same intention.

The **Financial Conduct Authority (FCA)**, for example, has identified six key outcomes for retail customers as follows:

1. Consumers can be confident that they are dealing with firms where the fair treatment of customers is central to the corporate culture.
2. Products and services marketed and sold in the retail market are designed to meet the needs of identified consumer groups and are targeted accordingly.
3. Consumers are provided with clear information and are kept appropriately informed before, during and after the point of sale.
4. Where consumers receive advice, the advice is suitable and takes account of their circumstances.
5. Consumers are provided with products that perform as firms have led them to expect, and the associated service is of an acceptable standard and as they have been led to expect.
6. Consumers do not face unreasonable post-sale barriers imposed by firms to change product, switch provider, submit a claim or make a complaint.

Firms are expected to be able to demonstrate that they are consistently treating their customers fairly and delivering fair outcomes relevant to their business. A firm needs to be able to:

- demonstrate that senior management have instilled a culture whereby they understand:
 - what the fair treatment of customers means
 - where they expect their staff to achieve this at all times, and
 - where (a relatively small number of) errors are promptly found, put right and learnt from

- appropriately and accurately measure performance against all customer fairness issues materially relevant to its business, and be acting on the results
- deliver those fair outcomes, and
- have no serious failings – whether seen through management information (MI) or known to the regulator directly.

Regulators will consider a firm's record in these areas when carrying out risk assessments of the firm and its supervisory approach. It is in the firm's interest to be able to demonstrate that treating customers fairly and honestly goes beyond just words and is followed through in practice.

3.2 Acting in the Client's Best Interest

Similarly, regulators expect firms and individuals to act in the best interest of their clients. Where any conflict of interest arises, the expectation is that it will be resolved in the best interests of the client.

Firms are also expected to act in the customer's best interest with regard to advice, ensuring the suitability of the advice and any investments recommended. They should, for example, avoid any bias in their recommendations which might arise as a result of commission or other remuneration.

3.3 How does Fairness Impact on Firms?



4.3.2 Understand how the concept of fairness impacts on financial services firms

Fairness is difficult to define as it involves a subjective assessment by one participant in the relationship in relation to the treatment

they have received from the other. Different people may have different expectations of fairness, which complicates the position of a firm trying to assess if its actions have been fair to a particular customer or market segment.

Firms should, therefore, ensure that any policy material is carefully worded where any aspect of fairness is being considered, to ensure that the policy can be consistently applied and demonstrated as being part of the company's approach to doing business. Other aspects that the firm might consider from the perspective of fairness include:

- incorporating the concept in the firm's strategy so that it is reflected in any new products and services
- observing compliance standards
- embedding fairness through the training of staff and measurement through monitoring compliance with the standards and other management information
- the need for transparency and detailed disclosure to clients and counterparties and the provision of information which is clear, fair and not misleading, and
- the provision of unbiased advice and recommendations which are in the interests of investors.

3.4 Financial Advice – Relevant Legal Concepts and Considerations



4.3.3 Understand legal concepts and considerations relevant to financial advice

The relationship between an adviser and their client is subject to the following legal concepts and considerations:

- **Law of contract and capacity** – the client will normally enter into an agreement with the adviser for the provision of advice. Capacity relates to the ability of the client to enter into a contract. Minors (children) and the incapacitated may require someone to contract on their behalf. In the case of children, an appropriate adult (eg, a parent or guardian) and for the incapacitated, an appointed legal personal representative or someone appointed by an appropriate court.
- **Law of agency** – the adviser may act on behalf of the client for activities such as buying and selling investments in the client's name or collecting income. In giving instructions, the adviser becomes an agent of the client and their actions may be binding on the client.
- **Legal identity** – the legal person is a physical body that has rights and duties on the one hand and certain behaviours and capability, eg, to contract, on the other. Companies and other entities are also legal bodies in law, with defined rights and duties. Incorporated bodies are entities in their own right with defined rights and duties, while unincorporated bodies are collectives in which rights and duties are held against its members.
- **Property ownership** – where advice is given, ownership of assets will normally vest in the name of the client, although some advisory firms may also offer custodial or trust services. In the latter case, assets may be registered in the name of a nominee or trustee.
- **Powers of attorney** – the client appoints one or more individuals to act on their behalf. The client may use a power of attorney, for example, where they wish another to take decisions on their behalf, in anticipation of some incapacity or perhaps in cases where they may be going overseas for a period.
- **Law of succession** – this may be an important consideration where the client wishes to pass on assets to their heirs, or

otherwise make provision for them.

- **Insolvency and bankruptcy** – this is an important consideration in that advice may be necessary to ensure the client does not contravene laws relating to insolvency or bankruptcy.
- **Use of trusts** – this is a legal arrangement whereby assets are managed by a person, persons or organisation for the benefit of another. In some countries they are commonly used in inheritance or estate planning to reduce the impact of tax. In others it is used to ensure an appropriate provision is made for dependants on the death of an individual, or funds can be made available to dependants in a controlled manner.

3.5 Senior Management Responsibilities, Management Information and Corporate Culture



4.3.4 Understand the role senior management play in maintaining fair conduct: senior management responsibilities; management information; corporate culture

The firm's executive management should expect to be questioned on how they maintain fair conduct and treatment of customers. This will form an integral part of the assessment regulators make of the firm. They will also need to demonstrate that the firm's management information (MI) is picking up the issues regulators may discover during periodic reviews of the business. The following expectations of regulators help senior management identify barriers to delivery of treating customers fairly outcomes in the culture of the firm:

- Leadership is central – where there is strong leadership with a clear vision of what treating customers fairly means for the firm, there is more likely to be a corporate culture which is geared towards delivering fair consumer outcomes.
- The integration of fair conduct and treatment into the firm's strategy is very important – in any developments in significant new products or target markets, or outsourcing arrangements, we would expect fair treatment implications for customers to be an automatic feature of those strategies. As current market conditions cause firms to alter their strategic direction, senior management should consider the implications for customers an integral part of their planning.
- Decision-making within the firm will also impact controls, including MI, which are also important so that senior management in the firm can satisfy themselves that the customer is being treated fairly.
- People issues – recruitment, training and competence – firms can influence the delivery of fairer outcomes by recruiting staff with appropriate values and skills, training them effectively and assessing their competence.



4. Client Outcomes



- 4.4.1 Understand how associated but non-transactional activities impact on the firm: product design and marketing; financial promotions/advertising; client documentation; fair contracts
-

4.1 Product Design and Marketing

Regulators typically authorise and regulate firms and ensure that the people who manage them are competent to do so. They may also regulate the design and marketing of financial products, particularly retail products. The extent to which regulators get involved in the detailed regulation of products varies across the world, but the financial crisis has prompted regulators to re-assess their approach and make changes where they think it appropriate. Regulators assess whether firms ensure that the fair treatment of customers is built into their governance and oversight arrangements.

What regulators look for may include:

- **Governance and oversight:**
 - a board engaged in ensuring products deliver the right outcomes for consumers
 - clearly allocated responsibilities for oversight of product governance
 - the effective inclusion of control functions such as compliance in oversight arrangements
 - policies and procedures that support the design of products appropriate to a specified target market
 - a design process that leads to appropriate matching of products to the needs of the target market, and
 - clear consideration of what customer usage or needs the product would not fulfil.
- **Target market:**
 - a target market that is plausible in terms of size, type of customers, geographical locations etc, and
 - products designed to meet customer needs – not simply copying a competitor's product.
- **Distribution:**
 - controls in place that ensure the distribution channels and strategy are compatible with the target market
 - details of the target market, product features and risks being accurately conveyed to distributors
 - interactions and communications with distributors that are likely to lead to fair customer outcomes, and
 - the firm taking action to address any mismatches between the actual distribution/sales and the intended target market.

4.2 Financial Promotions/Advertising

Firms must ensure that communications relating to investment business, including financial promotions are fair, clear and not misleading. The way in which this is achieved should be appropriate and proportionate and take account of the means of communication and what the communication is intended to convey. So, for example, communications aimed at professional clients may not need to include all the same information as those aimed at retail clients.

It is normal for the compliance function to review such promotions and approve them; the review is to ensure that it complies with the rules governing financial promotions which may also include advertising standards.

Firms should ensure that:

- any risk to a client's capital is made clear
- any quoting of yields gives a balanced impression of both the short-term and long-term prospects for the investment
- any complex charges for products or services are communicated fairly, clearly and in a manner which is not misleading, and
- that the firm's regulator is named.

In some cases, the firm's promotional literature might be used by other firms (eg, distributors or intermediaries) when selling packaged products. Any firm relying on promotional materials produced by another party should:



Take reasonable care to establish that an authorised firm has confirmed that the promotion complies with the rules.



Take reasonable care that it communicates it only to the type of recipient it was intended for.



As far as it is (or should be) aware, the promotion is still fair, clear and not misleading, and has not been withdrawn by the other party.



Ensure that the materials give a fair and not misleading impression of the producer of the product.

4.3 Client Documentation

A regulated firm will need to provide various pieces of documentation to its clients. The specific documents are determined by the role the firm is fulfilling, the types of activities it is undertaking, and the types of assets concerned. Key documents include:

- **key product information**, including a prospectus, terms and conditions and details of complaint and compensation procedures
- **suitability report**, based on an assessment of the client's needs and their risk appetite

- **contract note or deal confirmation**, showing the details of any transaction performed (eg, the asset, the price, the number of shares)
 - where provided, details of **cancellation or cooling-off rights**, ie, where the investor has the right to change their mind
 - **regular statements**, showing, for example, any additional investments and income reinvested
 - **tax certificates** relating to income earned/distributed, and
 - **annual and interim reports**, issued by the product provider and where appropriate or required regular valuations.
-

4.4 Fair Contracts

Firms should, in good time, before a retail client is bound by any agreement relating to investment business or ancillary services or before the provision of those services, whichever is earlier, provide that client with:

- the terms of any such agreement, and
- the information about the firm and its services relating to that agreement including authorised communications, conflicts of interest and the firm's authorised status.

Firms should provide the agreement and information in durable medium or via a website, where the website conditions are satisfied. Durable medium could include a printed document or an email attachment. A firm may provide the agreement and the information immediately after the client is bound by any such agreement if the agreement being concluded was made using email, telephone, or other types of not in-person communication.

A firm should establish a record that includes the agreement between itself and a client which sets out the rights and obligations of the parties, and the other terms on which it will provide services

to the client. The records should be maintained for an appropriate period, normally whichever is the longer between:

- five years
- the duration of the relationship with the client, or
- in the case of a record relating to certain pension transfers, indefinitely.

The Unfair Contract Terms Act 1977 is an Act of Parliament of the UK which regulates contracts by restricting the operation and legality of some contract terms. It extends to nearly all forms of contract and one of its most important functions is limiting the applicability of disclaimers of liability. The terms extend to both actual contract terms and notices that are seen to constitute a contractual obligation. Firms should not reduce their liability by using terms such as 'excluding' or 'limiting liability' unless it is reasonable and not acting against the customer.

4.5 Client and Counterparty Objectives and Risk Profile



4.4.2 Understand the factors to consider prior to entering into a transaction: client/counterparty objectives; client/counterparty risk profile; affordability; suitability of the investment

4.4.3 Understand factors that should be considered at the point of sale: clear information; suitability of advice

The goal of both parties to a contract is that the delivery and settlement of the transaction will take place. Where a deal takes place on a regulated market, the client will have reasonable assurance that the counterparty, for example, a market maker, has

met minimum requirements for admission to membership of the exchange or market. The counterparty will look to the broker's track record for reassurance that the client will pay the consideration for the purchase of an investment or deliver the stock if the client is selling. For example, the use of Delivery versus Payment (DvP) systems in which the transfer of securities only takes place once payment is made, is provided by recognised exchanges and serve to provide reassurance and confidence to both parties. In the case of exchange-traded derivatives, there will be a **Central Counterparty (CCP)** which will stand behind the settlement and clearing of transactions.

In the case of off-exchange transactions, there will be greater risk that the counterparty may not deliver. The difficulties with **Credit Default Swaps (CDSs)** and the inability to deliver the underlying sub-prime mortgage-based assets proved to be a major illustration of the failure of markets to recognise the risks involved and led to the collapse of Lehman Brothers, a significant counterparty to many traders.

The role of the compliance function is to ensure that appropriate due diligence is undertaken both on clients through thorough know your customer (KYC) assessments and on market counterparties. The KYC process will also involve the firm in ensuring they have a full understanding of the client's risk appetite. In order to do so, the firm will typically request the customer to complete a survey that will help them assess what level of risk the customer is willing to take. Generally, there are 3 categories:

- **Risk taker** – customer is willing to risk some or all of their investments to obtain a return
- **Risk neutral** – customer is willing to take some risk
- **Risk averse** – customer is not willing to take any risk.

Each of these can be further sub divided into low, medium, and high to further fine tune the type of products and services that are suitable for them. The risk profile of a customer changes over time

depending on their age and circumstances and will need to be reviewed on a regular basis.

4.6 Affordability/Suitability of the Investment

It is the responsibility of the firm to ensure that contracts being transacted are within the means of the client and are appropriate given their risk profile.

For example, a product that requires the client to invest a monthly amount of \$1,000 is not affordable if the client's income is \$2,000 since in that case, they are unlikely to be able to meet their monthly cost of living. Similarly, if such a client is assessed as a high risk-taker, but is entirely dependent on the income of the investment, cannot afford to invest in high-risk junk bonds.

Affordability and suitability go hand in hand since a product that is not affordable is certainly not suitable.

In addition, it is the firm's responsibility to ensure contracts are appropriate and suitable given the client's risk profile. Rules on appropriateness and suitability exist to ensure that firms providing services of advice or investment management take reasonable steps to ensure that personal recommendations (or decisions to trade) are appropriate or suitable for their clients' needs. Note that the rules on appropriateness apply to services of execution-only orders, and the rules on suitability to firms making a personal recommendation relating to designated investments and when they manage investments (ie, advisory or discretionary services).

When a firm makes a personal recommendation, or is managing a client's investments, it should obtain the necessary information regarding the client's:

- knowledge and experience in the investment field relevant to the specific type of designated investment business
- financial situation, and
- investment objectives, enabling the firm to make recommendations, or take the decisions which are suitable for the client.

A firm should provide a retail client with a suitability report if it makes a personal recommendation that the client:

- invests in a packaged product such as a mutual fund or regular savings scheme linked to such a fund or investment company
- buys, sells, surrenders, converts or cancels rights under, or suspends contributions to, a personal pension scheme
- elects to make income withdrawals or purchases a short-term annuity
- enters into a pension transfer or pension opt-out, or
- takes out, or modifies, a life assurance policy.

The suitability report includes an overview of the client's risk profile, personal circumstances, investment horizon, and current financial status and will be shared with the client to ensure it is complete and accurate.

4.7 Factors Prior to Entering Into a Transaction

Certain obligations will arise prior to entering into a transaction. Where the firm has provided financial advice to the client, specific documentation must be provided in which the firm explains the advice and the implication as well as a justification explaining why the advice provided was correct and appropriate. This material can often be lengthy – not only because of the complexity of aspects of

the advice process, but because firms are keen to demonstrate the basis on which advice was provided, to both regulators and ombudsmen.

Given the potential financial and reputational implications of a sustained ombudsman investigation, firms providing advice will be keen to demonstrate why certain approaches were rejected or certain types of investment assets dismissed from their planning. Otherwise, in the future, it might be claimed that the adviser did not consider all the asset types that should have been discussed.

4.8 Post-Sale Factors



4.4.4 Understand post-sale factors that may impact on the firm: handling complaints in line with international standards; avenues of redress; expected and actual product performance; safeguarding customer money and assets; reporting requirements

4.8.1 Handling Complaints in Line with International Standards

The International Standards Organisation (ISO) is an independent, non-governmental organisation that develops standards to ensure the quality, safety and efficiency of products, services and systems. Standard (ISO 10002) is a general standard to guide companies in the handling of complaints and in which they may gain accreditation which may be adopted subject to local regulatory requirements.

The Standard sets out guiding principles (including in respect of responsiveness and objectivity in complaint handling) before considering the different operational stages of a complaint. The

Standard provides a framework by which a firm can consider whether its complaint-handling approach is sufficient.

This is in respect of stages such as:

- receiving a complaint
- acknowledging a complaint
- investigating a complaint
- responding to a complaint, and
- closing a complaint.

4.8.2 Avenues of Redress

Contacting the Firm Directly

When a client has a complaint, the usual process is for them to first approach the firm to seek resolution. Regulators will normally encourage the client to contact the firm directly as soon as possible. Typically, regulated firms are required to investigate complaints promptly and reply to the client within an appropriate period, eg, eight weeks, either with the outcome of the investigation, or to inform the client they need more information.

Contacting the Financial Ombudsman

If an investor is not satisfied with the firm's response, an ombudsman service may be able to help. Although the scope and jurisdiction varies per country or region, these schemes typically cover a wide range of financial services including banking, insurance, mortgages, and credit cards. Their scope is related to disputes on misselling of financial products, complaints, disputes over insurance claims, issues with products and services, and allegations of misconduct or negligence. Their service is usually free and independent. The financial ombudsman scheme has the potential to improve accountability and increase trust in financial services.

In the UK, for example, the Financial Ombudsman Service (FOS) will ask the firm to explain what happened and then decide whether to uphold the complaint. Clients should usually contact the FOS within a fixed period of receiving the original response from the firm (eg, six months). In the UK, the FOS can now make awards of up to £455,000 for complaints referred to them after 1 April 2025 regarding acts and omissions by firms on or after 1 April 2019.

Taking Civil Action through the Courts

If the client remains unsatisfied, as a last resort, they can take the case to court. However, the client cannot usually take their complaint to court if they have already been through a complaints scheme or accepted an Ombudsman's decision.

4.8.3 Expected and Actual Product Performance

The expected investment performance and the actual performance may vary because of market movements, the economic conditions and the performance of individual companies or funds. Where the firm provides ongoing advice as part of its service, the firm will be expected to review the performance of the client's investments, provide periodic valuations and update the client on progress against the client's original investment objectives.

4.8.4 Safeguarding Customer Assets and Client Money

When holding client assets in safe custody, firms need to make adequate arrangements to safeguard clients' ownership rights, especially in the event of the firm's insolvency and to prevent the use of safe custody assets belonging to a client on the firm's own account, except with the client's express consent.

Firms should also introduce adequate organisational arrangements to minimise the risk of loss or diminution of the client's safe custody

assets. Firms must take the necessary steps to ensure that client money is held in an account(s) identified separately from any accounts used to hold money belonging to the firm.

National rules will confirm how such segregation is achieved – in particular, the actions required when a firm receives client money. For example, a firm that operates the 'normal approach' to segregation must promptly place client money received into one or more accounts opened with any of the following (as permitted by the regulations):

- a central bank
- an institution authorised to hold client money
- a bank authorised in a third country, or
- a qualifying money market fund.

In the UK, for example, there have been a number of high-profile and high-value penalties issued by the FCA, most of which did not result in an actual loss by any investor. Rather, the FCA is responding to the failure of the firm to establish and maintain processes and procedures that deliver compliance, and the risk exposure that arises where such controls are deficient.

4.8.5 Reporting Requirements

Any complaints need to be clearly recorded and key information must be reported to the regulator on a periodic basis including the number and types of complaints, whether they were resolved within the regulatory prescribed period, and the proportion not resolved. Records need to be maintained for a prescribed period.

Client assets and client money need to be reconciled on a daily basis, and typically any discrepancy needs to be reported to the regulator immediately after it has been found. The report needs to

include a description of why the discrepancy has occurred and the steps taken to resolve it.



5. Environmental, Social and Governance (ESG)



- 4.5.1 Know what is meant by environmental, social and governance (ESG)
- 4.5.2 Know the main international ESG initiatives: Task Force on Climate-Related Financial Disclosures (TCFD); United Nations supported Principles for Responsible Investment (PRI); Sustainable Finance Disclosure Regulations (SFDR)
- 4.5.3 Understand the importance of initiatives on: climate; green finance; corporate social responsibilities

Although industry professionals and investors use terms such as ESG, socially responsible investing (SRI), and ethical investing interchangeably, there are some nuances to note. ESG refers to a focus of investments in ESG factors based on their investment potential. SRI considers the ESG factors, but is driven by the individual values of the investors. Ethical investing refers to an

investment strategy based on the ethical principles of the investor or fund manager and typically excludes specific industries.

Each encompass how an investor might use their power as a shareholder to encourage better environmental and social behaviour from the companies they invest in. ESG are non-financial performance indicators to assess the impact of the firm or the investment on society.

As awareness of market activity and investment processes increased, investors have been seeking services that reflected their own ethical values, such as an attitude towards smoking, armaments, and environmental issues. Ethical finance is, therefore, concerned with investment decisions being underpinned and with environmental, social and/or ethical factors.

An example of ethical finance is money invested with an ethical provider that will be reinvested into institutions that benefit the environment locally, regionally, or globally, such as organic farming enterprises and human rights issues.

5.1 International ESG Initiatives

There are a number of international ESG initiatives that aim to promote and improve investments in ESG.

Taskforce on Climate-Related Financial Disclosures (TCFD)

Issued in 2017, and updated in 2021, the TCFD[♦] was established by the Financial Stability Board (FSB) with the goal to develop recommendations for more effective climate-related disclosures. On 23 October 2025, TCFD published their final status report and is now disbanded. The aim of the disclosures was to promote more informed investment, credit, and insurance underwriting decisions and, in turn, enable a better understanding of concentrations of carbon-related assets in the financial sector and the exposure of the

financial system to climate-related risks. A better understanding of the financial implications associated with climate change will empower market participants to channel investments to sustainable and resilient solutions, opportunities, and business models.

The TCFD has issued their recommended disclosures structured around four identifiable themes:

1. Governance

- Describe the board's oversight of climate-related risks and opportunities.
- Describe management's role in assessing and managing climate-related risks and opportunities.

2. Strategy

- Describe the climate-related risks and opportunities the organisation has identified over the short, medium, and long term.
- Describe the impact of climate-related risks and opportunities on the organisation's businesses, strategy and financial planning.
- Describe the resilience of the organisation's strategy, taking into consideration different climate-related scenarios, including a two degrees Celsius or lower scenario.

3. Risk Management

- Describe the organisation's processes for identifying and assessing climate-related risks.
- Describe the organisation's processes for managing climate-related risks.
- Describe how the processes for identifying, assessing, and managing climate-related risks are

integrated into the organisation's overall risk management.

4. Metrics and Targets

- Disclose the metrics used by the organisation to assess climate-related risks and opportunities in line with its strategy and risk management process.
- Disclose greenhouse gas (GHG) emissions, and their related risks. The three Scopes are different classifications relating to a company's emissions; for instance, emissions resulting from the company's operations or from employee commuting.
- Describe the targets used by the organisation to manage climate-related risks and opportunities, and performance against targets.

The TCFD developed specific additional guidance for the financial sector, as well as non-financial groups for recommendations related to strategy, risk management and metrics, and targets.

United Nations-Supported Principles for Responsible Investment (PRI)

The PRI defines its mission as follows:

'We believe that an economically efficient, sustainable global financial system is a necessity for long- term value creation. Such a system will reward long-term, responsible investment and benefit the environment and society as a whole.'

The PRI will work to achieve this sustainable global financial system by encouraging adoption of the Principles and collaboration on their implementation; by fostering good governance, integrity and accountability; and by addressing obstacles to a sustainable financial system that lie within market practices, structures and regulations.'

To achieve this mission, the PRI issued the following six principles:

- **Principle 1:** incorporate ESG issues into investment analysis and decision-making processes.
- **Principle 2:** be active owners and incorporate ESG issues into our ownership policies and practices.
- **Principle 3:** seek appropriate disclosure on ESG issues by the entities in which we invest.
- **Principle 4:** promote acceptance and implementation of the Principles within the investment industry.
- **Principle 5:** work together to enhance our effectiveness in implementing the Principles.
- **Principle 6:** each report on our activities and progress towards implementing the Principles.

The principles are voluntary, internationally-recognised investment principles offering a range of options for the incorporation of ESG into investment practice. In order to become a signatory, an organisation has to promise to incorporate ESG into their investment practices.

Sustainable Finance Disclosure Regulations

The Sustainable Finance Disclosure Regulations (SFDR) have been in force since 2021 and require fund managers, financial advisers, and other regulated firms to provide prescriptive and standardised disclosures on how they integrate ESG factors at the product and organisation level. The SFDR define proposals for the content, methodologies and presentation of sustainable disclosures in the following areas:

1. Principal adverse impact disclosures
2. Pre-product disclosures
3. Website product disclosures
4. Product periodic disclosures.

The SFDR is a European regulation introduced to:

‘improve transparency in the market for sustainable investment products, to prevent greenwashing and to increase transparency around sustainability claims made by financial market participants.’

In November 2025, changes are proposed to simplify the rules, lower the administrative burden, and improve enforcement. The changes will apply 18 months after SFDR2.0 comes into force, the date of which has not yet been announced.

SFDR requires financial market participants and financial advisers to disclose the following information on their website.

Type of information	Financial Market Participant	Financial Adviser
Sustainable risk policy	Information about policies on the integration of sustainability risks into the investment decision-making process.	Information about policies on the integration of sustainability risks into the investment or insurance advice.
Adverse sustainability impact	Consideration of principal adverse impacts of an investment decision on sustainability. Statement on due diligence policy mandatory for large entities and holdings. Comply or explain for all other entities.	Consideration of principal adverse impacts on sustainability factors in the investment or insurance advice. Comply or explain.

Remuneration policies	Confirmation remuneration policies are consistent with the integration of sustainability risks.	
------------------------------	---	--

The SFDR defines a number of mandatory and voluntary adverse sustainability indicators in relation to climate and the environment, as well as to factors related to social issues, employee rights, human rights, anti-corruption and anti-bribery. The sustainability factors are pre-defined and consist of:

- 32 mandatory indicators (16 environmental and 16 social), and
- 18 voluntary indicators (11 environmental and 7 social).

Other Examples

In addition to the PRI, TCFD, and SFDR which have international reach, there are a number of national initiatives such as the following:

- **USA** – the Environmental Marketing Guides (also called the Green Guides), which were finalised in 2020, include warnings about the use of blanket claims in marketing such as ‘eco-friendly’, third- party certifications where the terms of qualification are not specified.
- **China** – in 2018, the regulator released new guidelines whereby independent green bond verifiers must confirm a bond’s green credentials each year. A breach of the regulations will be subject to a penalty.
- **Singapore** – the Monetary Authority of Singapore (MAS) enhanced climate-related financial disclosures for banks and asset managers as part of its Green Finance Action Plan.

- **UK** – is developing their own Sustainability Disclosure Requirements (SDR) which will require certain investment products to display, among others, their sustainability characteristics.

5.2 Impact of Initiatives on Environmental and Corporate Responsibility

Corporate social responsibility (CSR) is a form of corporate self-regulation integrated into the business model of a company. CSR policy functions as a built-in, self-regulating mechanism whereby a business monitors and ensures its active compliance with the spirit of the law, ethical standards, and international norms. ESG criteria are a set of standards used by socially responsible investors to screen potential investments.

The goal of CSR is to embrace responsibility for the company's actions and encourage a positive impact on the environment, consumers, employees, communities, stakeholders and all other members of the public sphere.

Furthermore, CSR-focused businesses proactively promote the public interest by encouraging community growth and development, and voluntarily eliminating practices that harm the public sphere, regardless of legality. CSR is the deliberate inclusion of public interest into corporate decision-making, that is the core business of the company or firm, and the honouring of a triple bottom line: people, planet, and profit.

In crowded marketplaces, companies strive for a unique selling proposition that can separate them from the competition in the minds of consumers. CSR can play a role in building customer loyalty based on distinctive ethical values. Companies like to highlight their ethical values in their marketing material. Business service organisations can benefit from building a reputation for

integrity and best practice. However, once CSR is placed at the heart of the firm's market positioning, any failure to live up to those ideals will undermine customer trust and can have a substantial negative impact on the organisation. It could, for example, result in difficulties hiring qualified staff, shareholders disinvesting, or loss of customers.

The OECD has issued a number of reports, guidelines and principles including the following:

- **Guidelines for Multinational Enterprises** – Recommendations to multinational enterprises operating in, or from, adhering countries. They provide voluntary principles and standards for responsible business conduct in areas such as employment and industrial relations, human rights, environment, information disclosure, combating bribery, consumer interests, science and technology, competition, and taxation ♦.
- **Principles of Corporate Governance** – international standard for corporate governance to assist policy makers to evaluate and improve their legal, regulatory, and institutional framework.
- **Convention on Combating Bribery** – international anti-corruption instrument focused on the supply side of the bribery (ie, the person or entity offering the bribe).

In addition, the International Organisation of Securities Commissions (IOSCO) has published a Model Code of Ethics which recommends that firms adopt the following ethical principles:

- Integrity and truthfulness
- Promise-keeping
- Loyalty (fully disclosing conflicts of interest)
- Fairness to the customer
- Maintaining confidentiality.

It is important to ensure that any code of ethics is more than mere statements; there must also be a robust ethics education

programme in place.

CSR initiatives related to climate change (to support mitigation and adaptation actions to reduce the impact of climate change) and green finance (to generate a better overall environmental outcome) are becoming increasingly important to investors, indicating that companies and businesses are now more focused on investing in carbon neutrality-related outcomes. Investors and financial services firms are actively looking for sustainable investments and projects, and are either engaging more with the decisions of the companies or divesting in activities that negatively impact the environment, particularly in the context of climate change.



End of Chapter Questions

1. Name three of the standards and principles set out by regulators which they expect business and key individuals to observe.

- Integrity – a firm must conduct its business with integrity.
- Customers' interests – a firm must pay due regard to the interests of its customers and treat them fairly; and provide them with information which is clear, fair and not misleading; and advice which is suitable.
- Market conduct – a firm must observe proper standards of market conduct.
- Client assets – a firm must arrange adequate protection for clients' assets when it is responsible for them.

Answer reference: Section 1.2

2. Name three Chartered Institute for Securities & Investment (CISI) Code of Conduct Principles.

The CISI code of conduct principles are:

1. Personal Accountability
2. Client Focus
3. Conflict of interest
4. Respect for market participants
5. Professional development
6. Aware of capabilities
7. Respect others and the environment
8. Speak up & listen up

Answer reference: Section 1.3.1

3. What would be included in an internal code of conduct?

Many firms in financial services have adopted their own internal codes of conduct and ethics which they communicate to staff and customers. Such codes may reflect the aim of good ethical behaviour as well as regulatory compliance.

Answer reference: Section 1.4

4. What is a fiduciary duty?

The term 'fiduciary duty' originates from the Latin *fiduciarius*, meaning '(holding) in trust'; from *fides*, meaning 'faith' and *fiducia*, meaning 'trust'. It is a legal or ethical relationship of confidence or trust regarding the management of money or property between two or more parties, most commonly a fiduciary and a principal. The fiduciary (for example, a corporate trust company or the trust department of a bank) holds a fiduciary relation or acts in a fiduciary capacity to the principal (for example, a person whose funds are entrusted to it for investment).

5. What are the components to create an ethical culture?

- Instil the basics. An ethics or compliance function and articulated professional ethics standards are the foundations on which the other parts are built.
- Develop a well-known policy of 'programme follow through' which not only tries to detect violators but also follows up on the ethical concerns raised by employees. This is key, as it helps to demonstrate that the company and, specifically, the company leadership are committed to an ethical culture.
- Recognise that ethical and effective leadership creates 'an ethical tone' in companies, which employees detect and to which they respond. This ethical leadership should not be overlooked or understated as employees look to their leaders and managers for their own ethical tone. Thus, employees will have a more serious view of ethics if they perceive that their leaders and managers pay attention to, and promote, ethical behaviour.
- Make ethics discussions a part of normal day-to-day activities. Ethics discussions should be woven into the corporate culture by making ethics concerns part of the norm.
- Implement a simple rewards system for ethical conduct that demonstrates the company's endorsement of an ethical culture and gives additional public examples of the company's focus on ethical actions.
- Reinforce ethical standards on a regular, repeating basis.

- Monitor and keep in touch with employee concerns about ethics. This provides valuable insight both into where, and how, real ethics violations are going to occur, and how employees perceive the ethical culture within the company

Answer reference: Section 1.5.7

6. Name four of the benefits of fair and orderly markets.

The benefits of fair and orderly markets include:

- Investors will have the confidence to invest in securities issued by businesses which need to raise capital.
- They help to establish the environment to encourage economic development and wealth creation.
- They allow the transfer of capital between enterprises at fair prices for minimal cost.
- They successfully provide liquidity through the speed and ease with which capital transfers can be affected, and buyers and sellers are able to locate counterparties willing to trade a wide range of securities at acceptable prices quickly and efficiently.
- Investors can be reassured that settlement and delivery of stock will take place.
- Information will be readily available to ensure transparency.
- The way in which securities trades are handled and cleared will be controlled and rules adopted aimed at limiting the volatility of security prices.

Significant resources will be applied to the identification and prevention of market abuse.

Answer reference: Section 2.1

7. What are Information barriers?

An Information barrier, also known as a Chinese wall is the term given to arrangements made by a firm to manage conflicts of interest where information held by an employee in one part of the business must be withheld from (or, if this is not possible, at least not used by) the people working in another part of the business.

Answer reference: Section 2.4.1

8. What arrangements must a firm have in place under personal account (PA) dealing?

Firms must have arrangements in place to prevent their employees who are 'relevant persons' and involved in activities that could lead to conflicts of interest, or who could have access to inside information or other confidential client information, from:

1. entering into a personal transaction that is contrary to the Market Abuse Directive; involves misuse or improper disclosure of confidential information, or conflicts with the firm's duties to a customer
2. improperly advising or procuring that anyone else enters into a transaction that (if it had been done by the employee himself) would have fallen foul of the above or of a 'relevant provision', or
3. improperly disclosing information or opinion, if they know or should know that the person to whom he has disclosed it is likely to enter into a transaction that (if it had been done by the employee himself) would have fallen foul of the above or of a relevant provision, or encouraging someone else to do so.

Answer reference: Section 2.4.3

9. What could be classed as a lavish gift?

A holiday.

Answer reference: Section 2.4.4

10. What are the six fair approach outcomes for customers in the retail area?

The Financial Conduct Authority (FCA), for example, has identified six key outcomes for retail customers as follows:

1. Consumers can be confident that they are dealing with firms where the fair treatment of customers is central to the corporate culture.
2. Products and services marketed and sold in the retail market are designed to meet the needs of identified consumer groups and are targeted accordingly.
3. Consumers are provided with clear information and are kept appropriately informed before, during and after the point of sale.
4. Where consumers receive advice, the advice is suitable and takes account of their circumstances.
5. Consumers are provided with products that perform as firms have led them to expect, and the associated service is of an acceptable standard and as they have been led to expect.
6. Consumers do not face unreasonable post-sale barriers imposed by firms to change product, switch provider, submit a claim or make a complaint.

Answer reference: Section 3.1

11. Name four of the legal concepts and considerations that adviser and client relationships are subject to.

The legal concepts and considerations include:

- Law of contract and capacity
- Law of agency
- Legal identity
- Property ownership
- Powers of attorney
- Law of succession
- Insolvency and bankruptcy
- Use of trusts

Answer reference: Section 3.4

12. Who should expect to be questioned on how they maintain fair conduct and treatment of customers?

The firm's executive management should expect to be questioned on how they maintain fair conduct and treatment of customers, as this will form an integral part of the assessment regulators will make of the firm.

Answer reference: Section 3.5

13. What do regulators look for when ensuring that fair treatment of customers is built into governance and oversight arrangements?

- a board engaged in ensuring products deliver the right outcomes for consumers;

- clearly allocated responsibilities for oversight of product governance;
- the effective inclusion of control functions such as compliance in oversight arrangements;
- policies and procedures that support the design of products appropriate to a specified target market;
- a design process that leads to appropriate matching of products to the needs of the target market; and
- clear consideration of what customer usage or needs the product would not fulfil.

Answer reference: Section 4.1

14. What is covered under the Unfair Contract Terms Act 1977?

The Unfair Contract Terms Act 1977 is an Act of Parliament of the UK which regulates contracts by restricting the operation and legality of some contract terms. It extends to nearly all forms of contract and one of its most important functions is limiting the applicability of disclaimers of liability. The terms extend to both actual contract terms and notices that are seen to constitute a contractual obligation.

Answer reference: Section 4.4

15. What is the limit that the UK's Financial Ombudsman can award an eligible complainant?

The Ombudsman can now make awards of up to £455,000.

Answer reference: Section 4.8.2

16. Who can a firm open an account within order to hold client money?

National rules will confirm how such segregation is achieved – in particular, the actions required when a firm receives client money. For example, a firm that operates the 'normal approach' to segregation must promptly place client money received into one or more accounts opened with any of the following (as permitted by the regulations):

- a central bank
- an institution authorised to hold client money
- a bank authorised in a third country, or
- a qualifying money market fund.

Answer reference: Section 4.8.4

17. What is the general expectation for ESG?

The TCFD was established by the Financial Stability Board (FSB) with the goal to develop recommendations for more effective climate-related disclosures. On 23 October 2025, TCFD published their final status report and is now disbanded. The aim of the disclosures was to promote more informed investment, credit, and insurance underwriting decisions and, in turn, enable a better understanding of concentrations of carbon-related assets in the financial sector and the exposure of the financial system to climate-related risks. A better understanding of the financial implications associated with climate change will empower market participants to channel investments to sustainable and resilient solutions, opportunities, and business models.

Answer reference: Section 5.1

18. List the principal adverse disclosure requirements.

The TCFD has issued their recommended disclosures structured around four identifiable themes:

- **Governance**
 - Describe the board's oversight of climate-related risks and opportunities.
 - Describe management's role in assessing and managing climate-related risks and opportunities.
- **Strategy**
 - Describe the climate-related risks and opportunities the organisation has identified over the short, medium, and long term.
 - Describe the impact of climate-related risks and opportunities on the organisation's businesses, strategy and financial planning.
 - Describe the resilience of the organisation's strategy, taking into consideration different climate-related scenarios, including a two degrees Celsius or lower scenario.
- **Risk Management**
 - Describe the organisation's processes for identifying and assessing climate-related risks.
 - Describe the organisation's processes for managing climate-related risks.

- Describe how the processes for identifying, assessing, and managing climate-related risks are integrated into the organisation's overall risk management.
- **Metrics and Targets**
 - Disclose the metrics used by the organisation to assess climate-related risks and opportunities in line with its strategy and risk management process.
 - Disclose Scope 1, Scope 2, and, if appropriate, Scope 3 greenhouse gas (GHG) emissions, and their related risks. The three Scopes are different classifications relating to a company's emissions, for instance, emissions resulting from the company's operations or from employee commuting.
 - Describe the targets used by the organisation to manage climate-related risks and opportunities and performance against targets.

Answer reference: Section 5.1

Chapter Five

Governance, Risk Management and Compliance

Section 1

Corporate Governance

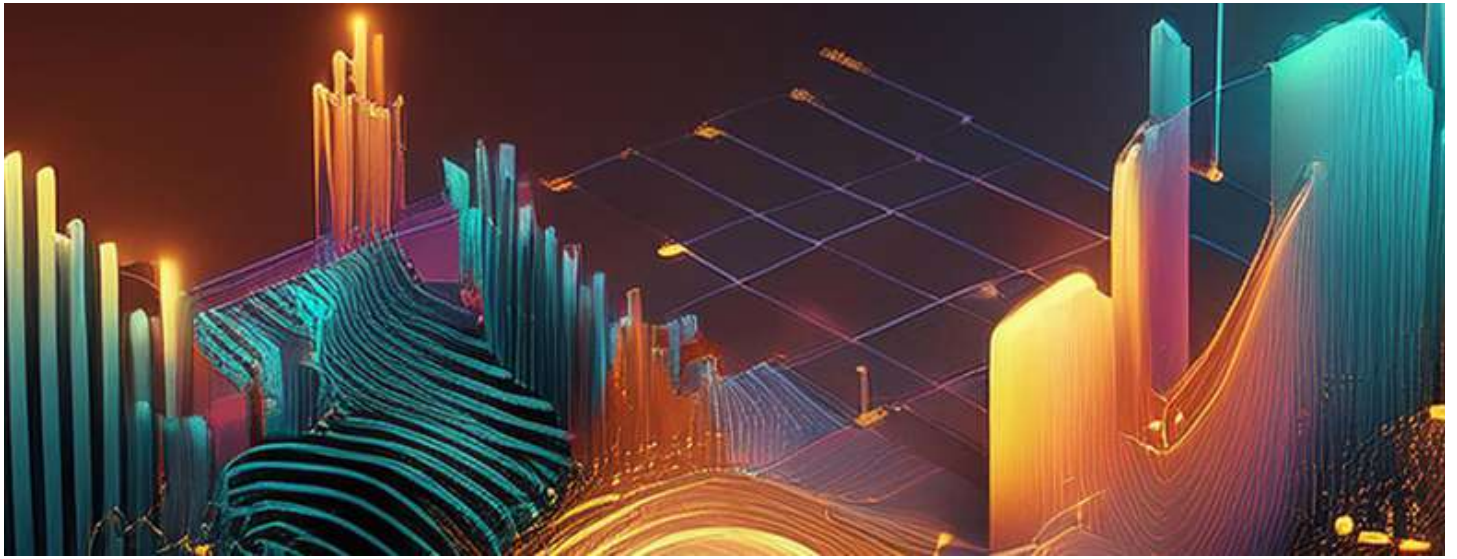
Section 2

Key Risk Types, their Application and Impact on the Compliance Function

Section 3

Compliance Risks

This syllabus area will provide
approximately 17 of the 100
examinations questions



1. Corporate Governance

1.1 Objectives of Corporate Governance



5.1.1 Understand the objectives of corporate governance

Effective corporate governance practices are essential to achieving and maintaining public trust and confidence in the banking system, which are critical to the proper functioning of the financial sector and economy as a whole. The Organisation for Economic Co-operation and Development (OECD) Principles of Corporate Governance[♦] define corporate governance as involving:

'a set of relationships between a company's management, its board, its shareholders and other stakeholders.'

Poor corporate governance can:

- Contribute to bank failures, which can pose significant public costs. Such failures also have the potential to impact on any applicable deposit insurance system, and there is the

possibility of broader macroeconomic implications (such as contagion risk and impact on payment systems). This was illustrated in the global financial crisis that began in mid-2007.

- Lead markets to lose confidence in the ability of a bank to properly manage its assets and liabilities, including deposits, which could in turn trigger a bank run or liquidity crisis.

In addition to their responsibilities to shareholders, banks also have a responsibility to their depositors, and to other recognised stakeholders. The legal system in each country determines the responsibilities a domestic bank may have to its shareholders, depositors and other relevant stakeholders, due to which, responsibilities may vary across jurisdictions.

Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. Good corporate governance should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and its shareholders and should facilitate effective monitoring. The presence of an effective corporate governance system, within an individual company or group and across an economy as a whole, helps to provide a degree of confidence that is necessary for the proper functioning of a market economy.

From a financial services sector perspective, corporate governance involves the manner in which the business and affairs of a firm are governed by its board and senior management, including how they:

- set the firm's strategy and objectives
- determine the firm's risk tolerance/appetite
- operate the firm's day-to-day business
- protect the interests of depositors, meet shareholder obligations, and take into account the interests of other recognised stakeholders, and

- align corporate activities and behaviour with the expectation that the firm will operate in a safe and sound manner, with integrity and in compliance with applicable laws and regulations.

1.2 Senior Management Leadership



5.1.2 Understand the importance of senior management leadership, accountability and personal responsibility

It is the responsibility of the board of directors to set out the governance structure for the organisation, to make sure it is implemented as intended, and to provide effective supervision over senior management. Members of the board need to act with honesty and integrity and need to be independent. Members of the board of directors and senior managers of financial institutions performing key roles need to be approved by the regulator to execute their function.

Approval needs to be obtained from the regulator prior to the senior manager performing their role. Criteria may vary by regulator, but typically include prior experience, character, and education. The requirement for senior management approval applies to all institutions that operate within the jurisdiction, although they may differ based on the size of the operation. Senior managers and members of the board can be held directly and personally accountable if they did not take reasonable steps to prevent or stop a breach in regulatory requirements.

In the United Kingdom (UK), the **Senior Manager and Certification Regime (SMCR)** was introduced in 2015 with the aim of reducing damage to consumers and to strengthen market integrity. It replaced the approved persons regime (APR) for senior

management and encourages senior management to take responsibility for their actions. In addition, there is a strong focus on improved conduct and governance structures. As part of the SMCR, each senior manager must have a statement of responsibilities (SoR) setting out their roles and responsibilities. Senior management functions include the following:

- Chief Executive
- Executive Director
- Partner
- Chair of Audit Committee
- Compliance oversight
- Money Laundering Reporting Officer (MLRO).

Under the SMCR, senior managers have to take personal responsibility for their actions and are held accountable. Clear personal responsibility and accountability aims to reduce harm to customers and strengthen market integrity. Although senior management is ultimately personally responsible, this does not mean they should not delegate. The delegation of tasks is perfectly permissible, but reasonable steps must be taken to ensure the delegated tasks are discharged appropriately.

1.3 Monitoring Corporate Governance



5.1.3 Understand the role of the compliance function in implementing and monitoring corporate governance standards

A firm's corporate governance standards need to reflect the regulations and practices of the various jurisdictions in which the firm operates. The compliance function should, therefore, provide a key contribution to the formulation of these standards; in particular to ensure that all relevant regulatory aspects are included.

Regulators will have local expectations of corporate governance – whether due to international standards, local or regional legislation/regulation, or their own domestic concerns. Therefore, the compliance function should ensure that the firm’s approach will be satisfactory.

A corporate governance manual is typically used to explain the corporate and management structure of a business, and is designed to help executives and others understand the governance framework and approach pertaining to their business. Strong governance is a vital ingredient in a successful, growing and dynamic business. The more successful a business becomes, and the faster it grows, the more important a corporate governance manual is in decision-making, risk-taking and helping executives remain in control of their business. A corporate governance manual also explains the corporate and management structure of a business.

As part of its work as the firm’s second line of defence, the compliance function should also include a review of these governance standards as part of its monitoring activity. This monitoring should include the regulatory standards relating to corporate governance, and also the activity of those board members and senior management in positions of significant influence. Any deviations should be reported to an appropriate level of management and, in the case of material deviations, to the board.



1.4 Unitary and Dual (Two-Tier) Boards



5.1.4 Know the main corporate governance structures:
unitary board; two-tier structure

There are two types of board structures. These are the unitary board, and the dual board or two-tiered structure.

The unitary board of directors is characterised by one single board comprising both executive and non-executive directors (NEDs). The dual board is a two-tiered structure consisting of a supervisory board and an executive board of management where there is a clear separation between the functions of supervision and management.

In a two-tier structure, a management board manages the company's business operation, but is accountable to, and supervised by, a supervisory board elected by shareholders.

Despite this structural difference between unitary and dual-board systems, the similarities in actual board practices are significant:

- Both types of systems comprise a supervisory function and a managerial function.
- The board of directors in a unitary board and the supervisory board in the two-tier system are usually elected by shareholders (though in some European countries, employees will also elect one or more supervisory board members).
- Both the unitary board and the supervisory board in the two-tier structure appoint the members of the managerial body.
- In addition, both the unitary board and the supervisory board usually have responsibility for ensuring that financial reporting and control systems are effectively functioning, and to ensure the company complies with laws and regulations.

1.5 Effective Management



- 5.1.5 Understand the impact of business and/or management structures on the effective management of the compliance function: matrix structures; silo structures; maintaining independence

1.5.1 Matrix Structures

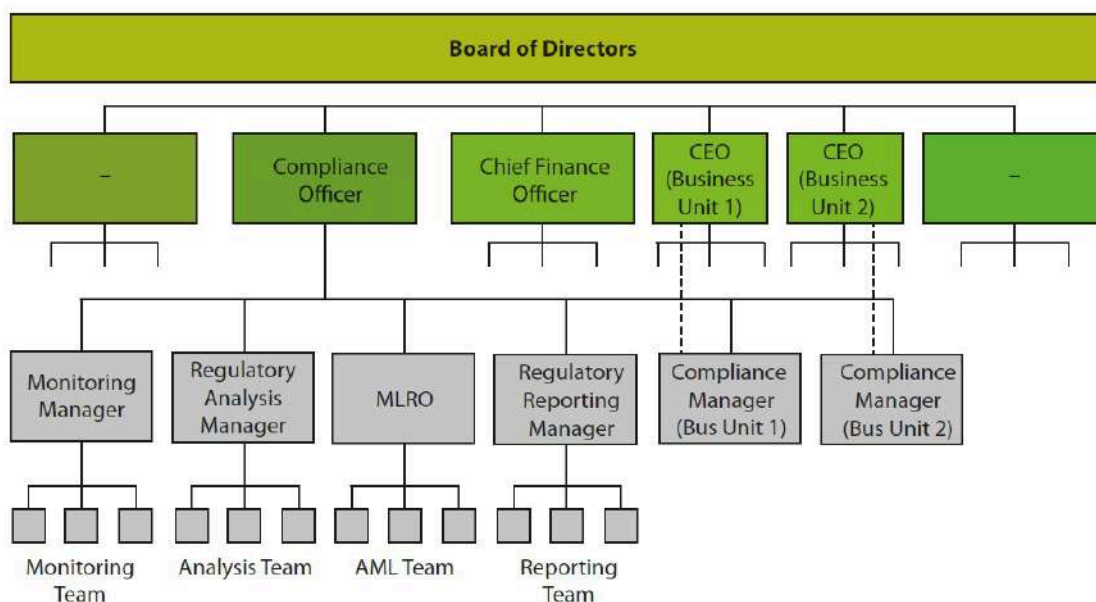
Traditional business hierarchy models saw individuals receiving authority from the person above them. Responsibilities would cascade down from a single point - for example, the board-level compliance director would establish a compliance structure which apportioned responsibility to their senior managers, who in turn would retain teams to ensure the work is performed.

While successful in terms of accountability, the increasing size and complexity of financial institutions highlighted limitations of such a model. Organisations need a balance between detailed knowledge of the products and services being provided by each business unit alongside the need for other disciplines to be centrally delivered by core teams of skilled personnel.

This need to balance efficient common services across an organisation (mirroring the traditional hierarchy) with dedicated activity within each business unit has led to a growth of 'matrix structures' within firms. The principle is that an individual may serve two or three managers rather than just one, having accountability to their functional manager for the delivery of services to a particular business unit, and having responsibility to another manager such as, for example, the chief executive officer (CEO) of that business unit for their contribution. Models can become more complex, with the individual having a functional responsibility across the wider business while also having specific responsibility to a particular business unit.

In a compliance setting, a member of the team may, therefore, have a responsibility to the compliance director in respect of their contribution to the compliance team's objectives (for example, performing regulatory analysis of consultation papers to determine what changes the firm might need to implement) while also having a matrix reporting line to the CEO of a particular business unit where that person has applicable detailed compliance experience.

The following diagram illustrates such a matrix structure, with dotted lines representing the matrix reporting lines to respective CEOs:



Such an approach should lead to a more flexible servicing model, as members of the team build and apply experience in multiple contexts to benefit the business overall. However, firms also must be careful to ensure that the implementation of matrix structures does not dilute staff accountability and clarity in the roles that each person fulfils. There can also be tensions if the managers in the matrix structure continue to expect that they can determine 100% of the employee's activity – forgetting that the employee has a matrix responsibility to another manager covering a portion of their time.

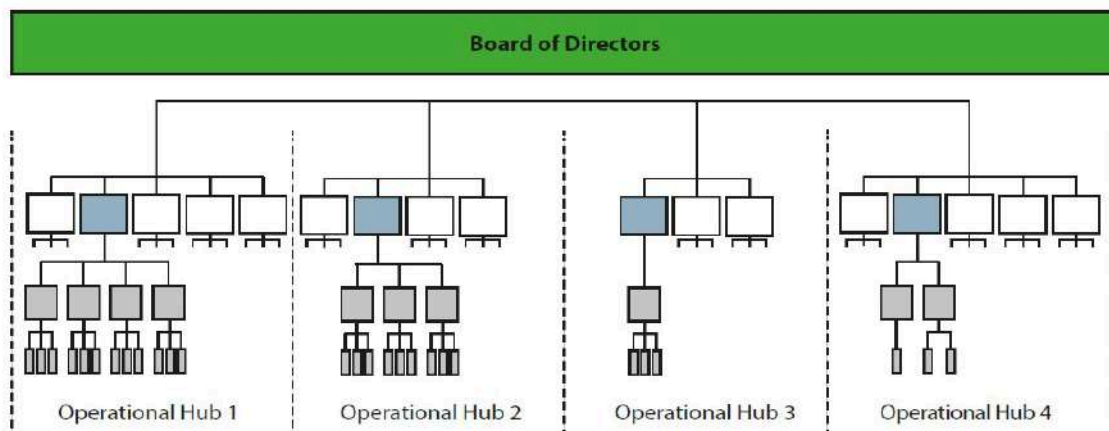
1.5.2 Silo Structures

Larger organisations may operate in a silo structure, where isolated groups of workers report to a line or functional manager. Imagine columns on a page with a line manager above each column and a group of workers inside each column under the manager of the division. As these groups operate independently, it is not unique to discover functions replicated in each silo.

In an information technology organisation, for instance, you might discover software programmers in the sales office, some more in the accounting department, and still more in corporate headquarters,

because each of these functioning units has a programming demand.

Such a structure is illustrated here, with the shaded boxes reflecting activity within the responsibility of a single director. Multiple functions are repeated in each office, as determined by the local requirements, with some functions being undertaken in multiple locations.



This has implications for all parts of the business, as such a structure is likely to become inefficient due to effort being duplicated in multiple areas. For compliance, there is an additional concern that replication of functions (eg, monitoring, advisory or regulatory analysis) in different locations can lead to inconsistency of the control infrastructure, and could ultimately undermine the clarity and consistency of liaison with regulators. The accountability of each person might be increased as they are responsible for delivering their specific function, though the overall structure must be robust to deliver group cohesion and cost control.

1.5.3 Maintaining Independence

Regardless of the structure chosen, the compliance function should clearly be independent within the firm. This involves four related elements:

1. The compliance function should have a formal status within the firm.

2. There should be a group compliance officer or head of compliance with overall responsibility for coordinating the management of the firm's compliance risk.
 3. Compliance function staff, and in particular the head of compliance, should not be placed in a position where there is a possible conflict of interest between their compliance responsibilities and any other responsibilities they may have.
 4. Compliance function staff should have access to the information and personnel necessary to carry out their responsibilities
-

1.6 Audit Contribution to Governance



5.1.6 Understand how auditing contributes to prudential corporate governance, accounting and reporting requirements: audit committees; internal audit; external auditors

The board should recognise and acknowledge that independent, competent and qualified internal and external auditors, as well as other internal control functions (including the compliance functions), are vital to the corporate governance process in order to achieve a number of important objectives. Senior management should also recognise the importance of the effectiveness of these functions to the long-term soundness of the firm.

The board and senior management can enhance the ability of the internal audit function to identify problems with a firm's risk management and internal control systems by:

- encouraging internal auditors to adhere to national and international professional standards, such as those established by the Chartered Institute of Internal Auditors (IIA) ♦

- promoting the independence of the internal auditor; for example, by ensuring that the internal audit function reports to, or has direct access to, the board or the board's audit committee
- recognising the importance of the audit and internal control processes and communicating their importance throughout the firm
- utilising the findings of internal audits in a timely and effective manner, and requiring timely correction of identified problems by senior management, and
- engaging internal auditors to judge the effectiveness of the risk management and compliance function, including the quality of risk reporting to the board and senior management, as well as the effectiveness of other key control functions.

The board and senior management:

- are responsible for the preparation and fair presentation of financial statements in accordance with applicable accounting standards in each jurisdiction, as well as the establishment of effective internal controls related to financial reporting, and
- can also contribute to the effectiveness of external auditors in order to ensure that the firm's financial statements fairly represent the financial position and performance of the company in all material respects by, for example, including in engagement letters the expectation that the external auditor will be in compliance with applicable domestic and international codes and standards of professional practice.

Non-executive board members should have the right to meet regularly – in the absence of senior management – with the external auditor and the heads of the internal audit and compliance functions. This can strengthen the ability of the board to oversee senior management's implementation of the board's policies and to

ensure that the firm's business strategies and risk exposures are consistent with risk parameters established by the board.

Senior management should promote strong internal controls and should avoid activities and practices that undermine their effectiveness. For example, senior management should ensure there is effective segregation of duties where conflicts could arise. They should also exercise effective control over employees in key business positions. This latter point has proven especially problematic where managers have failed to question employees who generate revenues or returns out of line with reasonable expectations (eg, where supposedly low-risk, low-margin trading activity generated unexpectedly high returns) for fear of losing either revenue or the employee. For example, in 2016, it emerged that Wells Fargo employees opened accounts in the name of customers without their consent in an attempt to meet unrealistic sales targets.

1.7 What does Due Diligence Mean?



5.1.7 Know the purpose and key elements of due diligence: identification; selection; fitness and propriety

Generally, due diligence refers to the care a reasonable person should take before entering into an agreement or a transaction with another party. Due diligence serves to confirm all material facts with regard to a transaction and is a key activity in good governance, serving to identify and limit risks. This is a way of preventing unnecessary harm to either party involved in a transaction.

Offers to purchase an asset are usually dependent on the results of due diligence analysis. This includes reviewing all financial records plus anything else deemed material to the sale. Sellers could also

perform a due diligence analysis on the buyer. Factors that may be considered are the buyer's ability to purchase, as well as other items that would affect the purchased entity or the seller after the sale has been completed.

For example, a due diligence investigation with regard to hedge funds refers to an in-depth review of a hedge fund's activity, conducted in order to ensure that the fund is in compliance with its prospectus. It is a roadmap for existing and potential investors in understanding whether a specific fund will meet their investment horizon, risk tolerance and investment strategy.

Such due diligence of a hedge fund would, therefore, include an examination of factors such as:

- a fund snapshot
- disclosed investment strategy
- historical returns
- assets under management (a copy of the fund's portfolio from the custodian is usually requested)
- audited financial statements if the fund is regulated
- fund's terms and details
- regulatory registration (if any)
- risk factors, or
- valuation.

Part of the due diligence process will be to review the senior management involved to ensure their fitness and propriety in order to verify they are financially sound and have appropriate skills, knowledge and experience. Due diligence will also be required in respect of other contractual relationships entered into by a firm, including the providers of material outsourced functions and the appointment of custodians. The results of due diligence will help to determine the selection of an investment or indeed confirm whether a takeover might proceed.

1.8 Corporate Governance Training



5.1.8 Understand how an effective training programme can contribute to good corporate governance

The commercial argument supporting corporate governance is simple – well-run companies produce better results. Much emphasis has been placed on the best practice of managing formal external relationships; establishing transparency; and emphasising legal, timely and trustworthy information.

From a regulatory perspective, it is important that the board and senior management fully understand their governance responsibilities and have the opportunity to test their knowledge periodically. The use of scenarios to discuss key governance and regulatory challenges can be an effective method of training.

An effective training programme for corporate governance would cover key governance issues such as managing conflicts, risks, and stakeholder management. In addition, it covers organisational issues such as the composition of the board, roles and responsibilities of board and senior management, corporate social responsibility, and internal control and risk management.

Provided the training is tailored to the organisation, and uses appropriate examples, it will assist instilling good corporate governance because it provides clarity on the organisational structure, and the principles and the culture of the organisation. This will in turn strengthen the risk and compliance culture and organisational effectiveness, advising and guiding the board.

1.9 Enhancing Corporate Governance – Background to the Bank for International Settlements (BIS) Principles



5.1.9 Understand the factors behind the formulation of the BIS Principles for enhancing corporate governance

5.1.10 Know the BIS Principles for enhancing corporate governance

Given the important financial intermediary role of banks in an economy, the public and the market have a high degree of sensitivity to any difficulties potentially arising from any corporate governance shortcomings in banks. Corporate governance is, thus, of great relevance both to individual banking organisations and to the international financial system as a whole, and merits targeted supervisory guidance.

The Basel Committee on Banking Supervision (BCBS) has had a longstanding commitment to promoting sound corporate governance practices for banking organisations. The BCBS's guidance assists banking supervisors and provides a reference point for promoting the adoption of sound corporate governance practices by banking organisations in their countries. The principles also serve as a reference point for banks' own corporate governance efforts.

The BCBS's 2006 guidance drew from the Principles of Corporate Governance that were published in 2004 and updated in 2023 by the OECD (see also chapter 1, section 1.1), and have since been revised following the BCBS's 2006 Principles that targeted key issues of corporate governance. Primary points in the 2006 guidance included:

- the board should be appropriately involved in approving the bank's strategy
- clear lines of responsibility should be set and enforced throughout the organisation

- compensation policies should be consistent with the bank's long-term objectives, and
- the risks generated by operations that lack transparency should be adequately managed.

Subsequent to the publication of the BCBS's 2006 guidance, there have been a number of corporate governance failures and lapses, many of which came to light during the global financial crisis which have resulted in a revision of the principles.

The BCBS's guidance is intended to assist banking organisations in enhancing their corporate governance frameworks and to assist supervisors in assessing the quality of those frameworks. They are meant to be applied within the framework of national laws, regulations and codes. In the event a country has adopted legal frameworks and standards (eg, for publicly traded firms) as well as accounting and auditing standards, supervisors are encouraged to periodically check their frameworks and standards for consistency with relevant BCBS guidance.

The BCBS prefers a governance structure composed of a board and senior management for reasons of independence, but also recognises that there are significant differences in the legislative and regulatory frameworks across countries regarding these functions. Therefore, in the guidance the terms board and senior management are used not to identify legal constructs, but as a way to refer to the oversight function and the management function. The guidance encourages practices that can strengthen checks and balances and sound corporate governance under diverse structures. The 13 principles are outlined in the following table:

The BIS Principles for Enhancing Corporate Governance

Principle 1	The board has overall responsibility for the bank, including approving and overseeing the implementation of the bank's strategic
--------------------	--

	objectives, governance framework and corporate culture.
Principle 2	Board members should be and remain qualified, individually and collectively, for their positions. They should understand their oversight and corporate governance role and be able to exercise sound and objective judgement about the affairs of the bank.
Principle 3	The board should define appropriate governance practices for its own work and put in place the means for such practices to be followed and periodically reviewed for ongoing effectiveness.
Principle 4	Under the direction of the board, senior management should carry out and manage the bank's activities in a manner consistent with the business strategy, risk appetite, remuneration, and other policies approved by the board.
Principle 5	In a group structure, the board of the parent company has the overall responsibility for the group and for ensuring the establishment and operation of a clear governance framework appropriate to the structure, business and risks of the group and its entities. The board and senior management should know and understand the bank group's organisational structure and the risks that it poses.

Principle 6	Banks should have an effective independent risk management function, under the direction of a chief risk officer (CRO) with sufficient authority, stature, independence, resources and access to the board.
Principle 7	Risks should be identified, monitored, and controlled on an ongoing bank-wide and individual entity basis. The sophistication of the bank's risk management and internal control infrastructure should keep pace with changes to the bank's risk profile, to the external risk landscape, and in industry practice.
Principle 8	An effective risk governance framework requires robust communication within the bank about risk, both across the organisation and through reporting to the board and senior management.
Principle 9	The bank's board of directors is responsible for overseeing the management of the bank's compliance risk. The board should establish a compliance function and approve the bank's policies and processes for identifying, assessing, monitoring, reporting, and advising on compliance risk.
Principle 10	The internal audit function should provide independent assurance to the board and should support board and senior management in promoting an effective governance process and the long-term soundness of the bank.

Principle 11	The bank's remuneration structure should support sound corporate governance and risk management.
Principle 12	The governance of the bank should be adequately transparent to its shareholders, depositors, other relevant stakeholders and market participants.
Principle 13	Supervisors should provide guidance for and supervise corporate governance at banks, including through comprehensive evaluations and regular interaction with boards and senior management, should require improvement and remedial action as necessary, and should share information of corporate governance with other supervisors.



2. Key Risk Types, their Application and Impact on the Compliance Function

2.1 Risk and Uncertainty



5.2.1 Understand the difference between risk and uncertainty

Many things in life are not certain, and we manage these issues in our everyday lives. Consider the question of whether you will arrive at work on time tomorrow morning and the number of events that could prevent success: whether the car will start, whether the roads will be clear, whether the trains will be operating – and that is before we consider less likely factors (for example, hurricanes, unseasonal snowfall, or earthquake damage).

As you probably felt when reading those last few items, one of the ways we handle uncertainty in our personal lives is through assessing whether certain events or outcomes are likely. The same is true when we consider professional matters.

Uncertainty is a general concept that simply recognises the potential of different outcomes arising. Uncertain matters tend to be vague rather than measurable; science or statistics are unable to help us make decisions. However, where we are able to use data or probability theory to assess and analyse potential outcomes, we are able to talk in terms of 'risk'.

One of the challenges facing a risk professional is, therefore, to identify areas of general uncertainty within a company, and then to deploy tools and analysis in order to quantify those issues as recognised risks – which can then be managed. A key aspect is, therefore, determining the likelihood of outcomes arising. In other words, assigning probabilities to matters of uncertainty in order to assess risk, and thus provide better information to senior management for decision-making.

However, to accurately quantify an event's probability of occurring, we need large amounts of observable, repeating data that can be grouped and analysed. This sort of data is available for credit and **market risk** analysis, but business risk has much less 'repeatable' data. Many business risk events (including operational risk) are rare events – and, in some cases, have not yet occurred.

Nevertheless, this technical difference between risk and uncertainty should not stop firms from protecting themselves against the negative consequences of less quantifiable events.

2.2 External Sources of Risk



5.2.2 Know the key external sources of business risk and their potential impact

External risks arise from changes in:

- the global economy

- the political arena
- the competitive environment
- social and market forces, and
- technological innovation.

Further business risks are also posed by unexpected shocks and natural events, and the actions of external stakeholders and third parties.

2.2.1 Economic Risk

In its simplest terms, the economy consists of the interaction between individuals and firms, and the allocation of their limited resources to maximise their financial positions. In other words, the economy is shaped by human behaviour, whether as individual consumers or as collectively arranged organisations. Individuals have limited money to spend and have to make choices on how to spend it. These choices are influenced by a combination of wants and needs. Wants are related to items such as fashion items and holidays whereas needs are related to items such as basic food and shelter. People's decisions are influenced by advertising, reviews, and the buying behaviour of others.

Therefore, a firm has to understand the current and potential future patterns of human behaviour that will affect the products or services it sells. For example, during an economic boom, a failure to anticipate an imminent downturn will result in firms continuing to increase their stocks using current input prices of raw materials. They will then find they need to reduce the prices of their finished goods to sell them in a recession. Equally, financial services firms with securitised mortgages on their books will find it difficult to sell them if there is a fall in house prices.

2.2.2 Political Risk

Wealth creation and its distribution tend to be viewed in different ways by different political parties. Therefore, a change in government will generally affect the financial sector and may be the cause of a rise, or fall, in the markets. This will depend upon the economic strategies that commentators expect the new leadership to implement.

Other political events, such as changes in economic policy, or tax law, will also affect the financial sector. Political changes, being so closely linked to the economy, can affect financial services firms in three main ways:

- A rise or fall in the markets in which firms invest.
- An increase or decrease in demand for the products which the industry sells.
- Changes to the legislative and regulatory environment in which financial services firms operate.

2.2.3 Risks from the Competitive Environment, Social and Market Forces

Firms are affected by the performance of other companies, especially those operating in related industries and markets. For example, if a competitor gains a critical mass of market share, it may become too expensive for some of the other firms to continue servicing the remaining customers. This will force one or more of them to exit that part of the market. On the other hand, if a close competitor fails, there may be scope to buy parts of their business at below their market price.

Firms in the finance sector are also particularly susceptible to certain changes in social and market forces, such as:

- the propensity to save
- attitudes to living on credit, and
- house prices and their relationship to demographic changes.

For example, when credit card debt and buying in instalments become normalised and debt rises, the chances that people will default increases. As a result of the global financial crisis central banks globally reduced interest rates which resulted in increased borrowing. As interest rates are rising, more people find themselves unable to meet the payments.

2.2.4 Technological Risk

The development of new technology is behind many of the increases in productivity that create economic growth.

For example, automation changed the way in which businesses organise their operations. 'Interconnectedness' is also affecting how information and data are transmitted, how businesses and people communicate, and how, when and where people work. The availability of fast and efficient telecommunications has enabled new ways of reaching customers and organising internal resources. In the past, workers may have had to relocate to where employers delivered their services. Now, a bank can 'outsource' individual functions to lower-cost overseas locations.

During the Coronavirus (COVID-19) pandemic, e-commerce soared due to the fact that many shops were closed. Just before the start of the pandemic, in the UK card payments overtook cash payments for the first time partly due to increased card payments in shops and partly due to increased online purchases. On the other hand, with the increase in automation, and e-commerce the risk of cybercrime has also increased.

In addition, internet services mean that expensive branch networks are no longer a prerequisite for success in the financial sector. In the UK, for example, banks have 34% of their branches since 2019. Information management has also improved – both in terms of firms making use of consumer data, and consumers gaining access to more information about products and services. Firms that do not

anticipate or keep up with technological change, or which specialise in older technology investments, risk falling behind.

2.2.5 Shocks and Natural Events

We live in an age of instant media coverage and shocks or natural events in one part of a country have the potential to adversely affect the national, or even the global economy. For example, after the 2004 Indian Ocean earthquake and tsunami, the Thai Prime Minister assessed the cost of damage at \$510 million. It was estimated that the disaster would reduce Thailand's 2005 GDP by 0.5%.

There was very little that firms in the affected areas could have done in advance to prepare for the tragedy, but firms which had planned in advance for generic disasters were able to recover operations more quickly than those who had not.

The same is also true to some extent of the events of the 9/11 attacks in the US – with the exception that operational recovery did not necessarily enable continued business because:

- the debris from the collapsing towers and the general chaos in the area meant the closure of the New York Stock Exchange (NYSE), as well as brokerage houses and banks in the Wall Street area, and
- the grounding of all aeroplanes prevented the clearing of cheques and the distribution of paper currency, creating uncertainty for financial institutions.

Despite this event having occurred in the US, the interrelationship between the financial markets and economies of the UK and the US caused the UK FTSE 100 to fall by 12%.

Coronavirus (COVID-19) Pandemic

The COVID-19 pandemic has resulted in the global shutdown of economies and businesses. Some, like supermarkets, have fared well and increased their business. Others, such as the hospitality industry

and non-essential businesses have lost out as a result of having to close their business for extended periods. The impact on the global economy is estimated to be three times more harmful than the 2008 crisis.

Although financial institutions reduced credit restrictions to assist companies throughout the pandemic, businesses continued to be assessed on their credit worthiness. Default risk – the risk a borrower is unable to meet their debt obligations – has been negatively impacted during the pandemic, and this is expected to continue for some time.

From a compliance perspective, the pandemic has resulted in additional risks such as an increased vulnerability to cybercrime, and the challenges associated with the sudden move to remote working. Although technologically most firms seem to have coped well with these changes, working from home has created a larger potential of data protection breaches, and the associated loss of interconnectivity between staff may result in patterns of behaviour related to market abuse and fraud being overlooked. Policy, processes, and procedures have been amended to cater for the new working environment. After the pandemic, employees have returned to work, but office workers continue to work at least some of their time from home.

2.2.6 Risks from Stakeholders and Third Parties

External stakeholders that create business risk typically include a firm's parent company, any major institutional investors, and any particularly large or important customers.

1. The parent company

- Where the parent owns more than one business it will take a 'global view' and this, at times, may cause it to question or alter the plans of its subsidiary firms.

- Unless parent firm expectations are carefully managed during the formulation of the plans, this can cause great inconvenience to the subsidiary firm. Quite often, by the time the plans are ready to be shared with the parent, staff may have been hired and external research may have been commissioned. Key customers may even have been consulted as part of the planning process.
- In some cases, particularly where the firm is a 'start-up' or embarking on a diversification of service, the 'parent' role may be held by a venture capital firm. This can bring a different set of expectations, such as a goal of achieving a certain level of financial return over a defined time period, or achieving a market listing.

2. **Major institutional investors**

Where institutional shareholders own large shareholdings in the firm, this gives them influence through voting rights. If these stakeholders have different views on, for example, the competence of certain board members. In some cases, there may be little that the firm can do to prevent them pushing for change.

3. **Large customers**

If a firm has an over-reliance on a particular customer, that relationship needs to be carefully managed. This is particularly important as there are often other firms in the industry that could provide the same services to this customer. Over the longer term, the firm should aim to dilute this risk by increasing its customer base.

The key to managing stakeholder risk is to:

- build relationships at senior levels

- understand their agenda and how it may differ from the firm's own agenda, and
- manage expectations with any new developments.

Other third parties that can also be a source of business risk might include:

- brokers
- solicitors
- IT and data suppliers
- outsourced back-office administrators, and
- advisers/industry consultants.

It will be important for the firm to ensure that, where possible, it can source equivalent goods and services from alternative suppliers. That way, if a third party defaults or delays delivery, there should be no service interruption to the firm's customers.

2.3 Internal Sources of Risk



5.2.3 Know the key internal sources of business risk and their potential impact

Internal risks arise from changes in:



Strategy



Operations



Financial



Legal and
regulatory

2.3.1 Strategic Risk

The Committee of European Banking Supervisors (CEBS) defines **strategic risk** as:

‘the current or prospective risk to earnings and capital arising from changes in the business environment and from adverse business decisions, improper implementation of decisions or lack of responsiveness to changes in the business environment.’

In simple terms, strategic risk revolves around two main questions:

1. Is the strategy right?
 - Producing the wrong strategy can be one of the most serious mistakes a board can make.
2. Is the strategy being properly implemented?
 - Failing to implement even the best of strategies may also lead a firm to extinction.
 - Does the board know whether, and how well, its strategy is being implemented?
 - If the strategy is not implemented, is this because the firm is being run by inexperienced or lax management? Or is the strategy so complex that it is impossible to implement?

2.3.2 Operational Risk

The BIS defines operational risk as ‘the risk of loss arising from processes, people, systems or external events’. The BIS states that operational risk is inherent in all banking products, activities, processes and systems, and that the effective management of

operational risk has always been a fundamental element of a bank's risk management programme. Therefore, having a sound operational risk management programme in place is a reflection of the effectiveness of the board and senior management in administering its portfolio of products, activities, processes and systems.

2.3.3 Financial Risk

At the simplest level, for a company to stay in business, its revenues must match or exceed its costs. Any agreement by the firm to offer credit terms to its customers creates a financial risk that the customer may not pay. Similarly, financial risk arises any time a firm deploys its corporate resources ahead of receiving payment for services – such as any investment to build up stock.

Financial risk is not limited to the internal informed decisions of a firm; it can also arise where a participant in the market is acting improperly. If the finances of a firm are 'glossed' to cover up losses, which in itself is a breach of the Corporate Governance Code, the pretence can be kept up only for a limited time before the firm runs into liquidity problems. Unless the underlying finances of a firm are sound, the firm will be 'found out' when markets or other environmental factors change. However, when the firm becomes insolvent there will be insufficient resources left to pay all its creditors.

Another source of financial risk stems from the use of gearing. Also known as leverage, gearing is the ratio of a firm's debts to the value of its equity. A company which looks sound on paper, but which has become over-g geared can suffer disproportionately if interest rate rises cause its debt to become more expensive, or if its revenues fall to a level too low to repay its debt. For these reasons, it is important that any firm offering credit terms to its customers should seek to obtain evidence of financial soundness in order to manage the associated financial risks.

2.3.4 Legal, Regulatory and Reputational Risk for Financial Services Firms

Financial services firms' failure to comply with legislation and regulations may result in serious consequences including financial penalties and loss of reputation (see section 3).

2.4 Effective Risk Management



5.2.4 Know the components and practical application of an effective risk management process

Risk management should identify what could go wrong, evaluate which risks should be dealt with, and implement strategies to address those risks. Firms that take pre-emptive action to identify their risks and formulate a response plan will be better prepared and have a more cost-effective way of dealing with them if those risk events do occur.

The key elements of a simple risk framework are:

- risk policies and governance at board level
- risk oversight – often performed by a dedicated risk management function, often organised by risk type and performing the following tasks:
 - identifying risks
 - assessing risks
 - ensuring that risks are appropriately controlled
 - monitoring and reporting on the risks and their associated controls, and
 - day-to-day risk management – this activity is inseparable from good business management and

must be owned by the business units, not the risk function.

Effective risk management means it is appropriate for the size and complexity of the organisation, and incorporates the three-line of defence model (chapter 2, section 2.1.3).

2.5 Assessment of Risks



5.2.5 Understand how the impact of risks on a firm's business activities are assessed and managed including operational resilience

2.5.1 Assessing External Risks

A number of different techniques are used to arrive at an understanding of a firm's business risk profile. Examples include:

- **PESTLE analysis** – this is an analysis of the external macro environment in which a business operates. This environment will inevitably contain factors which are beyond the firm's control or influence, but which are, nevertheless, important to be aware of when developing new products, businesses or strategies. Risks are considered under the following headings:
 - political
 - economic
 - social
 - technical
 - legal, and
 - environmental.
- **Business continuity/disaster recovery planning** – a company must take reasonable steps to ensure that its services are

robust given the various risks that affect its operations. For example, IT systems and infrastructure should be designed to include resilience against isolated failures of individual components, yet problems can arise that prevent the firm's primary processes from being completed. Disaster recovery planning covers the most significant threats facing the ongoing activities of the business – such as the inability to use a building or data centre as a result of fire, flood, or loss of utilities. Disaster recovery events generally require firms to relocate their staff to alternative premises for a period, until the primary facilities can again be used. It is a rare event for a firm to implement a full disaster recovery. The parallel discipline of business continuity planning requires the firm to establish protocols that would be invoked where physical premises remain serviceable yet some other event makes it impossible for certain services to be delivered in the usual manner. For example, the loss of telecommunications links may prevent some tasks from being performed in the normal manner, though as other processes remain operational it may not be a sound decision to implement full disaster recovery and relocate staff to alternative premises. The tension between restoring the lost service and completing other tasks needs to be understood. Thorough planning and testing through desktop exercises, will enable the firm to understand the time frames within which a business continuity event must be resolved before the firm will instead declare an emergency and invoke full disaster recovery, for example, moving all functions onto a back-up IT infrastructure.

- **Business process analysis** – this involves:
 - examining each high-level business process, and
 - describing both the internal processes and external factors which can influence those processes.

Having identified the external business risks on which to focus, each one should then be assessed so that the risks can be considered and

prioritised in order of 'potential damage'. This is preferable to simply tackling the ones that look most straightforward or interesting.

One of the simplest methods of assessing risks is the creation of a ranking hierarchy, which is a method of ranking risks in order of their significance to the firm. It is necessary to turn general uncertainty into manageable risk – which requires analysis. Such assessments may be subjective (based on the experience of the professionals involved) or objective (being supported by historical data) or both. In either event, the ranking decision depends on two criteria: the likelihood of the risk being realised, and the magnitude of the impact.

The likelihood of the risk can be represented as a range of probabilities that correspond to a rating. For example, depending on the business area being measured, the following ratings might be used:

Likelihood Probability Ratings

Very low	less than 1%	rating score = 1
Low	1% or more, but less than 5%	rating score = 2
Medium	5% or more, but less than 10%	rating score = 3
High	10% or more, but less than 20%	rating score = 4
Very high	20% or more	rating score = 5

Impact Loss Ratings

The impact of the risk is the potential loss if the risk occurs. This can be represented as a monetary range, and also assigned a rating in

line with the size and financial reserves of the firm. For example:

Very low	less than £5 million	rating score = 1
Low	£5 million or more, but less than £20 million	rating score = 2
Medium	£20 million or more, but less than £50 million	rating score = 3
High	£50 million or more, but less than £100 million	rating score = 4
Very high	£100 million or more	rating score = 5

A simple overall risk assessment is arrived at by multiplying the likelihood rating scores with the impact rating scores:

Risk score = likelihood score × impact score

However, in devising any mathematical model, it is necessary to consider the behaviour of numbers. The simple formula above would give a value of '5' where a 'very low' likelihood is combined with a 'very high' impact – yet a score of '6' when a 'low' likelihood is combined with a 'medium' impact. Compliance and risk professionals designing a risk assessment should, therefore, give careful consideration to the correct weighting of results which may lead them to use non-linear scales or other weighting factors to yield tailored outcomes suitable for the context of their business.

2.5.2 Assessing Internal Risks

Internal drivers of business risk are typically identified through a combination of techniques, such as the following:

- Structured brainstorming – an example of this is SWOT analysis that focuses participants' attention systematically on the firm's:
 - strengths
 - weaknesses
 - opportunities, and
 - threats.
- Industry best practice benchmarking performed by external consultants.
- Scenario analysis, including **stress testing** and reverse stress testing.
- Risk assessment workshops – going through the firm's corporate goals to bring out the factors that could prevent each goal from being met.
- Discussion with external auditors – external auditors are often well placed to give advice on potential areas of business risk (even if such risks fall outside the scope of the usual audit activity).

Having identified the key internal drivers of business risk, each one then needs to be assessed. As in the external business risk discussion above, the risks are usually scored by impact and likelihood, so they can be ranked and prioritised for mitigation effort.

2.5.3 Risk Appetite

Risk appetite, or risk tolerance, is the level(s) of loss that the firm is willing to accept in its different businesses over a specified time horizon at a given level of confidence, ie, the level of expected loss that the firm will not (or cannot) mitigate.

In the risk versus uncertainty discussion in the previous section, we considered the differences in the amount of data available for

assessing the likelihood of credit and market risk losses compared to that which is available for assessing the likelihood of business and operational risk losses. Risk appetite will need to be expressed in different ways for different risk types, to reflect the relative ease of assigning probabilities to the losses caused by each type.

For example, for more easily quantifiable risks the risk policy might include:

- a tolerance for direct financial loss, or
- specific risk measures, such as credit or market **value at risk (VaR)** metrics.

For less easily quantifiable risks, the policy might specify non-financial statements, such as:

- Our disaster recovery plans ensure that, following the loss of our main premises, the firm will reopen for business within eight hours.
- The firm has no appetite for reputational risk. All external communications must be approved by the head of marketing.

At the group level, the firm will need to tie its overall risk profile, which in effect is its current default risk tolerance, to its level of available risk capital.

Setting a risk appetite tends to be an iterative process, and often needs both a top-down and a bottom-up approach.

A top-down approach involves the board and senior management:

- identifying threats to the firm's objectives
- relating them to the 'coverage' available from the firm's capital/earnings/assets, and
- recognising that holding capital is not always the best mitigant for every risk and using scenario analysis to enable appropriate responses to be devised for each threat.

A bottom-up approach requires line management to adopt:

- a set of departmental 'acceptable occurrence' levels for errors and losses, and
- an appropriate set of **key risk indicators (KRIs)** which can be tracked against predefined tolerances.

The escalation mechanism for tolerance breaches also needs to be defined so that the bottom-up approach can be linked to the top-down approach.

2.5.4 Risk Register

Having identified and then assessed the various internal and external business risks facing the firm, and ranked the risks to decide the priority order for mitigation, the next stage is to construct a risk register (also known as a risk log).

This is simply a list of the identified risks, linked to the business objectives whose success would be threatened if the risk materialised. Each is assigned a risk score which is used to sort the risks so that the list runs from the most significant to the least significant. Each risk is assigned to an owner or lead person and then the mitigating actions would be listed, along with their deadlines for completion.

Finally, the sources of assurance and oversight would be given in order to allow periodic re-assessment of the risk and the status of the mitigating controls which the actions will have implemented. Both 'assurance' and 'oversight' refer to the mechanisms used by the firm to provide an objective view on the quality of each risk's management.

Mitigating controls are ways in which the likelihood and impact of a risk are reduced. They could, for example, include managerial sign-off of work before it leaves the department, or perhaps an IT system that requires a second member of staff to verify inputs for accuracy.

In summary, the usual column headings for a risk register are:

- business objective
- description of associated risk
- risk ranking
- lead person or department
- action plan
- target and completion dates
- sources of assurance and oversight (which may or may not be the lead person or department), and
- mitigating controls.

2.5.5 Operational Resilience

Since the global financial crisis, regulators have strongly focused on the financial **operational resilience** of banks to ensure the stability of the financial system. Increasing complexity and interconnectivity have made financial institutions vulnerable to operational disruptions such as the temporary loss of IT systems. The COVID-19 pandemic appeared unexpectedly and has clearly shown the need for firms to be able to suddenly amend their working processes which, in turn, has resulted in a larger vulnerability to cybercrime. Although COVID-19 was an extreme event, firms need to be able to respond to the challenges caused by uncertain events. In 2021, for example, the FCA in the UK issued final rules and guidance in relation to requirements to strengthen the operational resilience of the financial services sector.

2.5.6 Risk Management



5.2.6 Understand the key aims of the risk management function, the risk committee and their relationship with the compliance department

The resources to coordinate and monitor risks of all types are generally provided by a centralised risk management function which is independent from the business areas it serves. The Walker review in the UK, undertaken in 2009, is a review of UK corporate governance which found that the Combined Code of Governance that is in place remained more important than formal rules and regulations in promoting better overall corporate governance. Within firms that adhere to the 2009 Walker Review on Corporate Governance, the risk management function is accountable to the board risk committee and is typically tasked with:

- Ensuring that the firm has a robust and consistent risk management and control framework.
- Providing support, oversight and challenge on the firm's risk appetite statements.
- Owning the top-level strategic risk assessment process.
- Monitoring the firm's risk profile against its risk appetites.
- Playing a leading role in defining and embedding the firm's risk culture.
- Providing risk training across the firm.
- Working with other oversight functions such as compliance and audit to provide a comprehensive, robust and efficient assurance framework.

In addition, for all risk types, the risk management function would typically:

- Oversee and challenge the risk and control self-assessment programme to capture expected risks.
- Oversee and challenge the firm's scenario analysis to capture unexpected extreme risks.
- Help to define, and subsequently challenge, the KRIs used for risk monitoring.
- Ensure issues are properly escalated, assisting with root cause analysis for incidents and losses, and tracking any associated

actions.

- Test risk models and key controls within the business, and recommend improvements.
- Advise on risk-based process mapping.
- Support the firm's risk IT system(s).
- Benchmark the firm's risk control framework against industry good practice.

2.5.7 Compliance

Compliance and risk management are not the same, although some of their duties overlap and certainly the compliance function is an important component of a firm's overall risk management.

It is crucial that regulatory rules are followed, and that exceptions are noted and corrected in a timely manner. To do otherwise would represent a significant risk to the firm. Therefore, while there is clearly some overlap between compliance and risk management, each function nevertheless has a different agenda.

Compliance focuses primarily on ensuring that all rules and regulations are followed. Risk management focuses on ensuring that risks are understood, and that proactive decisions are made about which risks to take and which to manage or avoid.

Compliance risk is a significant factor in the overall risk framework of financial services firms. It is not limited to simple compliance with laws and regulations; it also encompasses sound fiduciary principles, prudent ethical standards, client documents, internal policies and procedures, and other contractual obligations.

Some examples of issues that could raise an institution's level of compliance risk are:

- substandard account acceptance and review processes
- shortcomings in the ethical culture and expertise of management and staff, or

- weak internal compliance systems and training programmes.

The compliance function has the same dilemma as the risk function – the need to be an adviser of the business on the one hand and the need to monitor relevant activities on the other. Compliance teams need to find a careful balance between the fundamentally different mindsets and approaches required by the proactive ‘trusted adviser’ versus the more reactive ‘independent watchdog’. The independent watchdog will report deviations to an appropriate level of management or, if appropriate, to the board of directors.

Effective compliance risk management is a collaborative process that involves all the various control functions within the organisation, such as risk management, internal control, fraud detection, legal and human resources. For example, the risk management function could help to detect potential compliance risks by identifying visible lapses that might indicate a more pervasive pattern of non-compliant behaviour ‘below the water line’. The human resources function would be involved in its role as the expert in managing people, communicating expected behaviours, designing appropriate appraisal and reward structures and determining disciplinary measures.

2.5.8 How Compliance and Risk Management Protect and Add Value

When firms embark on new areas of business or launch new products, they very often justify the strategy with a cost/benefit analysis. Such analysis compares the estimated likely revenues with the projected costs. If the former outweighs the latter, then the project is given the green light. Firms recognise that the value of such analysis is dependent upon accurate projections of both the costs and benefits and will strive to improve the accuracy of these numbers.

However, aside from the risk of poor projections, establishing new areas of business exposes a firm to additional risks – with the potential risk that the business sponsor within the firm may overlook the significance or scale of some risks. Certain risks, such as client litigation, can vastly overshadow the operational costs of supporting the venture. The same is true for compliance risks; it can be costly to use up a great deal of resource on a new business project and then find the product design is not compliant or the launch has to be delayed because authorisations are required.

If risk and compliance management staff are involved in the development process from the start, they will be able to advise on the likelihood and impact of any risks, including compliance risks. Ideally, this would take place at an early enough stage that mitigation can be built into the solution. Over time, this approach will protect and add value to the firm.



3. Compliance Risks



- 5.2.7 Know the BIS definition of 'compliance risk'
- 5.2.8 Know who BIS deem responsible for the management of compliance risk
- 5.2.9 Know what measures BIS state should be undertaken to manage compliance risk: formalised document establishing the compliance function; board approval; annual review

Compliance risk is defined by the BIS as:

'the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a firm may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities (together, compliance laws, rules and standards).'

Compliance laws, rules and standards generally cover matters such as observing proper standards of market conduct, managing conflicts of interest, the fair treatment of customers, and ensuring the suitability of customer advice. They, typically, include specific areas such as the prevention of money laundering and terrorist financing and may extend to tax laws that are relevant to the structuring of banking products or customer advice. A firm that knowingly participates in transactions intended to be used by customers to avoid regulatory or financial reporting requirements, evade tax liabilities, or facilitate illegal conduct will be exposing itself to significant compliance risk.

Compliance laws, rules and standards have various sources. These include primary legislation, rules and standards issued by legislators and supervisors, market conventions, codes of practice promoted by industry associations, and internal codes of conduct applicable to the staff members of the firm. These are likely to go beyond what is legally binding and embrace broader standards of integrity and ethical conduct.

While the board of directors is responsible for overseeing the management of the firm's compliance risk, the BIS deems the firm's senior management as responsible for the effective management of that risk, for establishing and communicating a compliance policy, for ensuring that it is observed, and for reporting to the board of directors on the management of the firm's compliance risk. Further details on the BIS prescribed measures to manage compliance risk can be found in chapter 2, section 1.1.

3.1 Using Technology to Aid the Management of Compliance Risks



5.2.10 Understand how technology can be utilised to enhance compliance risk assessment

A framework of technology tools can be used to aid the compliance function in the assessment of risks. Here are some examples of the ways in which technology can help the compliance function:

1. Prevention – ensuring that compliance requirements are built into line-of-business applications, such as workflow and image systems. An example would be to include prompts relating to anti- money laundering (AML) checks when new business applications are being processed.
2. Detection systems and reports which identify exceptions and specific types of transactions. These could aid the oversight of high-risk trades or enable the identification of politically exposed persons or sanctions list matches.
3. Recording incidents, control failures, breaches and complaints to meet record-keeping requirements; and the production of management information (MI) to identify trends in error rates. This will help to identify at an early stage any systemic problems that may arise.
4. Online regulatory information systems, providing up-to-date information on regulatory changes and industry developments, including regulator and supervisory actions. This will include information on any systemic risks identified.
5. Effective online training and refresher courses on key aspects, including financial crime prevention, treating customers fairly and handling complaints. The results of online testing can demonstrate any gaps in knowledge which may give rise to a compliance risk.

3.2 The Impact of Technology on Regulatory Risk



5.2.11 Understand how technology changes impact regulatory risk: cybercrime; FinTech; RegTech; Cloud data housing

The advance of technology significantly alters the way in which financial services operate, and has provided opportunities for new entrants to the market. It does, however, also have an impact on regulatory risk, specifically in the areas of cybercrime, Fintech and Regtech. The use of the cloud to store data can add further risk.

3.2.1 Cyber Crime

Cyber crime is considered to be a crime in which a computer is the object of the crime (hacking, phishing, or spamming) or is used as a tool to commit an offence such as hate crimes. Criminals may use computer technology to access personal information, business trade secrets or use the internet for exploitive or malicious purposes. Criminals can also use computers for communication and the storage of illegitimate documents or data. Criminals who perform these illegal activities are often referred to as hackers.

Some common cyber threats for individuals are:

- **phishing** – attempting to obtain personal details by sending out urgent sounding emails designed to entice people to click a link to a malicious website
- **file hijacking or ransomware** – locking computers until a ransom is paid
- **key logging** – obtaining user-ids, passwords and other sensitive information by capturing keystrokes using illegally installed software, and
- **ad-clicker** – enticing people to click on an ad which redirects to a malicious website.

Common cyber threats for businesses are hacking, Distributed Denial of Service (DDoS) attacks, and invoice fraud.

The National Cyber Crime Unit (NCCU) is the part of the National Crime Agency (NCA) that helps fight cybercrime in the UK. See the website '[Cybercrime](#)' for more information about the NCCU.

3.2.2 FinTech

As covered in chapter 1, section 1.8, financial technology, or FinTech, refers to the use of technology to advance or change the financial sector. Common examples of FinTech include:

- cryptocurrency and digital cash
- blockchain technology
- smart contracts
- open banking
- financial inclusion, and
- cyber security.

Regulatory sandboxes allow firms to test innovative propositions in the market with real consumers in a controlled environment. They are typically run by a regulator to allow businesses to test innovative products, services, business models and delivery mechanisms in the real market, with real consumers.

Example – The UK Financial Conduct Authority (FCA)

The UK FCA's sandbox is open to authorised firms, unauthorised firms that require authorisation and technology businesses. The sandbox seeks to provide firms with:

- the ability to test products and services in a controlled environment
- reduced time-to-market at potentially lower cost
- support in identifying appropriate consumer protection safeguards to build into new products and services, and
- better access to finance.

The sandbox also offers tools such as restricted authorisation, individual guidance, informal steers, waivers and no enforcement action letters.

Tests are closely overseen using a customised regulatory environment for each test – including safeguards for consumers.

Sandbox tests are expected to have a clear objective (eg, reducing costs to consumers) and to be conducted on a small scale, so firms will test their innovation for a limited duration with a limited number of customers.

Example – Hong Kong Monetary Authority (HKMA)

The FinTech Supervisory Sandbox (FSS), launched by the HKMA in September 2016, allows banks and their partnering technology firms (tech firms) to conduct pilot trials of their Fintech initiatives involving a limited number of participating customers without the need to achieve full compliance with the HKMA's supervisory requirements. This arrangement enables banks and tech firms to gather data and user feedback so that they can make refinements to their new initiatives, thereby expediting the launch of new technology products, and reducing the development cost.

3.2.3 RegTech

As covered in chapter 1, section 1.8.4, regulatory technology, or RegTech, is the use of technology to facilitate the delivery of regulatory requirements. Although the link between regulation and technology is not new, it is becoming more important with the increased levels of regulation and a focus on data and reporting. In addition, RegTech addresses the changes in financial services associated with dynamic FinTech, which has driven a different way of undertaking financial services which need to be addressed by

regulations. The disruption caused by FinTech will require a different, potentially significantly more data-intensive approach from regulators. RegTech is expected to incorporate automated analysis and real-time data provision as well as enhanced AML checking. The use of biometrics and social media changes how due diligence may be undertaken.

The FCA in the UK, similar to other regulators, has stated that they would specifically like to see solutions in the areas of:

- anti-fraud
- regulatory reporting
- market surveillance technologies
- social media analytics, and
- prudential analytics.

3.2.4 Cloud Data Hosting

Cloud data hosting agreements allow the data owner (eg, a financial institution) to store their data on a network of connected virtual and physical servers known as a cloud. The advantages are that the institution does not require in-house servers, the resources can be scaled to meet the needs of the user and the institution only pays for what they use. Cloud data hosting may, however, raise security issues, particularly in relation to sensitive data. Regulators usually consider cloud data hosting to be a form of outsourcing and apply the outsourcing regulations. Within the EU, the General Data Protection Regulation (GDPR) in relation to data processors and data controllers, applies to cloud data hosting.



End of Chapter Questions

1. What is corporate governance?

Corporate governance involves the manner in which the business and affairs of a firm are governed by its board and senior management, including how they:

- set the firm's strategy and objectives
- determine the firm's risk tolerance/appetite
- operate the firm's day-to-day business
- protect the interests of depositors, meet shareholder obligations, and take into account the interests of other recognised stakeholders, and
- align corporate activities and behaviour with the expectation that the firm will operate in a safe and sound manner, with integrity and in compliance with applicable laws and regulations.

Answer reference: Section 1.1

2. What can lead markets to lose confidence in the ability of a bank to properly manage its assets and liabilities?

Poor corporate governance can:

- Contribute to bank failures, which can pose significant public costs. Such failures also have the potential to impact on any applicable deposit insurance system, and there is the possibility of broader macroeconomic implications (such as contagion risk and impact on payment systems). This was illustrated in the global financial crisis that began in mid-2007.
- In addition, poor corporate governance can lead markets to lose confidence in the ability of a bank to properly manage its assets and liabilities, including deposits, which could in turn trigger a bank run or liquidity crisis.

Answer reference: Section 1.1

3. What is the definition of corporate governance according to the Organisation for Economic Co-operation and Development (OECD) Principles?

The OECD's principles definition of corporate governance is '*a set of relationships between a company's management, its board, its shareholders, and other stakeholders*'.

Answer reference: Section 1.1

4. Name the board structure typically found in Germany.

The dual (or 'Two Tier') board is common in Germany (and other continental European countries).

Answer reference: Section 1.4

5. What board structure is categorised by one single board comprising both executive and non-executive directors?

The unitary board of directors is characterised by one single board comprising both executive and non-executive directors (NEDs).

Answer reference: Section 1.4

6. What is the difference between unitary and dual boards?

The unitary board is characterised by one single board comprising both executive and non-executive directors. The dual board consists of a supervisory board and an executive board of management where there is a clear separation between the functions of supervision and management.

Answer reference: Section 1.4

7. Define a silo structure.

A 'silo' structure is one in which isolated groups of workers report to their own line or functional manager, with the potential result of effort being duplicated where multiple silos each have similar needs.

Answer reference: Section 1.5.2

8. Name the four elements of the concept of independence for compliance functions.

The concept of independence involves four related elements, as shown below:

1. The compliance function should have a formal status within the firm.

2. There should be a group compliance officer or head of compliance with overall responsibility for co-ordinating the management of the firm's compliance risk.
3. Compliance function staff, and in particular the head of compliance, should not be placed in a position where there is a possible conflict of interest between their compliance responsibilities and any other responsibilities they may have.
4. Compliance function staff should have access to the information and personnel necessary to carry out their responsibilities.

Answer reference: Section 1.5.3

9. How can senior management enhance the ability of internal audit to identify problems with a bank's risk management systems?

The board and senior management can enhance the ability of the internal audit function to identify problems with a firm's risk management and internal control systems by:

- encouraging internal auditors to adhere to national and international professional standards, such as those established by the Institute of Internal Auditors
- promoting the independence of the internal auditor, for example by ensuring that internal audit reports to and has direct access to the board or the board's audit committee
- recognising the importance of the audit and internal control processes and communicating their importance throughout the firm
- utilising, in a timely and effective manner, the findings of internal audits and requiring timely correction of identified problems by senior management, and

- engaging internal auditors to judge the effectiveness of the risk management and compliance function, including the quality of risk reporting to the board and senior management, as well as the effectiveness of other key control functions.

Answer reference: Section 1.6

10. Name five examination areas used when conducting due diligence on a hedge fund.

Due diligence of a hedge fund would include (non-exhaustive) an examination of the following factors:

- a fund snapshot
- disclosed investment strategy
- historical returns
- assets under management (a copy of the fund's portfolio from the custodian is usually requested)
- audited financial statements if the fund is regulated
- fund's terms and details
- regulatory registration (if any)
- risk factors, or
- valuation.

Answer reference: Section 1.7

11. Name three of the Bank for International Settlements (BIS) principles for enhancing corporate governance.

See the table detailing the BIS principles for enhancing corporate governance.

Answer reference: Section 1.9

12. What is the difference between risk and uncertainty?

Uncertainty is a general concept that simply recognises the potential of different outcomes arising. Uncertain matters tend to be vague rather than measurable; science or statistics are unable to help us make decisions. However, where we are able to use data or probability theory to assess and analyse potential outcomes, we are able to talk in terms of 'risk'.

Answer reference: Section 2.1

13. Name two external risks.

External risks arise from changes in:

- the global economy
- the political arena
- the competitive environment
- social and market forces, and
- technological innovation.

Answer reference: Section 2.2

14. What are the three main ways in which political change can affect the financial services sector?

Political changes, being so closely linked to the economy, can affect financial services firms in three main ways:

- A rise or fall in the markets in which firms invest.
- An increase or decrease in demand for the products which the industry sells.
- Changes to the legislative and regulatory environment in which financial services firms operate.

Answer reference: Section 2.2.2

15. Risks can arise from external stakeholders, such as a parent company. Name two other external stakeholders that can also be a source of risk for a business.

External stakeholders that cause business risk typically include a firm's parent company, any major institutional investors and any particularly large or important customers.

Answer reference: Section 2.2.6

16. What is the key to managing stakeholder risk?

The key to managing stakeholder risk is to:

- build relationships at senior levels
- understand their agenda and how it may differ from the firm's own agenda, and
- manage expectations with any new developments.

Answer reference: Section 2.2.6

17. What is gearing and how does it increase risk?

Also known as leverage, gearing is the ratio of a firm's debts to the value of its equity. A company which, on paper, looks sound, but which has become over-gearred can suffer disproportionately if interest rate rises cause its debt to become more expensive, or if its revenues fall to a level too low to repay its debt.

Answer reference: Section 2.3.3

18. What are the key elements of risk management?

Risk management focuses on identifying what could go wrong, evaluating which risks should be dealt with, and implementing strategies to address those risks.

Answer reference: Section 2.4

19. Explain PESTLE analysis.

PESTLE analysis – this is an analysis of the external macro environment in which a business operates. This environment will inevitably contain factors which are beyond the firm's control or influence, but which are, nevertheless, important to be aware of when developing new products, businesses or strategies. PESTLE analysis is often performed as a brainstorm with internal and external experts. Risks are considered under the following headings:

- political
- economic
- social
- technical
- legal, and
- environmental.

Answer reference: Section 2.5.1

20. How do you calculate a risk score?

A simple overall risk assessment is arrived at by multiplying the likelihood rating scores with the impact rating scores:

Risk score = likelihood score × impact score.

Answer reference: Section 2.5.1

21. When assessing and scoring a risk, two aspects are considered. One is its likelihood. What is the other?

The other is the impact loss.

Answer reference: Section 2.5.1

22. What is a SWOT analysis?

A SWOT analysis focuses participants' attention systematically on the firm's:

- strengths
- weaknesses
- opportunities, and
- threats.

Answer reference: Section 2.5.2

23. What is meant by a firm's risk appetite?

Risk appetite, or risk tolerance, is the level(s) of loss that the firm is willing to accept in its different businesses over a specified time horizon at a given level of confidence, ie, the level of expected loss that the firm will not (or cannot) mitigate.

Answer reference: Section 2.5.3

24. Name four risk register column headings.

The usual column headings for a risk register would be:

1. business objective
2. description of associated risk
3. risk ranking
4. lead person or department
5. action plan
6. target and completion dates

7. sources of assurance and oversight (which may or may not be the lead person or department)
8. mitigating controls.

Answer reference: Section 2.5.4

25. What is the difference between compliance and risk management?

Compliance focuses primarily on ensuring that all rules and regulations are followed. Risk management focuses on ensuring that risks are understood, and that proactive decisions are made about which risks to take and which to manage or avoid.

Answer reference: Section 2.5.7

26. Give three examples of issues that could raise an institution's level of compliance risk.

The three examples of issues that could raise an institution's level of compliance risk are:

1. substandard account acceptance and review processes
2. shortcomings in the ethical culture and expertise of management and staff, or
3. weak internal compliance systems and training programmes.

Answer reference: Section 2.5.7

27. What is the definition of compliance risk?

The expression 'compliance risk' is defined by the BIS as *'the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a firm may suffer as a result of its failure to comply*

with laws, regulations, rules, related self-regulatory organisation standards, and codes.'

Answer reference: Section 3

28. Name five ways in which technology can help the compliance function.

Five examples of the ways in which technology can help the compliance function are:

- Prevention – ensuring that compliance requirements are built into line-of-business applications, such as workflow and image systems. An example would be to include prompts relating to anti-money laundering checks when new business applications are being processed.
- Detection systems and reports which identify exceptions and specific types of transactions. These could aid the oversight of high-risk trades or enable the identification of politically exposed persons or sanctions-list matches.
- Recording incidents, control failures, breaches and complaints to meet record-keeping requirements and the production of management information to identify trends in error rates. This will help to identify at an early stage any systemic problems that may arise.
- Online regulatory information systems, providing up-to-date information on regulatory changes, industry developments, including regulator and supervisory actions. This will include information on any systemic risks identified.
- Effective online training and refresher courses on key aspects, including financial crime prevention, treating customers fairly and handling complaints. The results of online testing can demonstrate any gaps in knowledge which may give rise to a compliance risk.

Answer reference: Section 3.1

29. What is cybercrime?

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing or spamming) or is used as a tool to commit an offence.

Answer reference: Section 3.2.1

30. Describe FinTech and RegTech.

- FinTech refers to the use of technology to advance or change the financial sector.
- RegTech, short for regulatory technology, is the use of technology to facilitate the delivery of regulatory requirements.

Answer reference: Sections 3.2.2 and 3.2.3

31. What are the issues with cloud data hosting?

Cloud data hosting may raise security issues, particularly in relation to sensitive data.

Answer reference: Section 3.2.4



Appendices

1. **Compliance Manual – An Example of the Contents**
2. **Sample Checklist of Regulatory Requirements for Outsourcing**
3. **Proforma Monitoring Report**
4. **Regulator Enforcement Procedure**
5. **Global Standards**
6. **Principles of Good Practice for the Handling of Inside Information**

Appendix 1 – Compliance Manual – An Example of the Contents

Table of Contents

1. Introduction	5
1.1 The Purpose of the Compliance Manual	5
1.2 Scope of the Compliance Manual	5
1.3 The Regulations	5
2. Regulatory Framework	7
2.1 Introduction	7
2.2 Principles for Businesses	8
2.3 Scope of Permissions	9
3. Organisational Context	10
3.1 The Divisions within Risk & Compliance	10
3.2 Department Structure	12

4. Senior Management Responsibilities, Standards and Approved Persons	13
4.1 Introduction	13
4.2 Threshold Conditions	13
4.3 Suitability	14
4.4 Standards of Conduct Expected of a Regulated Company and its Employees	14
4.5 Compliance Risk	14
4.6 Approved Persons	15
5. Conduct of Staff	16
5.1 Introduction	16
5.2 Confidentiality	16
5.3 Anti-Bribery Policy	17
Reporting of Acts of Bribery	17
Market Practice	17
5.3.1 Gifts and Benefits	18
5.4 Internet and Email Monitoring	19
5.5 Insider Dealing	20
5.5.1 Introduction	

	20
5.5.2 How is the Offence Committed?	20
5.5.3 How do I Avoid Problems?	21
5.6 Personal Account (PA) Dealing	22
5.6.1 Introduction	22
5.6.2 General Rule	22
5.6.3 Transactions that Require Notification & Approval	22
5.6.4 Transactions that Require Notification only	23
5.6.5 Dealing Closed Period	24
5.6.6 Disciplinary Procedures for Non-Compliance	24
5.6.7 Confidentiality	25
6. Treating Customers Fairly	26
6.1 Introduction	26
6.2 The Regulations	26
6.3 Areas of Regulator Focus	27
6.4 What do the Regulations Require of YOU and the firm?	28
7. Whistleblowing Policy	29

8. Data Protection

32

8.1 Introduction

32

8.2 Authorisation

32

8.3 Access Rights

33

8.4 Security and Confidentiality

34

8.5 Overseas Processing

34

8.6 Data Protection Breaches

35

8.7 Miscellaneous

35

9. Financial Crime Prevention

36

9.1 Introduction

36

9.2 What is Money Laundering

37

9.3 Regulator Role in the Prevention of Money Laundering

37

9.4 Role of the Money Laundering Reporting Officer (MLRO)

37

9.5 The 3 Stages of Money Laundering

38

9.6 What do the Regulations Require of YOU and the firm?

38

9.7 What are the Offences and Punishments Relating to Money Laundering?

39

9.8 Other Forms of Financial Crime

40

9.9	What Circumstances might make you Suspicious?	40
9.10	When might I be Suspicious?	40
10.	Client Money and Client Assets	42
10.1	Introduction	42
10.2	What is Client Money?	42
10.3	Client Money and Asset Regulations	42
11.	Breaches	43
11.1	Introduction	43
11.2	Breach Register	43
11.3	Significant Breach	43
11.4	Notifiable Breach	43
12.	Complaints	45
12.1	Introduction	45
12.2	Scope of Regulatory Requirements	45
13.	Training & Competence (T&C)	47

13.1	Introduction and Scope of the Training & Competence Scheme	47
13.2	Regulatory Requirement	48
13.3	T&C Activity	48
13.4	Roles of Compliance and Human Resources Departments	49
13.4.1	Risk & Compliance Department	49
13.4.2	Human Resources	49
13.5	A Status of Competence	50
Appendix 1 – Approved Persons / Senior Managers Regime		51
Appendix 2 – Glossary of Terms for Personal Account Dealing		53
	List of Client Companies and Holding Companies that are Listed on the Stock Exchange	54
	List of Products Administered by Subject to the Personal Account Dealing Policy	55
	List of Companies with a Business Relationship with the Company	56
Appendix 3 – TCF Policy		57
Appendix 4 – Client Money		60
Appendix 5 – Common Types of Breaches		71
Appendix 6 – Complaints		74

Appendix 2 – Sample Checklist of Regulatory Requirements for Outsourcing

A firm must:

1. when relying on a third party for the performance of operational functions which are critical for the performance of regulated activities, on a continuous and satisfactory basis, ensure that it takes reasonable steps to avoid undue additional operational risk
2. not undertake the outsourcing of important operational functions in such a way as to impair materially:
 - a. the quality of its internal control, and
 - b. the ability of the Regulator to monitor the firm's compliance with all obligations under the regulatory system.

A firm should have effective processes to identify, manage, monitor and report risks and internal control mechanisms.

If a firm outsources critical or important operational functions or any relevant services and activities, it remains fully responsible for discharging all of its obligations under the regulatory system and must comply, in particular, with the following conditions:

1. the outsourcing must not result in the delegation by senior personnel of their responsibility
2. the relationship and obligations of the firm towards its clients under the regulatory system must not be altered

3. the conditions with which the firm must comply in order to be authorised, and to remain so, must not be undermined, and
4. none of the other conditions subject to which the firm's authorisation was granted must be removed or modified.

A firm must exercise due skill, care and diligence when entering into, managing or terminating any arrangement for the outsourcing to a service provider of critical or important operational functions or of any relevant services and activities.

A firm must in particular take the necessary steps to ensure that the following conditions are satisfied:

1. the service provider must have the ability, capacity, and any authorisation required by law to perform the outsourced functions, services or activities reliably and professionally
2. the service provider must carry out the outsourced services effectively, and to this end the firm must establish methods for assessing the standard of performance of the service provider
3. the service provider must properly supervise the carrying-out of the outsourced functions, and adequately manage the risks associated with the outsourcing
4. appropriate action must be taken if it appears that the service provider may not be carrying out the functions effectively and in compliance with applicable laws and regulatory requirements
5. the firm must retain the necessary expertise to supervise the outsourced functions effectively and to manage the risks associated with the outsourcing, and must supervise those functions and manage those risks
6. the service provider must disclose to the firm any development that may have a material impact on its ability to carry out the outsourced functions effectively and in compliance with applicable laws and regulatory requirements

7. the firm must be able to terminate the arrangement for the outsourcing where necessary without detriment to the continuity and quality of its provision of services to clients
8. the service provider must cooperate with the Regulator and any other relevant competent authority in connection with the outsourced activities
9. the firm, its auditors, the Regulator and any other relevant competent authority must have effective access to data related to the outsourced activities, as well as to the business premises of the service provider; and the Regulator and any other relevant competent authority must be able to exercise those rights of access
10. the service provider must protect any confidential information relating to the firm and its clients, and
11. the firm and the service provider must establish, implement and maintain a contingency plan for disaster recovery and periodic testing of back-up facilities where that is necessary having regard to the function, service or activity that has been outsourced.

A firm must ensure that the respective rights and obligations of the firm and of the service provider are clearly allocated and set out in a written agreement.

A firm must make available on request to the Regulator and any other relevant competent authority all information necessary to enable the Regulator and any other relevant competent authority to supervise the compliance of the performance of the outsourced activities with the requirements of the regulatory system.

A firm should notify the Regulator when it intends to rely on a third party for the performance of operational functions which are critical or important for the performance of relevant services and activities on a continuous and satisfactory basis. In some countries, prior

approval may be required, and permission may be limited geographically or for certain activities may be denied.

Appendix 3 – Proforma Monitoring Report

Evaluation of Compliance and Controls for:

Overall Report Rating Level:



The controls in place adequately address all significant risks identified and are operating effectively

Area/Process/Activity [eg, Charities Dealing]

Period Covered [Q1 2024]

Risk & Compliance Monitor: [Manager]

Report Addressed to: [The executive/senior manager of the area concerned]

Board Directors	Group Executives or Senior Management	Key UK Recipients	Internal Audit
AAA	BBB	CCC	DDD

Risk & Compliance

Reviewing Manager: [Team Leader]

Copies to:

File Reference: [File location online]

Version: [Final Draft]

Date Published: [29/3/24]

Contents

Part A – Executive Summary

Introduction

Compliance Monitoring Opinion

Prior Compliance Monitoring Opinion

Level One Recommendations

Rationale Supporting the Compliance Opinion

Business Area Executive Summary

Evaluations of the Central Environment

Acknowledgements

Part B – Recommendations

Level One Recommendations

Level Two Recommendations

Level Three Recommendations

Observations

Appendix A – Monitoring Report Objectives and Scope

Appendix B – Definition of Monitoring Opinions and Recommendation Levels

Appendix C – Sample Size Volumes by Company

Part A – Executive Summary

Introduction: This report sets out the findings of the Monitoring Team review of Dealing. Xxxxxx, Compliance Manager carried out the

Compliance Monitoring Opinion:

Red	Amber	Green
		

Prior Compliance

Monitoring Opinion: This area of business was last reviewed in Q3 2024, Green rating.

Level One Recommendations: None.

Rationale Supporting the Compliance Opinion:

To ensure RAG ratings are applied consistently across all business areas, each Level 1, 2 and 3 recommendation will have a numeric value applied. The total will determine the overall RAG rating.

Level 1 recommendation 25 points.

Level 2 recommendation 5 points.

Level 3 recommendation 2 points.

The total of the scores applied are added together to determine the overall review status.

0-19 will receive a Green review, 20-49 Amber and 50 or over will be Red.

These scoring rules will serve as a guide, which will be applied in the main, but the Compliance Monitoring Team reserve the right to modify a RAG rating where they are able to provide an overriding rationale.

The controls in place adequately address all significant risks identified and are operating effectively.

The review identified:

No Level 1 recommendations

Two Level 2 recommendations

Two Level 3 recommendations

No Observations

Business Area Executive Summary

Evaluation of the control environment

Process Overview:

Sample Size:

A total of (xx) work items were reviewed during the sampling period 1 October – 31 December 2023 across four client companies.

Staffing Levels:

Charities Dealing operates under the Executive Management of (name of the executive).

The team consists of (13) staff:

One Senior Manager (T&C Regulatory Supervisor)

Three Managers (one T&C Regulatory Supervisor and two T&C Overseers)

(x) Team Leaders

(x) Senior Administrators

(x) Two Administrators

(The experience within the team ranges from two months to ten years. There are two T&C Regulatory Supervisors and two T&C Overseers within the team. One Overseer is classed as Competent and one classed as a Trainee. There are two T&C Successors, both classed as trainees. One T&C file was reviewed and no exceptions were identified.)

Controls:

Checklists across all companies were reviewed for one individual day per month over the three months of the sampling period. The

Duplicate Deals Report, Non-End Report, Deal Timing Report, Large Deals Report, Exceptions Report, Cancelled/Rebooked Deals Report, Cancelled Deals Report, Failed Correspondence Misc. Report & Backdated Deals Report were also reviewed for each of these days and no exceptions were identified.

Control Certification has been reviewed across all companies during the sampling period. Postal Dealing UK raised one high issue and 31 low issues. All controls were reviewed and no exceptions were identified.

Procedures were reviewed and some exceptions were identified.

The Risk Assessment was reviewed and no exceptions were identified.

The Knowledge Base was reviewed and no exceptions were identified.

Breaches/Complaints:

(x) Breaches were recorded against the process during the sampling period, affecting two companies. One Deal was booked late and one Deal booked the wrong amount.

100% of breaches were sampled to check that the resolution had been actioned. No exceptions were identified.

No Data Protection Breaches were recorded against the process during the sampling period.

No Complaints were recorded against the process during the sampling period.

(xxx) pieces of work were completed during the sampling period.
Breach rate/Complaints rate (xx) (xx)

Recommendations:

There were four recommendations and no observations identified within this review.

There are no Level 1 recommendations.

There are two Level 2 recommendations.

- XXXXXXXX
- XXXXXXXX

There are two Level 3 recommendations:

- X
- •X

There were no observations made.

Acknowledgements:

Compliance Monitoring would like to thank the Charities Dealing Department for their help in completing this report.

Part B – Recommendations

Level One Recommendations: There are no Level 1 recommendations

Level Two Recommendations:

Rationale		Recommendation			
[Area of business]: [issue] [details of the issue found] This issue affected [xxxx] company:		[eg, Breach to be recorded]			
		Management response and comment			
		Breach raised [comment re action taken and feedback]			
Monitoring Recommendation Number	[000]	Responsibility	[Exec Director]	Status/Deadline	Closed

Level Three Recommendations:

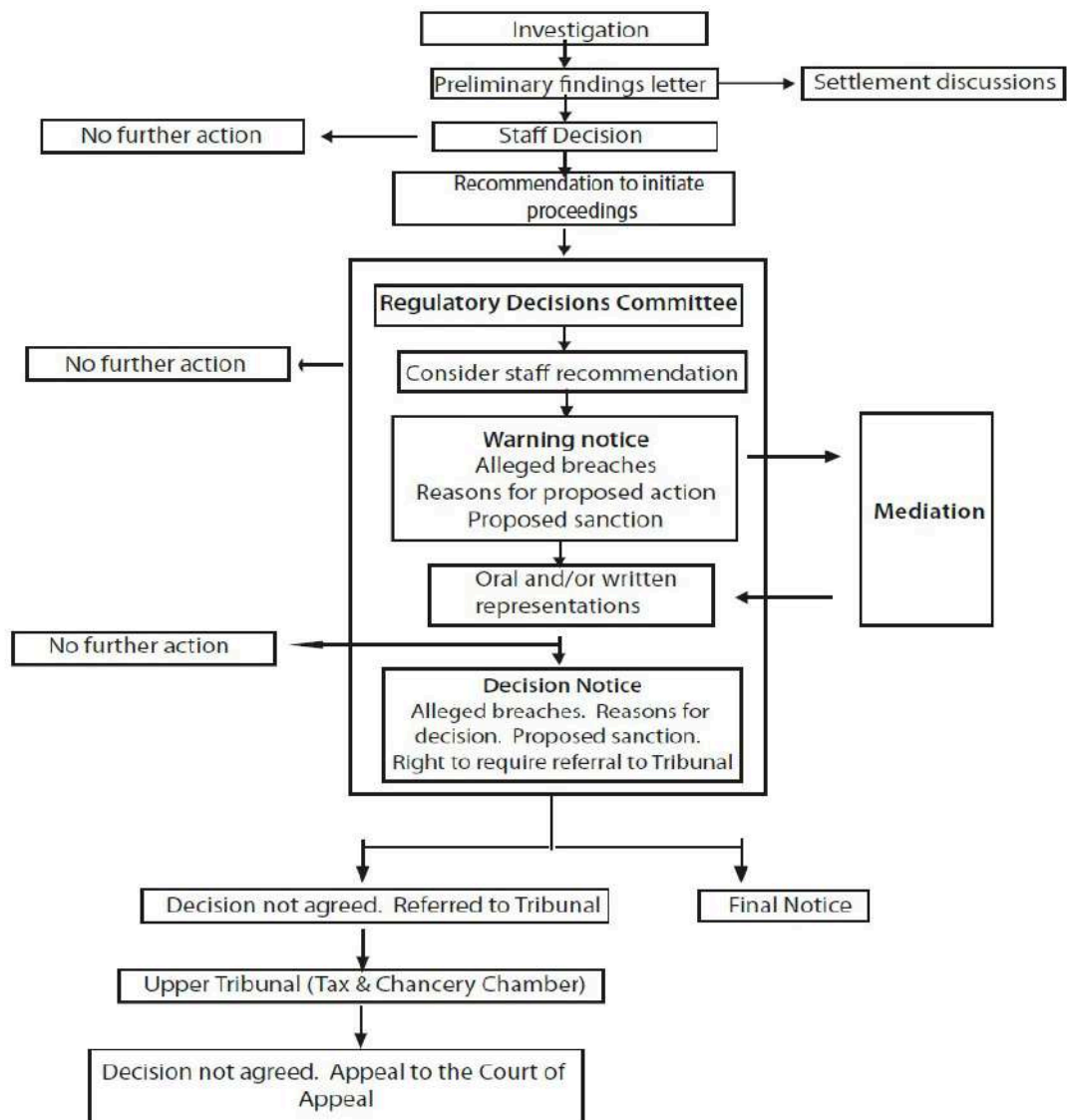
Rationale		Recommendation			
		Management response and comment			
Monitoring Recommendation Number	1315	Responsibility	B Jones	Status/Deadline	30/06/22

Observations made.

- Xxxxx
- Xxxxx
- Xxxxx
- Xxxxx

Appendix 4 – Regulator Enforcement Procedure

The diagram below shows the typical course of regulatory enforcement proceedings in the UK, as instituted by the Financial Conduct Authority (FCA) (note that as of November 2021, some of the Regulatory Decisions Committee (RDC) decisions have been moved to the Executive Procedure):



Appendix 5 – Case Study: Global Standards

Background

You are the Marketing Director of a UK-based international Fund Management Group which provides a range of collective funds sold mainly in the UK and Europe, where increasing competition has required ever greater marketing efforts and the development of innovative, new fund offerings.

One such new fund invests in high-tech companies located in and serving developing nations and uses some innovative derivative techniques to leverage performance, which has been very promising, although rather volatile.

As a result of UK regulatory requirements, detailed disclosure has been necessary in marketing and sales literature, to inform potential investors of the significant risks, including the volatility, to which the fund is subject. You consider that these explicit disclosures have constrained sales of what you are advised is, inherently, a sound fund.

The policy of your Group is that each group company must comply with the laws and regulations of the country in which they operate. There are no Group-wide standards.

The Situation

Faced with increasing competition and stringent regulatory requirements within the UK and European Union (EU), one of your team suggests that this high-tech fund be promoted, via your Asian

subsidiaries, to potential investors in countries in that region where regulatory requirements are less demanding.

On researching this idea, you find that there are several countries in the region where there appears to be growing demand for similar investments and where the local regulatory requirements do not require specific disclosure of the degree of risk or of the likely volatility of the fund. Furthermore, you ascertain that in two of these particular countries there is no equivalent to the UK Financial Services Compensation Scheme (FSCS).

An additional attraction of the fund is that it invests in a number of high-tech companies which are located in the region where you are considering increasing your promotion.

Your research also reveals that one of your principal competitors has enjoyed recent success in promoting one of its funds in this region, without any apparent problems arising from regulators or investors. Their fund also seems to be relatively high-risk, but this factor is not prominent in their marketing literature. This seems to be an attractive marketing opportunity; what would you do?

Specific Factors to Consider

In favour of increased promotional and sales activity are:

- This is an inherently sound fund in a region where there is growing demand and where the fund invests directly.
- There are no legal or regulatory requirements for your subsidiary to make the detailed risk and volatility disclosures that may have hindered marketing in the UK.
- There are no investor compensation arrangements to worry about.
- A competitor is, apparently, enjoying success without any problems.

On the other hand:

- Benign regulatory requirements in the region might change.
- The volatile performance of the fund means that the possibility of loss, as well as profit, by investors is higher than is normally acceptable.
- Foreign investors would be treated less favourably than home investors.
- In the event of losses by unsophisticated investors in this unrestricted fund, there might be a significant public backlash.
- Such a situation might damage your Group's reputation.

Ethical Deliberations

Your first consideration might be whether it is actually ethical for your Group to selectively adopt weaker local legal/regulatory requirements rather than the higher standards required in your home country.

Should it be a matter for each subsidiary board as to the level at which it sets its ethical standards?

In the event that the fund loses money and your firm considers that it is in its interests to compensate UK investors, notwithstanding the risk warning given, would you be comfortable that a less generous approach is taken towards investors in a different regulatory environment?

How much should the fact that a competitor, possibly with less rigorous standards, is taking advantage of a particular situation, influence your recommendation?

Recommendation

For a group with international or global representation, the absence of a group standard can be corrosive of standards, which are likely to gravitate towards the acceptance of the lowest standard.

However, in devising group standards it should be recognised that the standards accepted in the 'home' state are not necessarily the 'best' and higher standards may apply elsewhere. Additionally, there may be a distinction between minimum acceptable commercial standards and regulatory requirements.

Accordingly, by adopting the positions first, that a minimum group standard should apply and, secondly, that this should require the adoption of the higher of local standards or minimum group standards, the answer in this case would be that investors overseas should be subject to the same protections as are offered to UK investors, notwithstanding that the opportunity exists to get away with lower standards.

CISI Principles Applicable

Although all CISI principles are important, the below are most applicable in this context:

1. To act honestly and fairly at all times when dealing with clients.
2. To act with integrity in fulfilling your responsibilities.
3. To observe applicable law, regulations and professional conduct standards according to principles rooted in trust, honesty and integrity.
4. To strive to uphold the highest personal standards, including rejecting short-term profits which may jeopardise your reputation and that of your employer.

Appendix 6 – Principles of Good Practice for the Handling of Inside Information

1. Policies and procedures

Policies and procedures for the use and control of inside information should be established and reviewed from time to time. These should recognise the responsibility to control access to inside information and reduce the risk of misuse. There should be clear responsibility within organisations for overseeing controls and procedures in relation to inside information.

2. Awareness and training

Appropriate measures should be taken, including training, to assist staff in understanding the importance of keeping information secret and the implications of improper disclosure – including the potential civil and criminal liabilities for the firm and the individual. Ensuring policies are capable of being readily understood by all relevant staff is an important part of this approach.

3. 'Need to know' and other information controls

Reasonable steps should be taken to limit the number of those with access to inside information. Where practicable a 'need to know' policy should be applied.

4. Passing price-sensitive information to third parties

Reasonable care should be taken to ensure that where inside

information is provided to a third party, the third party is aware of its obligations in relation to the use and control of the information.

5. Information technology security

Appropriate consideration should be given to the security of and access to inside information on IT systems, including the implementation of controls to limit access.

6. Personal accounting policies

Reasonable consideration should be given to establishing personal account (PA) dealing policies; those policies should be made clear to staff along with the civil and criminal penalties for dealing on the basis of inside information or for enabling such dealing.

The principles and the practice suggestions in the annex are not a substitute for the relevant laws and regulations nor are they intended to have any legal effect or to be used by the FCA or other regulators: their objective is simply to help raise standards generally in relation to the use and control of inside information.

Suggested Policies and Procedures for the Handling of Inside Information

1. Policies and procedures

A firm's policies and procedures for the use and control of inside information should be established and reviewed from time to time. These should recognise the responsibility to control access to inside information and reduce the risk of misuse. There should be clear responsibility within organisations for overseeing controls and procedures in relation to inside information.

Good practice points to be considered include:

- Appoint a senior person with responsibility for maintaining good practice procedures; ensure they are trained and resourced and see that all members of staff know who this person is.
- Maintain documented policies on price-sensitive information handling that are regularly reviewed and updated.
- Conduct an internal review of the operation of policies, systems and procedures at least annually.
- Ensure that insider lists are complete, accurate and regularly updated.
- Have in place a policy on external contact enquiries, particularly with the media.
- Staff policies:
 - maintain procedures making it easy to report and discuss sensitive information being handled inappropriately
 - when staff who hold sensitive information leave a firm or change roles, conduct an 'exit interview' during which the leaver is reminded of the ongoing confidentiality of inside information
 - a policy on introducing temporary or contract staff to company policies regarding inside information
 - undertake staff vetting such as criminal record checks and references from previous employers, and
 - employment contracts to make staff aware of their duty of care regarding insider information together with the employer's right to access email, phone and other communication records as part of the employer's policy with regard to insider dealing.

2. Awareness and training

Appropriate measures should be taken, including training, to assist staff in understanding the importance of keeping information secret and the implications of improper disclosure – including the potential civil and criminal liabilities for the firm and the individual. Ensuring policies are capable of being readily understood by all relevant staff is an important part of this approach.

Good practice points for consideration include:

- Foster a culture that respects the sensitivity of inside information and establishes an awareness of the penalties for its abuse.
- Have a dedicated training responsibility.
- Hold induction training, as well as refresher training, for all staff regardless of position (including support staff).
- As new rules come into force, maintain an 'update' system.
- Test awareness and understanding from time to time.
- Maintain training records and review the process annually.

3. 'Need to know' and other information controls

Reasonable steps should be taken to limit the number of individuals with access to inside information. Where practicable, a 'need to know' policy should be applied.

Good practice points for consideration include:

- A policy for making someone an insider, including only passing inside information to colleagues if they are first alerted to their responsibilities regarding the information.
- Limit the number of insiders to a practical minimum and introduce a requirement to justify adding people to the insider list ('need to know' criteria).
- Communicate to other insiders when someone is removed from an insider list.

- Where practicable, separate deal teams from other parts of the business.
- Security of price-sensitive information:
 - have a policy on secure disposal of confidential documents/soft copy
 - monitor and enforce a clear desk policy to reduce the risk of non-insiders seeing papers left on desks (eg, contract cleaning companies)
 - maintain formal, written procedures for staff working off-site
 - use code names disguising the identities of relevant parties that are effective and not obvious
 - discourage staff reading or working on sensitive papers in public and discussing sensitive matters in public (eg, in taxis)
 - require staff working on deals only to discuss deals in meeting rooms
 - control the email distribution of sensitive information, ensuring the regular use of passwords on documents
 - control the hard copy distribution of papers (eg, numbered copies or bar codes on documents);
 - ensure hard copy sensitive information is stored in lockable cabinets and soft copy securely stored also, and
 - use restricted access systems in work and IT systems areas where sensitive information is handled.

4. Passing price-sensitive information to third parties

Reasonable care should be taken to ensure that where inside information is provided to a third party, the third party is aware of its obligations in relation to the use and control of the information.

Good practice points for consideration include:

- Maintain formal, written procedures when adding third parties to the information chain, formally making them insiders and spelling out the responsibilities inherent in handling the information.
- Obtain comfort that third parties appreciate the importance of safeguarding inside information and have appropriate procedures in place.
- Consider the third party's suitability as a recipient.
- Include third parties in the information chain as late as practical in the process.
- Orally explain responsibilities rather than simply exchanging standard confidentiality letters.

5. Information technology security

Appropriate consideration should be given to the security and access to inside information on IT systems, including the implementation of controls to limit access.

IT configurations will differ significantly between service providers and some of the following may not be applicable; however good practice points for consideration include:

- Where practical, restrict IT access only to named individuals in preference to a company-wide, open IT access.
- The use of a secure 'data room' with a robust portal restricted to named individuals.
- IT and other management support considered as insiders to comply with appropriate policies.
- Once a member of staff leaves or changes roles, the individual's IT access is to be removed.
- Employ 'ethical hackers' to check the robustness of IT systems and keep abreast of any new methods of data theft.

- Use code names and passwords for IT files and folders, including email subject lines.
- Password-protect all electronic equipment.
- Laptops, smartphones and such devices to have automatic locking after brief periods.
- Technology to generate an audit trail of access to sensitive files.
- Restrict emails with sensitive information going to personal websites.
- Maintain procedures for 'fat finger' errors on emails, letters or faxes (recalling emails quickly and IT check showing if emails have been opened).
- Use virtual private networks for staff who need access to system when working off-site.

6. **Personal accounting policies**

Reasonable consideration should be given to establishing PA dealing policies; those policies should be made clear to staff along with the civil and criminal penalties for dealing on the basis of inside information or for enabling such dealing.

Good practice points for consideration include:

- Maintain a formal, written procedure regarding PA dealing for all members of staff, ensuring awareness of this (consider including it in employment contracts) and test compliance from time to time.
- Ensure that staff are aware that insider dealing is a criminal offence.
- Explicit reference in PA dealing policy to derivatives, related products, sector 'knock-on', etc.
- Policy covers dealings under power of attorney and by immediate family.

- Policy addresses approach to dealings through discretionary accounts or manager, having regard to the independence of discretionary manager dealings.
- Consider restricting staff or relevant staff members from dealing without permission from their immediate manager or compliance officer. Refusal may be given without further explanation.
- Restrict staff members of service providers from dealing in client companies. (This should not apply where assets are managed by others for a staff member on a discretionary basis without input from the person concerned.)
- Require staff to maintain updated declarations of their holdings.
- Keep a written log of permission requests and their outcomes, including risk-based records of staff trading against announcements.



Glossary

Anti-Money Laundering Directive (AMLD)

The European Union's (EU's) AMLD is aimed at preventing the use of the financial system for the purposes of money laundering or terrorist financing. Since the first directive was adopted in 1990, it has been updated a number of times to ensure it remains current. The AMLD is incorporated in the laws and regulations of all EU member states.

Appointed Representative

An appointed representative is an individual or organisation that carries out certain regulated activities on behalf of an authorised firm under contract. The authorised person must have accepted in writing responsibility for the conduct of these regulated activities.

Authorisation

The requirement for firms to obtain authorisation from their regulator prior to conducting investment business.

Business Risk

The risk of loss due to an adverse external environment, such as high inflation affecting labour costs; an over-competitive market reducing margins or legal, tax or regulatory changes in the markets.

Central Bank

Central banks typically have responsibility for setting a country's or a region's short-term interest rate, controlling the money supply,

acting as banker and lender of last resort to the banking system and managing the national debt.

Central Counterparty (CCP)

The guarantor of contracts normally, but not necessarily, for exchange-traded products. Usually the clearing house of an exchange.

Central Securities Depository (CSD)

A central securities depository (CSD) is an institution that holds financial instruments, including equities, bonds, money market instruments and mutual funds.

Chinese Walls

Organisational barriers to the flow of information set up in large firms, to prevent the movement of confidential, sensitive information between departments and to manage any potential conflicts of interest.

Client

Individuals or firms that conduct business through an authorised person. Every client is either a customer (retail or professional) or an eligible counterparty.

Client Assets

Securities or other assets held by a firm on behalf of its clients. The assets have to be kept separate from the firm's own assets (segregated).

Compliance Risk

The risk to earnings or capital arising from violations; or non-conformance with laws, rules, regulations, prescribed practices or ethical standards.

Controlled Functions

Certain roles within authorised firms for which the Financial Conduct Authority (FCA) in the UK requires the role holder to be approved.

Credit Default Swap (CDS)

A bilateral financial contract in which one counterparty (the protection buyer) pays a periodic, or one-off fee (typically expressed in basis points on the notional amount), in return for a contingent payment by the other counterparty (the protection seller) following a credit event of a reference entity.

Credit Risk

The potential loss of earnings or capital due to an obligor's failure to meet the terms of a contract or otherwise failing to perform as agreed.

Dematerialised

The term used to describe stock which is held in electronic form rather than having ownership evidenced by way of paper certificates.

European Securities and Markets Authority (ESMA)

The European body responsible for the regulation of investment firms and markets and directly responsible for the regulation of credit rating agencies.

European Supervisory Authorities (ESAs)

Pan-European financial services regulatory bodies, each with responsibility for a different financial sector, introduced in early 2011. The three ESAs are the European Securities and Markets Authority (ESMA), the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA).

European Union (EU) Directives

Legislation issued by the EU to its member states requiring them to enact and implement local legislation.

Financial Conduct Authority (FCA)

In the UK regulatory regime, the FCA and the Prudential Regulation Authority (PRA) in the UK replaced the Financial Services Authority (FSA) in 2013. The FCA is responsible for regulating conduct in retail and wholesale markets, and supervising the trading infrastructure

that supports those markets. The PRA provides prudential regulation and supervision of banks, building societies, insurers and major investment.

Future

A futures contract is a form of legally binding arrangement by which parties commit to buying/selling a standard quantity and (if applicable) quality of an asset from/to another party on a specified date in the future, but at a price agreed today. Because the price is agreed at the outset, the seller is protected from a fall in the price of the underlying asset in the intervening time period (and vice versa).

Home State

The term used for the country where a financial services firm conducting cross-border business is based.

Host State

The term used for a country in which a financial services firm is doing business but is not based.

Inside Information

Information relating to a security, or an issuer, which is not publicly known and which would affect the price of the security if it were made public.

Insider Dealing

An offence which may be committed by an insider in possession of unpublished price-sensitive information if they attempt to deal in affected securities, encourage others to deal, or pass the information on.

Integration

The third stage of money laundering when the laundered funds have the appearance of being of legitimate provenance.

Key Risk Indicators (KRIs)

Objective measurement criteria that measure a firm's ongoing risk status.

Know Your Client/Customer (KYC)

The Money Laundering Regulations and the FCA rules require firms to take sufficient steps, before taking on a client, to satisfy themselves as to the identity of that client.

Layering

The second stage of money laundering, in which money or assets are typically passed through a series of transactions to obscure their true origin.

Liquidity Risk

The risk that an institution will not be able to meet its liabilities as they become due because of an inability to liquidate assets or obtain enough funding, or because it cannot easily unwind or offset specific exposures without significantly lowering market prices because of inadequate market depth or market disruptions.

Market Abuse

Offences judged on what a regular user would view as a failure to observe required market standards. The offences include abuse of information, misleading the market and distortion of the market.

Market Maker

A firm which quotes bid and offer prices for a named list of securities in the market. Such a firm is normally under an obligation to make a price in any security for which it is a market maker at all times.

Market Risk

The potential loss of earnings or capital arising from changes in the value of portfolios of financial instruments.

Markets in Financial Instruments Directive (MiFID)

An EU directive which replaced the Investment Services Directive (ISD) on 1 November 2007. It allows firms authorised in one member state to provide/offer financial services to customers in another member

state, subject to some restrictions. The second MiFID Directive (MiFID II) was implemented in 2018.

Misleading Statement

The term used for false, misleading or incomplete information given about an investment, in order to affect or influence its value.

Money Laundering (ML)

The process whereby criminals attempt to conceal the true origins of the proceeds of their criminal activities, and to give them the appearance of legitimacy by introducing them into the mainstream financial system.

Money Laundering Regulations

The regulations under which authorised firms and other businesses are required to comply with certain administrative obligations in order to prevent money laundering. The obligations include record-keeping, identification of clients, appointment of a nominated officer to receive suspicion reports and staff training. Failure to comply may result in a fine and/or imprisonment.

Money Laundering Reporting Officer (MLRO)

A senior employee who is responsible for assessing internal suspicion reports, and if these appear justified, reporting those suspicions to a law enforcement agency.

Multilateral Trading Facilities (MTFs)

A system operated by authorised firms which brings together multiple buyers and sellers of securities, but which is not an exchange.

Nominated Officer

A term for the officer who is required to receive a firm's internal suspicion reports under the Proceeds of Crime Act (POCA) 2002, the Terrorism Act and the Money Laundering Regulations; in practice, this is usually the same individual as the MLRO.

Nominee

The party which, under a legal arrangement, holds assets in its own

name on behalf of the true beneficial owner.

Operational Resilience

The ability to prevent, adapt, respond to, recover and learn from, operational disruptions.

Option

An option gives the holder the right (but not the obligation) to buy or sell a fixed quantity of an underlying asset on, or before, a specified date in the future. There are two basic types of option – puts and calls. The holder of a call option has the right to buy the underlying asset at a given price. The holder of a put option has the right to sell the underlying asset at a given price.

Permissions

Permissions are the specific activities which an authorised firm is permitted to carry on.

Placement

The first stage of money laundering in which money is introduced into the financial system.

Politically Exposed Person (PEP)

An individual who is, or has, been entrusted with a prominent public function, or an individual who is closely related to such a person. May also be referred to as a senior foreign political figure.

Prudential Regulation Authority (PRA) Handbook

The document that contains rules of the PRA in the UK, guidance and other provisions, with which PRA-authorised firms must comply. The

Handbook is divided into a number of separate sourcebooks and manuals covering different subjects.

Quran

The central religious text of Islam and the primary source for jurists. The Book of Divine Revelation that was delivered to humankind by the Prophet Mohammed (PBUH).

Regulated Activities

Activities for which authorisation from a regulator is needed unless it is exempt from the need for authorisation. Regulated activities are often defined in relation both to the activities themselves, and to the investments to which they relate.

Robo-Advice

Digital platforms that provide automated financial planning services with little, or no, human intervention.

Securities and Exchange Commission (SEC)

The US SEC is an independent agency of the US federal government whose main responsibility is to enforce federal securities laws, proposing securities rules, and to regulate the securities industry.

Senior Manager and Certification Regime (SMCR)

The SMCR was introduced to the UK in 2015 with the aim of reducing damage to consumers and to strengthen market integrity. As part of the SMCR, each senior manager must have a statement of responsibilities (SoR), setting out their roles and responsibilities. Senior managers and members of the board can be held directly and personally accountable if they did not take reasonable steps to prevent or stop a breach in regulatory requirements.

Settlement Fail

The non-occurrence of settlement or partial settlement of a securities transaction on the intended settlement date, due to a lack of securities or cash regardless of the underlying cause.

Stabilisation

The activity of supporting the price of a new issue of securities or bonds in order to minimise the volatility that can sometimes arise with new issues.

Strategic Risk

The risk of loss due to a suboptimal strategy being employed and associated with the way the institution is managed. For instance, a

competitor or product strategy may be employed that fails to maximise the return on the investment made.

Stress Testing

A means of testing the accuracy of value at risk (VaR) models against 'extreme' market event scenarios.

Tipping Off

An offence established under various pieces of anti-money laundering and terrorist financing legislation. It involves disclosing the fact that an investigation is, or is likely to be, underway, if that disclosure may imperil any such investigation.

Trustee

A person or organisation who is the legal owner of assets held in trust for someone else. The trustee is responsible for safeguarding the assets, complying with the trust deed and (if the trust is a unit trust) overseeing the activities of the unit trust's manager.

UK Bribery Act 2010

UK law applicable to all commercial organisations, making it an offence to offer or take bribes or negligently prevent bribery. It will be a defence for a firm, if it can demonstrate that it has 'adequate procedures' to prevent such conduct by persons associated with it.

Value at Risk (VaR)

The maximum loss that can occur with a specified confidence over a specified period of days.

Whistleblowing

The term used when an individual raises concerns over potential wrongdoing. In some countries, legislation provides some statutory protections for whistleblowers.



Multiple Choice Questions

The following questions reflect the standard that you will experience in your examination. Please note, however, they are not the actual CISI examination questions.

1. **Who is responsible for setting international standards to combat money laundering and terrorist financing?**
 - A. The Financial Action Task Force (FATF)
 - B. The United Nations Office on Drugs and Crime (UNODC)
 - C. The International Development Association (IDA)
 - D. The International Bank for Reconstruction and Development (IBRD)

2. **How are corporate governance standards usually monitored in financial firms?**
 - A. At an individual level according to individual ethical standards
 - B. Through the compliance function
 - C. Through the board
 - D. Through the use of external vendors

3. Which of the following BEST describes the purpose of a compliance manual?
- A. It provides potential clients with an understanding of which regulations affect them
 - B. It demonstrates that the company knows which regulations are relevant to its work
 - C. It formally documents the standards to be followed by all employees
 - D. It enables the compliance function to define how the business is performed
4. When regulators look at the culture of the firms they regulate, what are they looking for?
- A. Evidence that good behaviour is rewarded with higher bonuses
 - B. Evidence of a compliance culture
 - C. A high level of regulatory awareness
 - D. Underlying values and ethics
5. All of the following are an International Organisation of Securities Commissions (IOSCO) objective of securities regulation EXCEPT:
- A. The protection of investors
 - B. Ensuring that markets are fair, efficient, and transparent
 - C. Ensuring engagement by firms in the development of regulations
 - D. The reduction of systemic risk
6. Which of the following categorises a matrix structure of management?

- A. Each board director defines responsibility between the departments of their own function
 - B. Different offices/locations will adopt different structures in performing equivalent functions
 - C. The non-executive directors (NEDs) are specialised and oversee the work of a specific executive
 - D. Some individuals are accountable to multiple executive managers
7. **If a trader deliberately gives the misleading impression that demand for a particular share is greater than it really is, this type of behaviour is likely to be classed as:**
- A. a conflict of interest
 - B. whistleblowing
 - C. money laundering
 - D. market abuse
8. **Which of the following statements is TRUE regarding a two-tier board?**
- A. Such boards are common within the UK
 - B. The management board appoints the members of the supervisory board
 - C. The supervisory board oversees the work of the management board
 - D. The management board includes three non-executive directors
9. **To whom should an individual working at a financial services firm first report suspicion of money laundering?**
- A. The regulator
 - B. The police
 - C. The nominated officer

- D. The customer
10. **The European Systemic Risk Board (ESRB) is responsible for the:**
- A. supervision of the European Central Bank (ECB)
 - B. creation of a single EU rule book
 - C. oversight of the financial system within the EU
 - D. supervision of the European Banking Authority (EBA)
11. **The Bank for International Settlements (BIS) Principle 5 for enhancing corporate governance places which obligation on the board of the parent company in a group structure?**
- A. Appoint a chief compliance officer at group level, to ensure consistency of interpretation across different group companies
 - B. Implement a conflicts of interest policy that prevents any director serving on the boards of more than two group companies
 - C. Ensure that there are governance policies and mechanisms appropriate to the structure, business and risks of the group
 - D. Ensure that the non-executive directors of the parent company have rights to attend the board meetings of all subsidiary companies
12. **Which of the following BEST describes the difference between principles-based and rules-based approaches to financial regulation?**
- A. A principles-based approach is more prescriptive than a rules-based approach
 - B. A rules-based approach is more prescriptive than a principles-based approach

- C. A principles-based approach is less flexible than a rules-based approach
 - D. A rules-based approach is less flexible than a principles-based approach
13. **What does the Bank for International Settlements (BIS) define as 'the risk of loss arising from processes, people, systems, or external events'?**
- A. Regulatory influence
 - B. Operational risk
 - C. Market risk
 - D. Political risk
14. **For which of the following activities is a firm subject to the Markets in Financial Instruments Directive (MiFID)?**
- A. Providing investment advice without executing any trades
 - B. Performing foreign exchange transactions
 - C. Operating a collective investment scheme (CIS)
 - D. Owning shares listed in a different EU country
15. **Which ONE of the following statements relating to best practice in compliance is TRUE?**
- A. Compliance is the responsibility of specialist compliance staff alone
 - B. Compliance is the sole concern of the board of directors
 - C. Compliance is the sole concern of the senior management team
 - D. Compliance is a concern of everyone in an organisation

16. If a firm has a new products committee, which of the following is considered best practice in terms of the relationship between that committee and the compliance department?
- A. The compliance department should be told of any issues that are relevant to them
 - B. Compliance department staff should be asked to attend meetings when necessary
 - C. Compliance department staff should be represented on the committee
 - D. The committee should report directly to the head of compliance
17. An information barrier is an arrangement made by a firm to:
- A. segregate duties between any controlled functions roles
 - B. help manage conflicts of interest
 - C. ensure bonus allocations between different departments are fair
 - D. create a firewall that stops computer hackers from China
18. Which of the following instances of non-compliance with laws and regulations by an individual should the firm report to the regulator?
- A. Partaking in market abuse
 - B. Regularly failing to pass annual refresher training
 - C. Theft from colleagues
 - D. Failure to pass appropriate external examinations
19. In respect of the Foreign Account Tax Compliance Act (FATCA) under the UK-US intergovernmental agreement, which of the following are UK foreign financial institutions required to do?

- A. Report monthly to the Internal Revenue Service (IRS) on account holders who are US persons or foreign entities
 - B. Report annually to the IRS on account holders who are UK domiciled
 - C. Report to His Majesty's Revenue and Customs (HMRC) on account holders who are US persons or foreign entities
 - D. Report monthly to HMRC on account holders who are UK domiciled
20. **All of the following are applicable risk considerations when looking at uncertainty EXCEPT:**
- A. Potential to occur
 - B. Measurable
 - C. Impact
 - D. Consequences for decision-making
21. **In the last few years, regulators have encouraged firms to adopt which ONE of the following types of culture in order to ensure they embody the values which underlie the whole regulatory structure?**
- A. A pragmatic culture
 - B. A compliance culture
 - C. An ethical culture
 - D. A charitable culture
22. **How often should a money laundering reporting officer (MLRO) or another responsible senior executive provide information to its governing body and senior management on the effectiveness of the anti-money laundering systems and controls?**
- A. Every quarter

- B. Every six months
 - C. At least annually
 - D. Each time an incident occurs
23. **Who does the Bank for International Settlements (BIS) deem responsible for overseeing the effective management of compliance risk?**
- A. The board of directors
 - B. The chief executive officer
 - C. The compliance director
 - D. The risk manager
24. **Which of the following is TRUE in relation to continuing professional development (CPD)?**
- A. The compliance function is not permitted to review CPD records of individuals because they concern personal development
 - B. The individual responsible for compliance oversight must complete 50 hours each year
 - C. Regulation requires that the compliance function approves all internal CPD material developed by the firm
 - D. It can include reading industry update materials as well as attending seminars and conferences
25. **What is the most damaging effect of poor corporate governance in the financial sector?**
- A. Inappropriate bonus payments and rogue trader risk
 - B. Loss of confidence in an institution's ability to properly manage its assets and liabilities
 - C. Promotion and reward of unsuitable managers and directors

- D. Failure of the bank itself, creating job losses and loss of shareholder wealth
26. Which of the following is responsible for setting out the governance structure of an organisation?
- A. Head of Compliance
 - B. Board of Directors
 - C. Senior Management
 - D. SMCR Regime
27. Irrespective of a firm's organisational structure, the compliance structure needs to be:
- A. operating independently
 - B. sparsely resourced
 - C. subject to Basel Committee on Banking Supervision (BCBS) monitoring
 - D. an audit responsibility
28. Which of the following BEST describes the Islamic concept of *Riba*?
- A. Prohibition on giving/receiving interest
 - B. Fairness
 - C. Care for the environment at all times
 - D. Profitability
29. Under the Sarbanes-Oxley Act (SOX), which two officials must ensure that internal controls and procedures can provide accurate financial disclosures?
- A. The compliance officer and the money laundering reporting officer (MLRO)
 - B. The compliance officer and chief financial officer (CFO)

- C. The chief executive officer and the CFO
 - D. The chief operating officer and the CFO
30. Which of the following enables the board to enhance the ability of internal audit to identify problems with risk management systems?
- A. By setting internal examinations for internal audit staff
 - B. By ensuring that the internal audit function reports to, or has access to, the board or the board's audit committee
 - C. By requiring executive managers to respond to internal audit findings within one month of identification
 - D. By requiring internal audit managers to spend three months performing operational tasks every three years
31. Under the Sarbanes-Oxley Act (SOX), what is the maximum punishment for defrauding securities investors?
- A. A fine of up to \$1 million, plus gross business income for three years
 - B. Up to seven years in prison
 - C. Up to 25 years in prison
 - D. There is no limit
32. What action does the Foreign Account Tax Compliance Act (FATCA) require of US taxpayers holding financial assets outside the US?
- A. They should report to the Inland Revenue Service (IRS) where the assets are held
 - B. They should advise the IRS when interest/savings income is received on assets held outside the US

- C. They should sell the assets if/when instructed by the IRS
 - D. FATCA imposes no obligations on the US taxpayer
33. **Which European Supervisory Authority (ESA) has direct supervisory responsibility for credit rating agencies?**
- A. European Banking Authority (EBA)
 - B. European Securities and Markets Authority (ESMA)
 - C. European Banking Committee (EBC)
 - D. European Insurance and Occupational Pensions Authority (EIOPA)
34. **The effect of house price movements on a firm's mortgage business is an example of what type of risk?**
- A. Economic risk
 - B. Political risk
 - C. Technology risk
 - D. Operational risk
35. **One purpose of capital adequacy standards is to:**
- A. prevent a regulated firm from having an overdrawn bank account
 - B. prevent a bank from supporting excessive overdrawn accounts
 - C. ensure market liquidity for trading purposes
 - D. provide time for supervisors to intervene if a firm experiences difficulties
36. **In many countries, if a firm wishes to change the authorised business it can perform, which of the following should it submit?**
- A. Change of designation

- B. Part III submission
 - C. CRD IV notice
 - D. Variation of permission
37. **Which ONE of the following is a key difference between terrorist financing and other money laundering activities?**
- A. Only the layering of funds is required
 - B. Only quite small sums of money are often required to commit terrorist acts
 - C. Terrorist funding rarely involves the transfer of funds between jurisdictions
 - D. Terrorist groups do not tend to have links with other criminal activities
38. **What stipulation is included in the Bank for International Settlements (BIS) Principle 5?**
- A. The compliance function should be independent
 - B. Staff should be vetted prior to hiring
 - C. Continuing professional development (CPD) should be performed and evidenced
 - D. Firms should not retain any benefit arising from regulatory breaches
39. **If your firm is subject to a dawn raid, which of the following best describes the officials you should allow to enter the premises?**
- A. Any member of the regulator's staff, providing that they have proof of identity and you verify it with the regulator concerned
 - B. Any member of the regulator's staff (who will normally be accompanied by a police officer) named in the search warrant
 - C. Any person named in the search warrant

- D. Only police officers
40. Which statement BEST describes the confidentiality surrounding suspicious activity reports (SARs)?
- A. The relevant client should be notified of the SAR
 - B. Confidentiality is subject to the obligations to report a valid SAR
 - C. General staff can be briefed regarding the control failure and resolution steps taken once the SAR has been submitted
 - D. The money laundering reporting officer (MLRO) should advise the company's board about the SAR
41. Which of the following was a primary point of the Basel Committee's 2006 principles for enhancing corporate governance?
- A. Compensation policies should be consistent with the bank's long-term objectives
 - B. Thematic complaints against the bank should be subject to board reporting each quarter
 - C. The finance director should not have responsibility for the internal audit function
 - D. All operational data input should be subject to review for accuracy
42. Which of the following is a stage in a successful money laundering operation?
- A. Segregation
 - B. Differentiation
 - C. Integration
 - D. Aggregation
43. Which of the following is the BEST description of 'layering'?

- A. The process of defining a Chinese wall
 - B. Aggregating a firm's capital adequacy across a range of financial asset groupings
 - C. The process of obtaining regulatory permissions
 - D. Moving money around through a series of transactions to disguise the ultimate owner
44. Which of the following BEST describes a 'Ponzi' scheme?
- A. A loan to a client made on terms favourable to the client rather than the firm
 - B. A fraudulent investment that uses a new investor's money to pay old investors a profit
 - C. A type of scam in which investors are subjected to high-pressure selling tactics
 - D. An investment vehicle featuring a high initial charge (known as a haircut)
45. Which of the following outcomes could arise for a regulated firm exposed to counterparty risk?
- A. The firm may be subject to regulatory penalty
 - B. The firm may need to submit a suspicious activity report (SAR)
 - C. The firm may need to replace its chief financial officer (CFO)
 - D. The firm may suffer financial loss due to default
46. In which circumstances will a firm freeze the funds/assets it holds for a client?
- A. When a suspicious activity report (SAR) is raised regarding the client's account
 - B. When a SAR is reported to a law enforcement agency (LEA) regarding the client's account

- C. When the client is identified as a politically exposed person (PEP)
 - D. When the client is identified as a sanctioned individual
47. Which of the following is a document issued by the Organisation for Economic Co-operation and Development (OECD) that is of relevance to corporate social responsibility (CSR)?
- A. The Model Code of Ethics
 - B. Convention on Combating Bribery
 - C. Embedding Integrity
 - D. Defence against Financial Crime
48. The Bank for International Settlement's (BIS's) definition of 'compliance risk' notes that a firm may suffer as a result of failure to comply with relevant laws, highlighting the risk of legal or regulatory sanctions, material financial loss, and what other consideration?
- A. Loss of reputation
 - B. Loss of senior staff
 - C. Loss of clients through regulatory action
 - D. Loss of opportunity
49. Which of the following documents is most likely to give rise to concerns about misuse of inside information?
- A. A magazine article about recruitment highlighting staffing issues at a company
 - B. Confidential government papers regarding a change to capital gains tax
 - C. A paper listing possible implications of Greece leaving the euro currency

- D. Unpublished draft reports and accounts of a listed company
50. Which of the following does NOT need to be recorded on an insider list?
- A. The name of the person who identified the individual as being an insider
 - B. The identity of each person who has access to inside information
 - C. The reason why the person is on the insider list
 - D. The date on which the insider list was created and updated
51. What can be described as a typical self-regulatory model?
- A. Industry to decide how best to regulate itself, with no government intervention
 - B. Combination of industry rules with government oversight
 - C. Industry regulates itself, but the government decides appropriate qualifications for participants
 - D. Industry takes responsibility for the implementation of government policy
52. Which of the following BEST describes due diligence?
- A. A contractual obligation to provide monitoring reports to a client
 - B. The care a reasonable person should take before entering into an agreement or transaction
 - C. A financial payment to pay for second line of defence functions
 - D. The process by which a principles-based regulator oversees a firm

53. **What actions should a firm take in respect of personal account (PA) dealing?**
- A. Ensure all staff use the firm's client money bank account to effect dealing
 - B. Ensure that all staff are invited to refresher training every 24 months
 - C. Install system-based controls to prevent individuals dealing in their own name
 - D. Ensure any outsourced service provider maintains records of transactions by relevant persons
54. **Which of the following is a feature of a multilateral trading facility (MTF)?**
- A. It must deliver transparency pre-trade, though not post-trade
 - B. Firms use such facilities to execute trades for their clients against their own book or other clients
 - C. They must meet the standards required by the Accounting and Auditing Organization for Islamic Financial Institutions (AAOIF) and the Islamic Financial Services Board (IFSB)
 - D. Prices/charges are public and applied consistently across all members
55. **Which of the following is an effect of the two-tier board structures?**
- A. The chairman needs to accept the views of the executive management
 - B. The firm must appoint three non-executive directors to ensure executive accountability
 - C. There is clear separation between the functions of supervision and management

- D. The finance function is independent of the operational executives
56. **Where is the Committee on Banking Supervision based?**
- A. The Hague
 - B. Brussels
 - C. Basel
 - D. Luxembourg
57. **Why should a firm perform breach analysis?**
- A. It is a monthly regulatory requirement
 - B. The firm must ensure the logging process is working correctly
 - C. The third line of defence will raise a recommendation if the second line of defence has not performed this review
 - D. Such analysis can indicate trends and so help control the business
58. **Which of the following is a partnership between the World Bank Group and United Nations Office on Drugs and Crime (UNODC) to end safe havens for corrupt funds?**
- A. Stolen Asset Recovery Initiative (StAR)
 - B. Politically exposed person (PEP)
 - C. Financial Action Task Force (FATF)
 - D. International Monetary Fund (IMF)
59. **Which of the following would NOT satisfy the definition of a UK politically exposed person (UKPEP)?**
- A. Tony Blair (former UK Prime Minister)
 - B. Piers Corbyn (brother of Jeremy Corbyn MP)

- C. Lady Hale (Deputy President of the UK Supreme Court)
 - D. Air Chief Marshall Sir Stephen Hillier (Chief of the Air Force)
60. **Which of the following is key to managing stakeholder risk?**
- A. Appoint non-executive directors
 - B. Establish a remuneration committee
 - C. Reduce the firm's risk appetite
 - D. Build relationships at senior levels
61. **What is the key objective of corporate governance in banks?**
- A. To ensure that a company is well managed for the benefit of shareholders
 - B. To ensure that employees are able to work in an ethical workplace
 - C. To give clarity to non-executive directors on their roles
 - D. To achieve and maintain the confidence and trust of the public
62. **Which of the following BEST describes an outsourcing relationship?**
- A. Firm A retains the services of Firm B, which assumes regulatory and practical responsibility for completing the tasks
 - B. The outsourcing firm performs all the work
 - C. The outsourcing firm retains regulatory responsibility for those tasks outsourced
 - D. The service provider and outsourcing firm must have equivalent regulatory authorisation

63. Which of the following roles has specific statutory responsibilities?
- A. Group compliance officer
 - B. Money laundering reporting officer (MLRO)
 - C. Head of IT
 - D. All employees of an authorised financial services firm
64. In what way should a risk-based approach to combating money laundering produce better results?
- A. Firms should think about the underlying issues, rather than adopting a 'tick-box' approach to compliance
 - B. If the risk is sufficient, a nominated officer must be appointed
 - C. The risk priority will ensure discussion of money laundering at board meetings
 - D. It ensures that the firm's risk management function collaborates with the money laundering reporting officer (MLRO)
65. Tax avoidance is BEST described as which one of the following?
- A. Falsely claiming to live in another country to receive payments without paying tax
 - B. Use of legally permissible methods to reduce the amount of tax owed
 - C. Intentionally avoiding paying part of all tax liability by illegal means
 - D. Performing a large number of transactions to disguise the origins of an asset

66. Under the 'three lines of defence' model, what is generally viewed as the third line?
- A. Risk management
 - B. Internal audit
 - C. The regulator
 - D. The board
67. Which of the following is NOT an action that an investor could take to protect themselves from becoming a victim of financial crime?
- A. Shred sensitive material, such as financial statements, before disposal
 - B. Keep passwords and personal identification number (PIN) numbers secure
 - C. Carefully read the terms and conditions of a product
 - D. Consider whether the investment sounds too good to be true
68. Industry specialised knowledge is a key element of an effective self-regulatory model because:
- A. the complexity of markets and products increases
 - B. the government must levy fines where firms do not abide by the code
 - C. a standard approach to compliance monitoring activity must be agreed
 - D. International Organization of Securities Commissions (IOSCO) Principle 4 requires firms to demonstrate their engagement in establishing the framework
69. Which of the following is NOT an aspect of the compliance role in the development of new businesses?

- A. Performing a risk assessment
 - B. Determining the scope of regulation
 - C. Signing off from the operating model
 - D. Highlighting material changes to existing relationships
70. **What concept might be described as ‘the level of loss that the firm is willing to accept in its different businesses over a specified time horizon at a given level of confidence’?**
- A. Stress testing
 - B. Return on capital employed
 - C. Profitability coefficient
 - D. Risk appetite
71. **Which of the following describes a key element of a ‘dawn raid’?**
- A. It is performed by regulatory staff in isolation, acting under their statutory powers
 - B. The team can only interview personnel present at the point the raid began
 - C. All persons participating in the raid should be named on a warrant
 - D. IT equipment must not be touched if the data is encrypted
72. **Which of the following is NOT an element of the independence of the compliance function?**
- A. Their responsibilities should not lead to conflicts of interest
 - B. They should have access to information and personnel

- C. Compliance should have a formal status within the firm
 - D. The group compliance officer or head of compliance should not have responsibility for other functions (such as legal, risk management, or finance)
73. **What is the mandate of the United Nations Office on Drugs and Crime (UNODC)?**
- A. It sets principles for self-regulatory models
 - B. It publishes lists of politically exposed persons (PEPs)
 - C. It assists member states in the struggle against illicit drugs, crime, and terrorism
 - D. It supports corporate governance in developing countries
74. **Which of the following is a predicate offence in respect of money laundering?**
- A. Depositing stolen money in a bank account
 - B. Performing multiple investment transactions to disguise the audit trail of stolen goods
 - C. Bribing a public official
 - D. Tipping off a money launderer
75. **The Committee of European Banking Supervisors (CEBS) defines what form of risk as 'the current or prospective risk to earnings and capital arising from changes in the business environment and from adverse business decisions, improper implementation of decisions or lack of responsiveness to changes in the business environment'?**
- A. Economic risk
 - B. Political risk
 - C. Company risk
 - D. Strategic risk

76. Which of the following is an EU policy goal supported by the Markets in Financial Instruments Directive (MiFID)?
- A. The free movement of people
 - B. Strengthening the euro
 - C. Extending the range of services that can be 'passported'
 - D. Ensuring that asset managers are subject to appropriate supervision
77. Which of the following BEST describes the three stages used to create a model to drive a compliance monitoring programme?
- A. Research, review, repeat
 - B. Information gathering, scoring, weighting
 - C. Placement, layering, integration
 - D. Accuracy, completeness, existence
78. Which of the following is NOT an example of money laundering?
- A. Handling the proceeds of crime
 - B. Handling stolen goods
 - C. Assisting a known criminal to buy a house
 - D. A client of the firm requesting the proceeds of a share sale in cash
79. Which of the following is an example of tax evasion?
- A. Falsely claiming to live outside the UK in order to receive payments without paying tax
 - B. Investing using an individual savings account (ISA)
 - C. Investing using an offshore trust
 - D. Performing a large number of transactions to disguise the origins of an asset

80. Which of the following is an element of compliance independence?
- A. The internal audit function should report to the chief finance officer
 - B. The head of compliance has overall responsibility for coordinating the management of the firm's compliance risk
 - C. The compliance department should only have restricted access to operational material
 - D. The compliance director's budget should increase according to pre-tax profits
81. Which of the following is NOT said to have extraterritorial reach?
- A. UK Bribery Act
 - B. Sarbanes-Oxley Act
 - C. Foreign Corrupt Practices Act
 - D. Independent Commission on Banking
82. Robo-advice is best described as a digital platform that provides:
- A. a tool for financial advisors when assessing risk appetite
 - B. automated financial advice with limited human intervention
 - C. call centre activities for wealth management advice
 - D. tailored financial advice alongside the financial advisor
83. Why might an 'orphan structure' offshore trust be appealing to criminals?
- A. No checks are required when depositing money

- B. Offshore jurisdictions have no suspicious activity reporting controls
 - C. It enables mortgage fraud through misrepresentation
 - D. The trust's beneficiary is not identified
84. **What variable is commonly combined with 'likelihood' to determine risk for business continuity planning (BCP) purposes?**
- A. Impact
 - B. Distance
 - C. Cost
 - D. Probability
85. **In what areas of the firm should the compliance function be able to exercise oversight?**
- A. All departments where compliance risk exists
 - B. Operational processing areas
 - C. All areas aside from corporate finance (which is subject to financial audit)
 - D. Corporate services departments, such as legal and human resources
86. **In what way does a rules-based approach to regulation put strain on the regulator?**
- A. It must hold an increased range of public hearings
 - B. It must find an increased number of firms to penalise for poor behaviour
 - C. The rules must always provide a reliable distinction between right and wrong
 - D. More firms must receive individual guidance

87. **What mechanism should deliver an independent review of the operational work performed by the firm?**
- A. Capital adequacy calculation
 - B. Regulatory returns
 - C. Compliance monitoring programme
 - D. Money laundering reporting officer (MLRO) report
88. **In respect of the firm's systems and controls for financial crime prevention, which of the following is a responsibility of the firm's directors and senior management?**
- A. Internal audit must review the controls every two years
 - B. Ownership of financial crime prevention must be allocated to the chief risk officer or chief compliance officer
 - C. To understand their personal liability if legal obligations are not met
 - D. Publish the money laundering reporting officer (MLRO) report for review by all shareholders
89. **The misappropriation of assets is a typical objective of financial misstatement. Which of the following is an example of the misappropriation of assets?**
- A. Pressure to meet market expectations, minimise tax or inflate earnings to secure bank finance
 - B. Embezzling receipts through collections accounts
 - C. Effecting payments to fictitious vendors
 - D. Opening a custody account in a false name
90. **Which ONE of the following statements BEST describes principles-based regulation?**

- A. It is based on very detailed statements of what firms and individuals should do in order to comply
- B. Firms and individuals decide how, and to what extent, they must meet the principles
- C. Regulation based on principles was discredited after the financial crisis of 2008
- D. In the event of conflict, rules override principles

91. What ensures an effective compliance function?

- A. The compliance function must be able to accommodate the needs of both management and 'front desk'
- B. Compliance must be able to demonstrate that it has systems and controls in place to accommodate the regulators needs
- C. Compliance must be able to maintain up-to-date records for the board and the regulators
- D. Compliance must be able to advise and assist the relevant persons responsible for carrying out regulated activities to comply with the firm's obligations

92. In the context of money laundering, layering is BEST described as:

- A. introducing money into the financial system
- B. moving money around the financial system
- C. legitimately maintaining the funds in the financial system
- D. taking the funds out of the financial system

93. What is the purpose of setting standards and principles for firms and key individuals?

- A. To provide non-binding guidance

- B. To provide binding guidance
 - C. To ensure that firms abide by both standards and regulations
 - D. To ensure that the spirit as well as the letter of the regulations are met
94. **The maximum penalty for a breach of the General Data Protection Regulation (GDPR) is the higher of:**
- A. up to 2% of annual turnover or €50 million
 - B. up to 4% of annual turnover or €20 million
 - C. up to 10% of annual turnover or €5 million
 - D. up to 12% of annual turnover or €15 million
95. **Under the Second Payment Services Directive (PSD2), a payment service is defined as a service enabling:**
- A. cash to be deposited or withdrawn
 - B. transfers to be made
 - C. paper transactions
 - D. Society for Worldwide Interbank Financial Telecommunication (SWIFT) transactions
96. **The Office of Foreign Asset Control is part of the:**
- A. UN Security Council
 - B. European Central Bank (ECB)
 - C. US department of Treasury
 - D. Financial Action Task Force (FATF)
97. **Cyber crime is BEST defined as a crime in which:**
- A. a computer is the object of the crime
 - B. the crime is committed using the internet
 - C. the government is restricting internet access
 - D. a call centre defrauds the customers

98. **The Taskforce on Climate-Related Financial Disclosures has identified recommendations along which of the following four themes?**
- A. Governance, strategy, risk management, metrics and targets
 - B. Compliance, operational risk, statistics, profitability
 - C. Governance, operational risk, compliance, climate returns
 - D. Board of directors, compliance, governance, climate effort
99. **Under the Central Settlement Depository Regulations (CSDR), settlement of a transaction needs to be placed on which of the following dates?**
- A. Buy-in date
 - B. Actual settlement date
 - C. Intended settlement date
 - D. Extension date
100. **Which of the following is an area, as defined by the Sustainable Finance Disclosure Regulations (SFDR), where firms need to provide disclosures?**
- A. Post contractual product sheets
 - B. Principal adverse impact
 - C. Green finance
 - D. Corporate Social Responsibility (CSR)

Answers

1. **A Chapter 3, Section 1.3.4**

The Financial Action Task Force (FATF) sets standards to combat money laundering and terrorist financing.

2. B Chapter 5, Section 1.3

The firm should maintain sound control functions, including an effective compliance function that, among other things, routinely monitors compliance with laws, corporate governance rules, regulations, codes and policies to which the bank is subject to; and ensures that deviations are reported to an appropriate level of management and, in case of material deviations, to the board.

3. C Chapter 2, Section 1.3.1

The purpose of the compliance manual is to formally document the standards to be followed by all employees.

4. D Chapter 4, Section 1

Regulators are looking for an ethical culture that embodies the values that underlie the whole regulatory structure, giving proper protection to consumers of financial services. This goes deeper than regulatory awareness, which is taken as a given, or a compliance culture which risks a 'tick-box' mentality. Bonuses may be reduced for poor behaviour but are ultimately revenue-related.

5. C Chapter 1, Section 1.4 and 2.2.3

The three International Organisation of Securities Commissions (IOSCO) objectives of securities regulation are preserve market integrity, preserve financial integrity, and protect investors.

6. D Chapter 5, Section 1.5.1

The principle of matrix management is that an individual may serve two or three managers rather than just one.

7. D Chapter 4, Section 2

Any behaviour that is likely to distort the market is classed as market abuse.

8. C Chapter 5, Section 1.4

The management board is accountable to the supervisory board, elected by shareholders.

9. C Chapter 3, Section 3.4

A nominated officer in practice is usually the money laundering reporting officer (MLRO). The MLRO is responsible for reviewing and reporting cases onwards.

10. C Chapter 1, Section 2.2.4

The European Systemic Risk Board (ESRB) was established on 1 January 2011 with responsibility for the macro prudential oversight of the financial systems within the EU.

11. C Chapter 5, Section 1.9

Principle 5 states: 'In a group structure, the board of the parent company has the overall responsibility for adequate corporate governance across the group and ensuring that there are governance policies and mechanisms appropriate to the structure, business and risks of the group and its entities.'

12. B Chapter 1, Section 1.3

A principles-based approach to financial regulation is one where principles are set at a high level and it is left to the firm or individual to decide how, and to what extent, they must meet these principles. In contrast, a rules-based approach is much more prescriptive, often provides very detailed rules and is much less flexible.

13. B Chapter 5, Section 2.3.2

This is the Bank for International Settlements' (BISs') definition of operational risk.

14. A Chapter 1, Section 1.5.2

Providing investment advice is the only option here that is a Markets in Financial Instruments Directive (MiFID) activity. While deals involving collective investment scheme units are subject to MiFID, the operators of such schemes are exempt.

15. D Chapter 2, Section 1.1.1

It is vital that compliance is a concern of everyone in an organisation and should be viewed as an integral part of the firm's everyday activities. Compliance is not the responsibility of specialist compliance staff alone.

16. C Chapter 2, Section 1.4.1

The compliance function proactively identifies, documents and assesses the compliance risks associated with the firm's business activities, including the development of new products and business practices, the proposed establishment of new types of business or customer relationships, or material changes in the nature of such relationships. If the firm has, for example, a new products committee, operations committee or risk management committee, compliance function staff should be represented on such committees.

17. B Chapter 4, Section 2.4.1

There is no requirement for a firm to have Information Barriers in place; they are just one example of how to manage conflicts of interest.

18. A Chapter 2, Section 2.1.5

It is possible that an individual may be subject to external regulatory sanction, particularly if the breach amounted to serious market abuse.

19. C Chapter 1, Section 1.5.3

Under the Foreign Account Tax Compliance Act (FATCA) and the US-UK intergovernmental agreement, a UK foreign financial institution

must report to His Majesty's Revenue and Customs (HMRC) on its account holders who are US persons or foreign entities with substantial US ownership.

20. B Chapter 5, Section 2.1

Uncertain matters are not measurable; where we can apply data and probability theory to analyse potential outcomes we talk of 'risk'.

21. C Chapter 4, Section 1.1

Regulators are increasingly taking the view that they have an obligation to consider and make judgments in relation to the ethics and culture of the firms they regulate; having a compliance culture is simply not enough. What is needed is an ethical culture in the firm which embodies the values which underlie the whole regulatory structure.

22. C Chapter 3, Section 2.5

To prove corporate governance, a firm should ensure that any review includes the effectiveness of the anti-money laundering (AML) systems and controls and is conducted at least annually.

23. A Chapter 5, Section 3

The board of directors is responsible for overseeing the management of the firm's compliance risk.

24. D Chapter 2, Section 1.6

Only D is true. Continuing professional development (CPD) may include appropriate professional examinations, access to regulatory updates and bulletins and industry updates.

25. B Chapter 5, Section 1.1

The single most widespread and damaging effect of poor corporate governance in the financial sector is loss of confidence by the public in an institution and in the financial sector as a whole. The damage

is inflicted contagiously onto well-run institutions too. Inappropriate bonus payments, rogue trader risk, promotion of unsuitable or incompetent managers and bank failure are symptoms of poor corporate governance – these symptoms can act as a bellwether or an early warning that something is amiss in an institution.

26. B Chapter 5, Section 1.2

It is the responsibility of the board of directors to set out the governance structure for the organisation, to make sure it is implemented as intended, and to provide effective supervision over senior management. Members of the board need to act with honesty and integrity and need to be independent. Members of the board of directors and senior managers of financial institutions performing key roles need to be approved by the regulator to execute their function.

27. A Chapter 2, Section 1.1.1

Irrespective of the organisational structure, an effective compliance function should operate independently and be sufficiently resourced.

28. A Chapter 1, Section 1.4.2

is a prohibition on the giving and earning of interest.

29. C Chapter 1, Section 1.5.2

The chief executive officer and chief finance officer are responsible for ensuring that internal controls and procedures can provide accurate financial disclosures.

30. B Chapter 5, Section 1.6

Promoting the independence of the internal auditor, for example by ensuring that the internal audit function reports to, or has direct access to, the board or the board's audit committee.

31. C Chapter 1, Section 1.5.2

The maximum punishment for defrauding securities investors is up to 25 years in prison.

32. A Chapter 1, Section 1.5.3

Under the Foreign Account Tax Compliance Act (FATCA), US taxpayers holding financial assets outside the US will report those assets to the Inland Revenue Service (IRS).

33. B Chapter 1, Section 2.2.4

The European Securities and Markets Authority (ESMA) has direct supervisory responsibility for credit rating agencies.

34. A Chapter 5, Section 2.2.1

This risk arises in the wider economy, rather than within the firm's activity or political sphere.

35. D Chapter 1, Section 2.7.2

Capital standards are designed to provide supervisory authorities with time to intervene to accomplish the objective of orderly wind-downs.

36. D Chapter 2, Section 1.8.3

The process to amend authorisation is known in many countries as a 'variation of permission'.

37. B Chapter 3, Section 1.1

One of the major differences between terrorist financing and other money laundering activities is that, often, only quite small sums of money are required to commit terrorist acts. Terrorist organisations can, however, require significant funding and will employ modern techniques to manage and transfer the funds between jurisdictions, hence the similarities with money laundering. Terrorist groups also tend to have links with other criminal activities.

38. A Chapter 2, Section 2.1.3

The Banking Committee on Banking Supervision (BCBS) states in Principle 5 that the compliance function should be independent.

39. **C Chapter 2, Section 3.1.5**

Regulatory staff will normally be accompanied by a police officer and have a warrant (in which they are named) to search the premises. This includes any technical staff named on the warrant. The investigators are entitled to use reasonable force to enter the premises, but they are obliged to show the warrant.

40. **D Chapter 2, Section 3.1.7**

Staff may refer concerns about specific transactions or other activities to their line manager to obtain advice or guidance. However, the suspicion should still be logged and referred to the money laundering reporting officer (MLRO).

41. **A Chapter 5, Section 1.9**

A primary point of the 2006 principles was that compensation policies should be consistent with the bank's long-term objectives.

42. **C Chapter 3, Section 1.2**

The three stages of a successful money laundering operation are placement, layering, and integration.

43. **D Chapter 3, Section 1.2**

Layering involves moving money around in order to make it difficult for the authorities to link the placed funds with the ultimate beneficiary of the money.

44. **B Chapter 3, Section 1.5**

The term 'Ponzi scheme' is used to describe a financial services product that claims a level of investment return that is not supported by the investment activity undertaken. The shortfall between the returns generated and those claimed is made up by using the money of new investors.

45. D Chapter 3, Section 2.1

The potential that a firm may be unable to deliver on its promises to another is termed 'counterparty risk' or 'default risk'.

46. D Chapter 3, Section 3.4

The firm must freeze funds if a customer is identified as being on the sanctions list on the government website of suspected terrorists or sanctioned individuals and entities.

47. B Chapter 4, Section 5.2

The Organisation for Economic Co-operation and Development (OECD) has issued a number of documents, including the Convention on Combating Bribery.

48. A Chapter 5, Section 3

Compliance risk is defined by the Bank for International Settlements (BIS) as 'the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a firm may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities'.

49. D Chapter 4, Section 2.2

Such a document contains specific and price-sensitive information and has not yet been made public.

50. A Chapter 4, Section 2.4.2

Every insider list must contain: the identity of each person having access to inside information; the reason why such person is on the insider list; and the date on which the insider list was created and updated.

51. B Chapter 1, Section 1.4

In the financial services sector, self-regulation is typically a unique combination of private interests with government oversight, which has delivered an effective and efficient form of regulation for a complex and dynamic environment.

52. **B** **Chapter 5, Section 1.7**

Generally, due diligence refers to the care a reasonable person should take before entering into an agreement or a transaction with another party.

53. **D** **Chapter 4, Section 2.4.3**

When outsourcing takes place, arrangements must be such that the outsource service provider maintains a record of personal transactions undertaken by relevant persons and provides it to the firm promptly on request.

54. **D** **Chapter 1, Section 1.6.3**

For a multilateral trading facility (MTF), prices/charges are public and applied consistently across all members.

55. **C** **Chapter 5, Section 1.4**

Dual boards consist of a supervisory board and an executive board, where there is clear separation between the functions of supervision and management.

56. **C** **Chapter 2, Section 1.1.1**

It is the Basel Committee on Banking Supervision (BCBS).

57. **D** **Chapter 2, Section 3.1.6**

Analysis of breaches will be helpful to indicate trends and provide managers and senior managers with information to help control the business.

58. **A** **Chapter 3, Section 1.3.3**

The Stolen Asset Recovery Initiative (StAR) is a partnership between the World Bank Group and the United Nations Office on Drugs and Crime (UNODC) that supports international efforts to end safe havens for corrupt funds.

59. **A** **Chapter 3, Section 2.7.3**

A politically exposed person (PEP) is defined as ‘an individual who has, at any time in the preceding year, been entrusted with prominent public functions and an immediate family member or known close associate of such a person’. This includes Members of Parliament, members of Supreme Courts, and high-ranking officers in the armed forces.

60. **D** **Chapter 5, Section 2.2.6**

The key to managing stakeholder risk is to:

- build relationships at senior levels
- understand their agenda and how it may differ from the firm’s own agenda, and
- manage expectations with any new developments.

61. **D** **Chapter 5, Section 1.1**

Effective corporate governance practices are essential to achieving and maintaining public trust and confidence in the banking system, which are critical to the proper functioning of the financial sector and economy as a whole.

62. **C** **Chapter 2, Section 1.8.1**

The outsourcing firm retains regulatory responsibility for the tasks outsourced.

63. **B** **Chapter 2, Section 1.4**

The compliance function may contain specific statutory responsibilities – such as an officer fulfilling the role of money laundering reporting officer (MLRO).

64. A Chapter 1, Section 1.3

A rules-based approach requires strict adherence to precise rules with little allowance for interpretation. It is typically inflexible and may result in a tick-box exercise.

65. B Chapter 3, Section 1.7

Tax avoidance is the use of legally permissible methods to reduce the amount of tax owed. This is generally achieved by claiming permissible deductions, credits and allowances.

66. B Chapter 2, Section 2.1.3

The third line of defence is generally delivered by the firm's internal audit function.

67. C Chapter 3, Section 2.6

Investors can do a number of things to reduce the likelihood of becoming a victim of financial crime: use a shredder to shred statements before disposal; keep passwords and PIN numbers secure; and remember that if an investment sounds too good to be true, it probably is.

68. A Chapter 1, Section 1.4.1

Industry-specific knowledge is important given the increasing complexity of markets and products.

69. C Chapter 2, Section 2.1.6

The five aspects of compliance's role in the development of new business are:

- due diligence
- risk assessment
- scope of regulation

- highlighting material changes in the nature of existing relationships, and
- assessing and reporting potential reputational risks.

70. D Chapter 5, Section 2.5.3

This is a description of risk appetite, also expressed as the level of expected loss that the firm will not (or cannot) mitigate.

71. C Chapter 2, Section 3.1.5

Regulatory staff will normally be accompanied by a police officer and have a warrant (in which they are named) to search the premises.

72. D Chapter 2, Section 2.1.3

The concept of independence involves four related elements:

- Compliance should have a formal status within the firm.
- There should be a group compliance officer or head of compliance.
- Their responsibilities within the firm should not lead to conflicts of interest.
- They should have access to information and personnel.

73. C Chapter 3, Section 1.3.1

The United Nations Office on Drugs and Crime (UNODC) is mandated to assist member states in their struggle against illicit drugs, crime and terrorism.

74. C Chapter 3, Section 1.4

A predicate offence is the underlying criminal offence that gives rise to criminal proceeds, which is then the subject of a money laundering charge.

75. D Chapter 5, Section 2.3.1

This is the Committee of European Banking Supervisors' (CEBS') definition of strategic risk.

76. **C** **Chapter 1, Section 1.5.2**

The Markets in Financial Instruments Directive (MiFID) supports two key policy goals of the EU, one of which is extending the range of investment services for which a firm can obtain an EU passport.

77. **B** **Chapter 2, Section 1.5**

There are essentially three key stages in establishing a programme: information gathering, scoring, and weighting.

78. **D** **Chapter 3, Section 1.1**

Requesting share proceeds in cash is unusual, and may even be suspicious, but does not constitute money laundering. A money launderer is more likely to want the proceeds of a sale to remain within the banking system as 'clean money'. Handling proceeds of a crime is clearly money laundering. Handling stolen goods is money laundering as this is also the proceeds of a crime. Assisting a known criminal to buy a house is likely to be with laundered money unless the criminal can prove beyond doubt that the money was obtained legitimately. Ethically, you would not even consider this account.

79. **A** **Chapter 3, Section 1.7**

Tax evasion is the illegal act of not paying taxes due – such as by claiming tax reliefs to which the individual was not entitled.

80. **B** **Chapter 5, Section 1.5.3**

An element of independence is that there should be a group compliance officer or head of compliance with overall responsibility for coordinating the management of the firm's compliance risk.

81. **D** **Chapter 1, Section 1.5**

The UK Bribery Act, the Sarbanes-Oxley Act, and the Foreign Corrupt Practices Act are examples of legislation that have an effect beyond

national borders.

82. B Chapter 1, Section 1.8.2

Robo-advice or robo-advisors are digital platforms that provide automated financial planning services with little, or no, human intervention. A robo-advisor collects information from customers concerning their financial situation, future goals, and risk appetite by means of online surveys. This information is then used as input into an algorithm to provide investment advice.

83. D Chapter 3, Section 1.5

The use of orphan models might be used to disguise the chain of ownership for certain assets, and the identity of the beneficiaries is not stated.

84. A Chapter 5, Section 2.5.1

A simple risk assessment is derived by multiplying the likelihood rating scores with the impact rating scores.

85. A Chapter 2, Section 1.8.5

The compliance function should be able to carry out its responsibilities on its own initiative in all departments of the firm in which compliance risk exists.

86. C Chapter 1, Section 1.3

A rules-based approach must be sufficiently detailed to always provide a reliable distinction between right and wrong.

87. C Chapter 2, Section 1.5

The purpose of the compliance monitoring programme is to provide an independent review of the operational work performed by the firm.

88. C Chapter 3, Section 2.3

The directors and senior management of an authorised financial firm are expected to understand the potential personal liability if legal obligations are not met.

89. **B** **Chapter 3, Section 1.6**

Embezzling receipts through collections accounts is an example of misappropriation of assets.

90. **B** **Chapter 1, Section 1.3**

The success of a principles-based approach will depend upon firms and individuals making the right choices and doing the right thing because that is what they ought to do. Having strong ethical standards, often set by professional bodies like the CISI, plays a key role.

91. **D** **Chapter 2, Section 1.1**

An effective compliance function needs to be independent of both the front desk and management. At the same time, a compliance culture must be embedded throughout the firm itself and not simply a departmental function. Maintenance of records forms part of the compliance duties, but does not necessarily show that the function is effective.

92. **B** **Chapter 3, Section 1.2**

Layering involves moving money around in order to make it difficult for the authorities to link the placed funds with the ultimate beneficiary of the money. This might involve buying and selling foreign currencies, shares or bonds in rapid succession, investing in collective investment schemes or insurance-based investment products, or moving the money from one country to another.

93. **D** **Chapter 4, Section 1.2**

By setting such standards and principles for firms and key individuals, the regulator aims to ensure that the culture and

operation of a firm meet the spirit, as well as the letter, of the regulations.

94. B Chapter 1, Section 1.5.1

Under the General Data Protection Regulation (GDPR), organisations in breach of GDPR can be fined up to 4% of annual global turnover or €20 million (whichever is greater).

95. A Chapter 1, Section 1.5.2

Payment services are defined as 'services enabling cash to be deposited in or withdrawn from, for example, a bank account, as well as all the operations required to operate the account. This can include transfers of funds, direct debits, credit transfers and card payments. Paper transactions are not covered by the directive'.

96. C Chapter 3, Section 2.7.2

The Office of Foreign Asset Control (OFAC) is part of the US Department of the Treasury and acts under presidential national emergency powers, as well as the authority granted to it by specific legislation.

97. A Chapter 5, Section 3.2.1

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing or spamming) or is used as a tool to commit an offence (child pornography or hate crimes).

98. A Chapter 4, Section 5.1

The Taskforce on Climate-Related Financial Disclosures (TCFD) has identified recommendations around governance, strategy, risk management, metrics and targets.

99. C Chapter 1, Section 1.5.2

Under CSDR, all transactions should be settled on the intended settlement date (at the latest two business days after the trade date).

100. **B** **Chapter 4, Section 5.1**

The Sustainable Finance Disclosure Regulations (SFDR) were developed in 2020 by the three European Supervisory Authorities (ESAs) defining proposals for the content, methodologies and presentation of sustainable disclosures in the following areas:

1. Principal adverse impact disclosures.
2. Pre-contractual product disclosures.
3. Website product disclosures.
4. Product periodic disclosures.

Syllabus Learning Map

Syllabus Unit/ Element		Chapter/ Section
---------------------------	--	---------------------

Element 1	Introduction	Chapter 1
1.1	Models of regulation On completion, the candidate should:	
1.1.1	Understand the objectives and benefits of regulation	1.1
1.1.2	Know the interaction between law and regulation	1.2
1.1.3	Understand the main differences between rule-based and principles-based approaches to financial regulation	1.3
1.1.4	Understand models of self-regulation	1.4
1.1.5	Understand the regulation of faith- and ethical-based finance and the	1.4

	attendant regulatory implications	
1.1.6	Understand the purpose of the following: • Data Protection, eg, GDPR • Tax Reporting, eg, CRS, FATCA • Market Integrity, eg, MiFID II, MiFIR, MAR, EMIR, PSD2, Sarbanes Oxley Act (2002), CSDR • Financial Crime, eg, UK Bribery Act (2010), FCPA, AMLD	1.5
1.1.7	Understand how regulation operates in an exchange-traded environment	1.6
1.1.8	Understand the key benefits of regulated market structures: • trading venues (exchanges, multilateral trading facilities and organised trading facilities) • systematic internalisers	1.6
1.1.9	Understand how regulation applies to OTC derivatives transactions	1.7
1.1.10	Understand how regulators approach FinTech products • distributed ledger technology (DLT) and digital assets • robo-advice • artificial intelligence and big data	1.8

	regulators' expectations on the compliance function regarding FinTech products	
1.2	The International Approach to Regulation On completion, the candidate should:	
1.2.1	Know the jurisdiction of different types of regulators	2.1
1.2.2	Understand the role of International regulatory organisations: - Bank for International Settlements (BIS) - Financial Stability Board (FSB) - The International Organization of Securities Commissions (IOSCO) - European regulatory bodies - The European System of Financial Supervision (ESFS) - European Supervisory Authorities (ESAs) - The European Systemic Risk Board (ESRB) - Securities and Exchange Commission (SEC) - International Sustainability Standards Board (ISSB)	2.2

1.2.3	Know the role that professional bodies play in relation to regulatory requirements	2.2
1.2.4	Understand how international regulatory organisations aid the implementation of regulation in developing countries	2.2
1.2.5	Know the three objectives of securities regulation as defined by IOSCO	2.2
1.2.6	Understand how regulators implement their regulatory objectives	2.3
1.2.7	Understand different regulatory approaches to supervision • risk-based • rules-based • thematic • relationship-based • principles-based	2.3
1.2.8	Know IOSCO's Principles 1 to 8 relating to the Regulator	2.4
1.2.9	Know regulators' enforcement powers	2.5
1.2.10	Understand what types of activities and investment products are generally required to be regulated	2.6
1.2.11	Understand the requirements regulation places on firms:	2.7

	• Minimum entry standards • Initial and ongoing capital and other prudential requirements • Requirement to establish an internal compliance function • Conduct of business	
1.2.12	Understand how regulators facilitate and regulate cross-border business • specific legislation • memoranda of understanding between individual regulators • regulatory colleges • recognition of third countries	2.8
1.2.13	Understand what regulations apply to a firm with international branches and subsidiaries: • contractual agreements between regulators • home/host	2.8
1.2.14	Understand the challenge of conducting business whilst meeting the regulatory expectations and approach of multiple regulatory bodies • international • domestic	2.8

Syllabus Unit/ Element		Chapter/ Section
---------------------------	--	---------------------

Element 2	The Compliance Function	Chapter 2
2.1	International Best Practice On completion, the candidate should:	
2.1.1	Understand the fundamental systems and controls a firm should implement in order to conduct its business in line with international regulatory standards	1.1
2.1.2	Understand BIS Principle 6 and the requirement for adequate resources	1.2
2.1.3	Understand the practical applications of a formalised document of compliance policies and procedures: compliance manual	1.3
2.1.4	Understand how an effective compliance function can add value to a business	1.4
2.1.5	Know how to produce and implement an effective compliance programme	1.4

2.1.6	Understand how regulatory requirements should be integrated into operating systems, policies and procedures	1.6
2.1.7	Know the difference between regulations and internal policies and procedures	1.7
2.1.8	Understand the potential regulatory implications of business strategies: • outsourcing and oversight • capital requirements • variation of permissions • control framework	1.8
2.1.9	Know how to prepare an effective compliance report for management	1.8.5
2.1.10	Know what basic information compliance officers should have access to	1.8.5
2.2	The Role of the Compliance Function within a Firm On completion, the candidate should:	
2.2.1	Understand the responsibilities and accountabilities of management and staff for compliance with regulations	2.1

2.2.2	Understand how to monitor whether a business is in compliance with regulations and internal policies and procedures	2.1.1
2.2.3	Understand the risks associated with non-compliance for firms and the financial services industry	2.1.2
2.2.4	Understand BIS Principle 5 relating to the independence of the compliance function and senior management accountability	2.1.3
2.2.5	Understand the relationship between compliance and other departments including the 'three lines of defence'	2.1.3
2.2.6	Understand the role compliance has in training and maintaining competence and awareness: • educating staff on compliance issues • acting as a contact point for compliance queries from staff members • providing written guidance to staff	2.1.4
2.2.7	Understand how to monitor an individual's compliance with regulations and internal policies and procedures	2.1.5

2.2.8	Understand the range of potential outcomes to remedy non-compliance by an individual within a firm • training and development activities • internal disciplinary measures • external regulatory sanction • legal avenues	2.1.5
2.2.9	Understand the role compliance plays in new business development: • due diligence • risk assessment • scope of regulation and approval • highlighting material changes in the nature of existing relationships • assessing and reporting potential reputational risks	2.1.6
2.2.10	Understand the purpose of a compliance monitoring programme: • risk-based • reporting • planned	1.5

2.2.11	Understand the key considerations in developing a compliance monitoring programme	1.5
2.2.12	Understand how to conduct an effective compliance monitoring programme: • working papers meeting with senior management • management responses • risk mitigation plans	1.5
2.3	Managing Regulatory Relationships On completion, the candidate should:	
2.3.1	Understand the relationship between the firm and regulator	3.1
2.3.2	Understand how an effective regulatory relationship can be of strategic importance to a firm: • advocating opinion • involvement in consultation • drafting regulatory responses • making representations and applications • obtaining effective guidance	3.1
2.3.3	Understand what to do if your firm is the subject of a regulatory or law	3.1.5

	enforcement visit: • scheduled • unscheduled ('dawn raid')	
2.3.4	Understand what to do if a regulatory breach occurs	3.1.6
2.3.5	Know what types of information must be disseminated to whom in the event of a regulatory breach	3.1.6
2.3.6	Know what information may be disseminated and what should remain confidential if financial crime is suspected or detected	3.1.7
2.3.7	Know what types of information should remain confidential in the normal course of business	3.1.7

"ClimateGreen financeCorporate social responsibilities

Syllabus Unit/ Element		Chapter/ Section
---------------------------	--	---------------------

Element 3	Managing the Risk of Financial Crime	Chapter 3
-----------	---	-----------

3.1	Money Laundering, Terrorist Financing and the Standards Required of Firms On completion, the candidate should:	
3.1.1	Understand the concepts of money laundering and terrorist financing	1.1
3.1.2	Know the stages of the money laundering process: • placement • layering • integration	1.2
3.1.3	Know the role of international agencies in combating money laundering and the financing of terrorism: • United Nations Office on Drugs and Crime (UNODC) • International Monetary Fund (IMF) • World Bank	1.3
3.1.4	Know the role of the Financial Action Task Force (FATF) in combating money laundering and terrorist financing: • jurisdictions with strategic deficiencies	1.3

	the challenge of jurisdictional differences	
3.1.5	Understand the role of predicate offences in financial crime: - fraud - embezzlement - bribery - corruption	1.4
3.1.6	Understand how financial services firms may be utilised for financial crime: - Ponzi schemes - boiler rooms - money laundering - offshore trusts - beneficial ownership - cyber crime	1.5
3.1.7	Understand how a firm or its representatives may collude in the propagation of financial crime: - misstatement of financial circumstances - corporate fraud	1.6
3.1.8	Know the concepts of facilitation of tax evasion and tax avoidance	1.7

3.1.9	Know the concepts of dual criminality, extradition and mutual legal assistance	1.8
3.2	Practical Implications On completion, the candidate should:	
3.2.1	Understand how external financial crime issues may impact on a firm: • reputational • systemically • counterparty risk • unreliable market valuations	2
3.2.2	Understand how financial crime may directly impact a firm: • theft of data • theft of assets	2
3.2.3	Understand the responsibilities of directors and senior management in relation to anti-money laundering (AML), combating financial crime (CFC) and anti-corruption (AC) initiatives	2.3
3.2.4	Understand the role of the Money Laundering Reporting Officer (or equivalent) in relation to financial crime	2.5
3.2.5	Understand the implications of using a risk-based approach to	2.4

	identifying money laundering	
3.2.6	Know the measures firms can adopt to inhibit the likelihood of financial crime	2.5
3.2.7	Know the measures individuals can adopt to inhibit the likelihood of financial crime	2.6
3.2.8	Understand the rationale behind sanctions screening	2.7
3.2.9	Understand the purpose behind screening individuals: • risk-based approach • politically exposed persons (PEPs)	2.7.3
3.3	Policies, procedures and controls required of firms On completion, the candidate should:	
3.3.1	Understand the risks to a firm posed by its clients, products and delivery systems	3
3.3.2	Understand the controls a firm should have in place to minimise its risk to fraud, money laundering and terrorist financing including a training programme	3.2 & 3.3

3.3.3	Know the criteria for an effective suspicious transaction reporting system	3.4
-------	--	-----

Syllabus Unit/ Element		Chapter/ Section
---------------------------	--	---------------------

Element 4	Ethics, Integrity and Fairness	Chapter 4
4.1	Ethics On completion, the candidate should:	
4.1.1	Understand how ethical principles relate to the financial services sector: • regulatory standards • professional codes of conduct • internal codes of conduct	1
4.1.2	Understand the impact of the following when applying an ethical approach within an organisational or team environment: • self-interest • fiduciary responsibilities • the role of the agent • the role of stakeholders • the role of the group or team	1.5

4.1.3	Understand the advantage of ethical behaviours and decision-making over rule-based compliance	1.5
4.1.4	Understand the importance of senior management leadership in developing and maintaining ethical standards	1.5.6
4.1.5	Know how training programmes can be used to promote ethical decision-making	1.5.7
4.2	Market Integrity On completion, the candidate should:	
4.2.1	Understand the benefits of a fair and orderly market	2.1
4.2.2	Understand the implications of false and misleading statements, behaviours and practices	2.1
4.2.3	Understand what type of information may be deemed to be price-sensitive non-public information	2.2
4.2.4	Understand how individuals may legally possess price-sensitive non-public information	2.3
4.2.5	Know what activities can constitute 'insider dealing'	2.2

4.2.6	Understand how systems and controls can minimise exposure to strategies and behaviours that might impair market integrity: • information barriers insider • lists (including watch and restricted lists) personal • account dealing gifts and • entertainment conflicts of • interest policies	2.4
4.2.7	Understand the importance of whistleblowing for market integrity	2.4
4.3	Fair Conduct On completion, the candidate should:	
4.3.1	Understand expected compliant standards of behaviour for firms and individuals: • honesty & fair treatment • acting in the client's best interest	3
4.3.2	Understand how the concept of fairness impacts on financial services firms	3.3
4.3.3	Understand legal concepts and considerations relevant to financial advice	3.4

4.3.4	Understand the role senior management play in maintaining fair conduct: • senior management responsibilities • management information • corporate culture	3.5
4.4	Client Outcomes On completion, the candidate should:	
4.4.1	Understand how associated but non-transactional activities impact on the firm: • product design and marketing • financial promotions/advertising • client documentation • fair contracts	4
4.4.2	Understand the factors to consider prior to entering into a transaction: • client/counterparty objectives • client/counterparty risk profile • affordability • suitability of the investment	4.5

4.4.3	Understand factors that should be considered at the point of sale: • clear information • suitability of advice	4.5
4.4.4	Understand post-sale factors that may impact on the firm: • handling complaints in line with international standards • avenues of redress • expected and actual product performance • safeguarding customer money and assets • reporting requirements	4.8
4.5	Environmental, Social and Governance (ESG) On completion, the candidate should:	
4.5.1	Know what is meant by Environmental, Social and Governance (ESG)	5
4.5.2	Know the main international ESG initiatives: • Task Force on Climate-Related Financial Disclosures (TCFD) • United Nations supported Principles for Responsible Investment (PRI)	5.1

	Sustainable Finance Disclosure Regulations (SFDR)	
4.5.3	Understand the importance of initiatives on: - climate - green finance - corporate social responsibilities	5.2

Syllabus Unit/ Element		Chapter/ Section
---------------------------	--	---------------------

Element 5	Governance, Risk Management and Compliance	Chapter 5
5.1	Corporate Governance On completion, the candidate should:	
5.1.1	Understand the objectives of corporate governance	1.1
5.1.2	Understand the importance of senior management leadership, accountability and personal responsibility	1.2
5.1.3	Understand the role of the compliance function in implementing and monitoring corporate governance standards	1.3

5.1.4	Know the main corporate governance structures: • unitary board • two-tier structure	1.4
5.1.5	Understand the impact of business and or management structures on the effective management of the compliance function: • matrix structures • silo structures • maintaining independence	1.5
5.1.6	Understand how auditing contributes to prudential corporate governance, accounting and reporting requirements: • audit committees • internal audit • external auditors	1.6
5.1.7	Know the purpose and key elements of due diligence: • identification • selection • fitness & propriety	1.7
5.1.8	Understand how an effective training programme can contribute to good corporate governance	1.8

5.1.9	Understand the factors behind the formulation of the BIS Principles for enhancing corporate governance	1.9
5.1.10	Know the BIS Principles for enhancing corporate governance	1.9
5.2	Key Risk Types, their Application and Impact on the Compliance Function On completion, the candidate should:	
5.2.1	Understand the difference between risk and uncertainty	2.1
5.2.2	Know the key external sources of business risk and their potential impact	2.2
5.2.3	Know the key internal sources of business risk and their potential impact	2.3
5.2.4	Know the components and practical application of an effective risk management process	2.4
5.2.5	Understand how the impact of risks on a firm's business activities are assessed and managed including operational resilience	2.5
5.2.6	Understand the key aims of the risk management function, the risk	2.5.6

	committee and their relationship with the compliance department	
5.2.7	Know the BIS definition of 'compliance risk'	3
5.2.8	Know who BIS deem responsible for the management of compliance risk	3
5.2.9	Know what measures BIS state should be undertaken to manage compliance risk: • formalised document establishing the compliance function • board approval • annual review	3
5.2.10	Understand how technology can be utilised to enhance compliance risk assessment	3.1
5.2.11	Understand how technological changes impact regulatory risk: • cyber crime • FinTech • RegTech • cloud data hosting	3.2

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 should not change by more than plus or minus 2.

Element number	Element	Questions
1	The International Regulatory Environment	20
2	The Compliance Function	24
3	Managing the Risk of Financial Crime	20
4	Ethics, Integrity and Fairness	19
5	Governance, Risk Management and Compliance	17
Total		100

Assessment Structure

A two-hour examination of 100 multiple choice questions.

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

Expand your connections

Tap into a global network of 54,000+ CISI members today!

Join a thriving professional community and take your career to the next level. Become a CISI member to access:

Mentoring Scheme

Get guidance from an experienced mentor or offer to reverse mentor a senior professional.

LinkedIn Community

Connect with like-minded professionals in our exclusive CISI LinkedIn group.

Events

Attend hundreds of in-person and online events every year to expand your knowledge and network.

Young Professionals' Network

Your go-to hub for career support, expert tips, and valuable networking opportunities. Join the network today for exclusive content and events.

Connect with us:



The_CISI



CISI



The CISI



CISITV



thecisi



The_CISI



Endless opportunities await with **CISI qualifications**

Elevate your skills, advance your career and strengthen your personal brand with globally recognised CISI qualifications – designed to open doors worldwide.

Find your next CISI qualification today

Book your exam