
SECTION 2

CORPORATE GOVERNANCE, VIGILANCE, SYSTEMS AND CONTROLS

2.1

STATUTORY OBLIGATIONS

Paragraph 4 of the Code, requires all licenceholders to have in place procedures to forestall and prevent money laundering and terrorist financing. It is a criminal offence for a licenceholder to fail to establish, maintain and operate such procedures. Where such an offence is committed with the consent or connivance of, or is attributable to neglect on the part of an officer of the business, he too shall be deemed to have committed a criminal offence. The definition of officer includes a director, manager or secretary and a person purporting to act as such.

Under paragraph 4(3) of the Code, in determining compliance with the Code, a court may take account of any relevant Commission supervisory or regulatory guidance as to the systems, controls and procedures that must be established by licenceholders.

The list of relevant businesses that fall within the scope of the Code is set out in Schedule 1 of the Code.

In addition, the Rule Book imposes further obligations on licenceholders, a breach of which may lead to the Commission taking regulatory action against the licenceholder itself or key persons of the licenceholder.

2.1.1 Senior management responsibilities: systems and controls

The Board and senior management has a responsibility to ensure that a licenceholder's systems and controls are appropriately designed and implemented, and are effectively operated to reduce the risk of the business being used in connection with money laundering or terrorist financing.

The Board or senior management of a licenceholder must establish documented systems and controls which:

- (a) establish and maintain a risk-based strategy to preventing and detecting money laundering and terrorist financing;
- (b) consider what barriers (including cultural barriers) exist to prevent the operation of effective systems and controls to counter money laundering and terrorist financing;
- (c) ensure adequate resources are given to the Money Laundering Reporting Officer ("MLRO") and compliance function to enable the standards within this Handbook to be adequately implemented and periodically monitored and tested;
- (d) place specific AML/CFT accountabilities and responsibilities on the board, senior management, the MLRO and appropriate staff;
- (e) develop clear customer acceptance policies;
- (f) determine (or receive confirmation of) the true identity of customers, including those who stand behind corporate vehicles and trusts;
- (g) determine the nature of the business that the customer expects to conduct and the commercial rationale for the business relationship;
- (h) require all CDD information to be accurate, relevant and up to date (licenceholders are not automatically required to replace identity documents simply because they have expired since first being obtained);
- (i) require business relationships and transactions to be effectively monitored on an ongoing basis with particular attention to transactions which are complex, both large and unusual, or of an unusual pattern of transactions or which have no apparent economic or lawful purpose;

- (j) apply increased vigilance to transactions and relationships posing higher risks of money laundering or terrorist financing;
- (k) require examination of the background and purpose of transactions and circumstances and a review of CDD information and documents held (taking steps to obtain relevant information and documents where appropriate) in the scenarios specified at paragraph 6 of the Code;
- (l) ensure procedures are established and maintained which allow the MLRO and any other designated person to have access to all relevant information, which may be of assistance to them in considering suspicious transaction reports ("STRs");
- (m) require a disclosure to the Financial Crime Unit ("FCU") when there is knowledge or suspicion or reasonable grounds for knowing or suspecting money laundering or terrorist financing, including attempted money laundering or terrorist financing;
- (n) maintain records for the prescribed periods of time;
- (o) raise awareness amongst all management and staff of the risks of becoming concerned in arrangements involving criminal money and provide specific training for appropriate staff;
- (p) require close liaison with the Commission and the FCU on matters concerning vigilance, systems and controls.

In the absence of the systems and controls outlined above, a licenceholder must not enter into a business relationship or carry out a one-off transaction.

2.2

THE APPOINTMENT OF A MONEY LAUNDERING REPORTING OFFICER ("MLRO")

Paragraph 14 of the Code requires licenceholders to appoint an MLRO. The MLRO is the person who is nominated to ultimately receive internal reports and who considers any report in the light of all other relevant information for the purpose of determining whether or not it gives rise to a knowledge or suspicion of money laundering.

Licenceholders are also required under Rule 8.18 of the Rule Book to appoint a Deputy MLRO to cover for any absence of the MLRO. The Deputy MLRO should be of similar status and experience to the MLRO. MLROs and Deputy MLROs should not be placed in any situation of conflict of interest.

In order that they can carry out their responsibilities effectively the MLRO and Deputy MLRO should:

- (a) normally be resident in the Isle of Man;
- (b) have a sufficient level of seniority, independence and authority within the business;
- (c) be carrying out a compliance, audit or legal role;
- (d) have sufficient resources, including sufficient time and support staff;
- (e) have regular contact with, and ready access to, the Board and other members of senior management to ensure that executive management is able to satisfy itself that the statutory obligations are being met and that the business is taking sufficiently robust measures to protect itself against the risk of money laundering and terrorist financing;
- (f) be fully aware of both their own and their organisation's AML/CFT obligations; and
- (g) have access to all relevant information, which may be of assistance in evaluating STRs.

It is a requirement of the Commission's General Licensing Policy that all MLROs and Deputy MLROs are subject to the Commission's vetting procedures. Therefore licenceholders must notify the Commission of the proposed appointment and identity of the MLRO and Deputy MLRO and any subsequent changes.

2.2.1 Role and responsibilities of the MLRO

The principal objective of the MLRO is to act as the focal point within a licenceholder for the oversight of all activity relating to the prevention and detection of money laundering and terrorist financing.

The responsibilities of the MLRO will normally include:

- (a) undertaking the internal review of all suspicions in the light of all available relevant information and determining whether or not such suspicions have substance and require disclosure to the FCU;
- (b) maintaining all related records;
- (c) giving guidance on how to avoid tipping off the customer if any disclosure is made and managing any resulting constructive trust scenarios;
- (d) providing support and guidance to the Board and senior management to ensure that money laundering and terrorist financing risks are adequately managed;
- (e) liaising with the FCU and if required the Commission and participating in any other third party enquiries in relation to money laundering or terrorist financing prevention and detection, investigation or compliance; and
- (f) providing reports and other information to senior management.

Additional guidance on the role of the MLRO is contained in Section 6.

2.3

COMPLIANCE CULTURE AND THE COMPLIANCE FUNCTION, VIGILANCE AND ROBUSTNESS

The Commission expects each licenceholder to give due priority to establishing and maintaining an effective compliance regime and culture.

The Commission recognises that effective AML/CFT policies and procedures can only be delivered through partnership with the industry and, accordingly, expects all licenceholders to ensure that they establish an open and positive approach to compliance and AML/CFT issues amongst all employees.

Licenceholders must adopt a robust approach and not flinch from asking their customers "awkward" questions in circumstances of unusual activity. Any reluctance or failure by the customer to provide credible and verifiable answers should almost always give grounds for suspicion about his/her activities, make the licenceholder reconsider the wisdom of doing business with him/her and, potentially, lead to a disclosure being made to the FCU.

2.3.1 Common cultural barriers to an effective AML/CFT control system

Despite the implementation of AML/CFT policies and procedures, cultural barriers may hinder an effective organisational system of AML/CFT control. Licenceholders need to recognise and address them. The human element is very important in this context in that policies and procedures only work if they are understood, followed and enforced by those required to comply with them. Sometimes referred to as 'human factors', the inter-relationships between different employees within a licenceholder and between employees and customers, can result in the following damaging barriers:

- (a) Senior management being unwilling to lead on the concept of the need for sound corporate ethics.
- (b) More junior employees assuming that their concerns or suspicions are not significant.
- (c) Employees being unwilling to subject high value (therefore important) customers to effective CDD checks.
- (d) Local management or customer relationship managers outside the Isle of Man pressurising employees in the Isle of Man to transact without obtaining all relevant CDD and business information.

(e) Employees being unable to understand the commercial rationale for customer relationships, so that potentially suspicious activity is not identified.

(f) Lack of time and/or resources to address concerns generating a tendency for line managers to discourage employees from raising concerns.

(g) Conflict between the desire on the part of employees to provide a confidential and efficient customer service and the requirement for employee vigilance in respect of money laundering and terrorist financing prevention and detection.

Policies and procedures will be documented and, therefore, have a tangible nature. On the other hand, the prevailing culture of an organisation is intangible and its impact upon the documented policies and procedures may be hard to assess. The board and senior management must, therefore, identify any relevant cultural barriers and take appropriate steps to resolve them.

2.4

TAKING A RISK BASED APPROACH

2.4.1 Determining the risk

A licenceholder must, under Rule 9.4 of the Rule Book, undertake an assessment of how vulnerable it is to money laundering and terrorist financing. In doing so it should consider the extent of its exposure to risk by reference to its customers, products and services and the manner in which it provides these products and services to its customers. These risks should be properly addressed by policies, procedures and controls.

The licenceholder should record and document its risk assessment. The assessment should be revisited and updated from time to time. An annual reassessment might be appropriate for a dynamic, growing business, but this might not be necessary for an established business with static products and services. The risks identified at Section 2.8 may trigger such a reassessment.

The following list of considerations may help a licenceholder to undertake this risk assessment.

(a) Actively involving all members of senior management in determining the risks posed by money laundering and terrorist financing within those areas for which they have responsibility.

(b) Considering organisational factors that may increase exposure to the risk of money laundering and terrorist financing e.g. business volumes and outsourcing aspects of regulated activities or compliance functions.

(c) Considering the nature, scale and complexity of its business, the diversity of its operations, the volume and size of its transactions, and the degree of risk associated with each area of its operation.

(d) Considering who its customers are and what they do.

(e) Considering whether any additional risks are posed by the jurisdictions with which its customers (including intermediaries and introducers) are connected. Factors such as high levels of organised crime, increased vulnerabilities to corruption and inadequate frameworks to prevent and detect money laundering and the financing or terrorism will affect the risk.

(f) Considering the characteristics of the products and services that it offers and assessing the associated vulnerabilities posed by each product or service.

(g) Considering how it establishes and delivers products and services to its customers. E.g. risks could be higher where relationships may be established remotely (non-face-to-face), or may be controlled remotely by the customer (straight through processing of transactions).

Further guidance on these matters is given below.

2.4.2 Organisational Risk

Organisational factors that may enhance the level of exposure to the risk of money laundering and terrorist financing include:

- (a) target market place;
- (b) monetary strategies;
- (c) business volumes;
- (d) geographical areas of business activity;
- (e) outsourcing aspects of regulated activity / compliance functions.

2.4.3 Customer Risk

Clear customer acceptance policies and procedures should be developed by all licenceholders. They should have a system of risk grading which includes a description of the types of customer that are likely to pose a higher than average risk of money laundering and terrorist financing. CDD requirements at the outset of a relationship and thereafter should then be tailored proportionally according to the perceived risks. In other words, the higher the risk of the customers, the more extensive the requirements. For example, a policy may require only basic account opening CDD requirements for a low balance, low turnover deposit account, whilst extensive CDD would be essential for an individual (or corporate entity) with unclear fund sources or who requires the setting up of complex structures.

Additional guidance on CDD requirements is provided in Sections 3 and 4.

2.4.4 Business risk

Licenceholders must consider the extent to which they are exposed to money laundering and terrorist financing. In so doing, they must take account of the primary objectives of money laundering. These include:

- (a) the intention and requirement to benefit and retain the proceeds of predicate crimes;
- (b) the need to disguise ownership of criminal property which could otherwise provide a link between the launderer and the predicate crime;
- (c) the desire to retain an element of control over the criminal property;
- (d) the need to disguise the origins of criminal property.

Organisational risk, customer risk and product/service risk, including the means by which those products and services are delivered must all be taken into account.

2.4.5 Product/service risk

Licenceholders should consider the characteristics of the products and services that they offer and the extent to which they are vulnerable to money laundering and terrorist financing abuse. Particular risks are associated with the formation and management of companies and trusts. Generally, any form of legal entity or related service that enables individuals to divest themselves of ownership of property whilst retaining an element of control over it is vulnerable. Examples include the following:

- (a) companies that can be incorporated without the identity of the ultimate underlying principals being disclosed;
- (b) certain forms of trusts or foundations including blind trusts, dummy settlor trusts and settlor directed trusts where knowledge of the identity of the true underlying principals or controllers cannot be guaranteed;
- (c) the provision of nominee shareholders;
- (d) companies issuing bearer shares;

(e) correspondent banking relationships - a correspondent account can be used to transfer funds on behalf of unidentified third parties;

(f) wire transfers - speed and ease of transmission across jurisdictions;

(g) any financial service or product that is capable of being provided on a non-face-to-face basis or controlled by a customer remotely.

The highest risk products or services are those with high values and volumes; those where unlimited third party funds can be freely received; or those where funds can regularly be paid to third parties without evidence of identity of the third parties being obtained. For example, some of the highest risk products are those offering money transfer facilities through cheque books, wire transfers, deposits from third parties or other means. Corporate and personal current accounts and high value deposit/investment accounts naturally fall within this category. Wealth management and private banking facilities can be particularly vulnerable.

Some of the lowest risk products and services are those where funds can only be received from a named investor by way of payment from an account held in the investor's name. The funds can then only be redeemed to the same investor's account. Such products do not allow third party funding or payments and no opportunity is presented for the onward transmission of funds to third parties in the arrangement. Regulated open and closed-ended investment funds, some insurance products, retail credit business, some asset finance, and low value deposit/savings accounts generally fall within this category.

Notwithstanding the reduced risks of money laundering posed by such products and services, they provide criminals with an opportunity to convert property into a different form for the duration of the relationship and to conceal ownership of funds, particularly where they disguise their interest behind an entity that makes the investment on their behalf. Therefore no product or service is ever immune from the laundering process.

Licenceholders should also consider how they deliver products and services to their customers and the extent to which this might increase the risk. For example, risks are likely to be greater when relationships can be established remotely (non-face-to-face), or when they may be controlled remotely by the customer ("straight-through" processing of transactions).

2.4.6 Activity risk

Licenceholders should consider risks inherent in the nature of the activity of the account holder and the possibility that the transaction may itself be a criminal transaction. The arms trade and the financing of the arms trade is an example of an activity that poses multiple AML and other risks, e.g.:

(a) Corruption risks arising from procurement contracts;

(b) PEP risks;

(c) Terrorism and terrorist financing risks as shipments may be diverted.

In addition to the movement of weapons and the proceeds of corruption, international bodies have also drawn attention to the need for vigilance in identifying potential attempts by countries that are the subject of sanctions to raise funds for programmes to develop nuclear and other weapons of mass destruction.

2.5

EXISTING CUSTOMERS

The Anti-Money Laundering (Amendment) Code 1999 disapplied the requirements of the Anti-Money Laundering Code 1998 to pre-1998 customers. This was revoked on the coming into force of the Criminal Justice (Money Laundering) Code 2007 in September 2007. There is no longer a blanket exemption to applying CDD procedures to pre-1998 existing business relationships.

In addition, paragraph 6 of the Code requires licenceholders to undertake CDD on their "continuing business relationships" in certain circumstances as soon as reasonably practicable. The phrase "continuing business relationships" includes pre-1998 customers. One such circumstance outlined in the Code is when the

licenceholder becomes aware of anything which causes them to doubt the veracity or adequacy of the information and documents held.

Rule 9.4 of the Rule Book requires licenceholders to undertake a risk assessment having regard to the persons to whom they provide products and services. This risk assessment must cover licenceholders' existing business relationships and must be undertaken as soon as reasonably practicable after Part 9 of the Rule Book comes into force.

It follows that the risk assessment for existing business relationships must include a review of the information and documentation held in respect of those customers. Such a review will highlight those relationships where there is doubt about the veracity or adequacy of the information and documentation held.

An appropriate time to conduct CDD procedures on existing relationships will therefore be at any time when a licenceholder becomes aware that any of the circumstances at paragraph 6 of the Code apply either as a result of the risk assessment or otherwise. Licenceholders may demonstrate that it has applied CDD procedures where it does so in accordance with Sections 3 and 4 of the Handbook.

2.6

ACQUISITION OF A BUSINESS OR A BLOCK OF CUSTOMERS

Before acquiring a business with established business relationships or a block of customers, licenceholders must make enquiries of the vendor to establish the level and appropriateness of the CDD information and verification documentation held in relation to the business to be acquired.

Licenceholders may rely on documentation and information previously obtained by the vendor where the following conditions are met:

- (a) The vendor is a person who falls within the definition of an Acceptable Applicant under paragraph 5(4) of the Code; and
- (b) The licenceholder has assessed that the CDD policies, procedures and controls operated by the vendor are satisfactory; and
- (c) The licenceholder has obtained from the vendor the CDD information and verification documentation for each customer to be acquired.

Where the above conditions are not met or there are deficiencies in the CDD information and verification documentation, the licenceholder must determine and implement a programme to apply CDD and verification procedures on each customer and to remedy deficiencies.

2.7

EMPLOYEE SCREENING

Paragraph 15 of the Code states that licenceholders must establish, maintain and operate appropriate procedures in order to be satisfied of the integrity of any new directors or partners and all new appropriate employees. Therefore, licenceholders must satisfy themselves that the directors, partners and employees are fit and proper for the performance of their roles (see Section 7.2).

2.8

TECHNOLOGICAL DEVELOPMENTS

Rule 9.13 of the Rule Book requires licenceholders to maintain appropriate procedures and controls for the purpose of preventing the misuse of technological developments for the purpose of money laundering or terrorist financing.

Licenceholders must ensure that appropriate staff keep abreast of relevant technological developments and identified methodologies in money laundering and terrorist financing schemes. This may involve reviewing papers from international bodies such as the FATF Typologies; warnings and information issued by regulators and law enforcement as well as information issued by industry bodies or trade associations.

The appropriate system must embrace keeping up to date with such developments and the potential new risks and impact they may have on the products and services offered by licenceholders. Risks identified must be fed into the business risk assessment required at Rule 9.4 in the Rule Book.

2.9

COMPLIANCE MONITORING

A licenceholder must have procedures to ensure that they regularly monitor and sample test the implementation and operation of all AML/CFT procedures and controls. If appropriate, having regard to the risk of money laundering and terrorist financing and the size of the business, this may be undertaken by the compliance and internal auditing departments. The effectiveness of awareness raising and training for appropriate staff should also be monitored and tested on a regular basis.

If appropriate, having regard to the risk of money laundering and terrorist financing and the size of the business, the Board or senior management should commission a periodic report (at least annually) from the Compliance Officer (or MLRO if appropriate). This report is to ensure that AML/CFT compliance is being undertaken to the necessary standards and should specify the details of the compliance of the licenceholder with the Code, the Rule Book and this Handbook during the relevant period.

The periodic report may include:

- (a) The means by which the effectiveness of the licenceholder's systems, controls and procedures have been managed and tested.
- (b) Significant compliance deficiencies identified and details of action taken or proposed to address any such deficiencies.
- (c) Failure to apply the Isle of Man requirements in branches and subsidiaries, any advice received from the Commission and details of action taken.
- (d) The number of internal reports received and the number of subsequent disclosures submitted to the FCU, any perceived deficiencies in internal or external reporting procedures, and the nature of changes proposed or implemented to address any such deficiencies.
- (e) Information concerning the training programme for the preceding year, which staff have received training, the methods of training and the nature of the training.
- (f) Changes made or proposed in respect of new legislation, regulatory requirements or guidance.
- (g) A risk assessment of any new types of product or service, or new distribution channels, and the proposed or implemented measures to counter money laundering or terrorist financing.
- (h) The nature of actions taken in response to notices highlighting jurisdictions that do not sufficiently apply the FATF Recommendations, or which are the subject of international countermeasures, and the measures taken to manage and monitor business relationships connected with such jurisdictions.
- (i) Any recommendations concerning additional resource requirements to ensure effective compliance with the licenceholder's statutory and regulatory obligations.

To assist the Compliance Officer (or MLRO) in preparing the periodic report, and to ensure that the report is a fair and accurate assessment, a licenceholder may wish to provide support from its internal audit or compliance function as appropriate, or to seek an assessment from external sources.

Where a licenceholder is part of a group or involved in multiple jurisdictions, a consolidated report may be appropriate.

2.10

MANAGED LICENCEHOLDERS

For the avoidance of doubt, any licenceholder that is managed by another licenceholder retains the responsibility for ensuring compliance with AML/CFT requirements.