2 CORPORATE GOVERNANCE

Please Note:

- Regulatory requirements are set within this section as *AML/CFT Codes of Practice*.
- This section contains references to Jersey legislation which may be accessed through the JFSC website.
- Where terms appear in the Glossary this is highlighted through the use of italic text. The Glossary is available from the JFSC website.

2.1 Overview of Section

1. Corporate governance is the system by which enterprises are directed and controlled and their risks managed. For those law firms undertaking Schedule 2 business, *money laundering* and the *financing of terrorism* are risks that must be managed in the same way as other business risks.
2. On the basis that law firms tend to be partnerships, rather than this Handbook referring to the responsibilities of "the Board" (as is the case in the *AML/CFT Handbook*) it refers to the responsibilities of the senior management of the law firm. In the case of a sole trader, senior management will be the sole trader.
3. A sole practitioner will not necessarily be a sole trader[1].
4. Under the general heading of corporate governance, this Section therefore considers:
   - senior management responsibilities for the prevention and detection of *money laundering* and the *financing of terrorism*;
   - requirements for risk management *systems and controls*, and for training; and
   - the appointment of a Money Laundering Compliance Officer (the ***MLCO***) and Money Laundering Reporting Officer (the ***MLRO***).
5. This Handbook describes the requirements for a law firm's general framework of *systems and controls* to combat *money laundering* and *the financing of terrorism* as its "***systems and controls***". This Handbook refers to the way in which those *systems and controls* are to be implemented into the day-to-day operation of a law firm as its "***policies and procedures***".

2.2 Measures to Prevent Money Laundering and Financing of Terrorism

Statutory Requirements

6. *In accordance with Article 37 of the Proceeds of Crime Law, a relevant person must take prescribed measures to prevent and detect money laundering and the financing of terrorism. Failure to take such measures is a criminal offence and, where such an offence is proved to have been committed with the consent or connivance of, or to be attributable to neglect on the part of, an officer, partner or member of the relevant person, they too shall be deemed to have committed a criminal offence.*

[1] "sole trader" is defined in Article 1(1) of the Money Laundering Order.

7. *Article 37 of the Proceeds of Crime Law enables the Chief Minister to prescribe by Order the measures that must be taken by a relevant person. These measures are established in the Money Laundering Order.*

2.3 Senior Management Responsibilities

Overview

8. The key responsibilities of senior management, set out in further detail below, are to:

   › identify the firm's *money laundering* and *the financing of terrorism* risks;

   › ensure that its *systems and controls* are appropriately designed and implemented to manage those risks; and

   › ensure that sufficient resources are devoted to achieving these objectives.

9. Senior management is assisted in fulfilling these responsibilities by a *MLCO* and *MLRO*. Larger or more complex firms may also require dedicated risk and internal audit functions to assist in the assessment and management of *money laundering* and *the financing of terrorism* risk.

Statutory Requirements

10. *Article 11(1) of the Money Laundering Order requires a relevant person to establish and maintain appropriate and consistent policies and procedures in respect of the person's financial services business, and financial services business carried on by a subsidiary, in order to prevent and detect money laundering and the financing of terrorism.*

11. *Article 11(9) of the Money Laundering Order requires a relevant person to take appropriate measures for the purpose of making employees whose duties relate to the provision of relevant services (**relevant employees**) aware of policies and procedures required under Article 11(1) of the Money Laundering Order and of Jersey's money laundering legislation. Article 11(10) of the Money Laundering Order requires a relevant person to provide relevant employees with training in the recognition and handling of transactions carried out by or on behalf of persons who are, or appear to be, engaged in money laundering or the financing of terrorism.*

12. *Article 11(11) of the Money Laundering Order requires a relevant person to establish and maintain adequate procedures for (i) monitoring compliance with, and testing the effectiveness of its policies and procedures; and (ii) monitoring and testing the effectiveness of measures to promote AML/CFT awareness and training of relevant employees (see Section 9 of this Handbook).*

13. *Articles 7 and 8 of the Money Laundering Order require that a relevant person appoints a MLCO and a MLRO.*

AML/CFT Codes of Practice

~~14. Senior Management must establish a formal strategy to counter *money laundering* and the *financing of terrorism*. Where a Jersey law firm forms part of a group operating outside the Island, that strategy may protect both its global reputation and its Jersey business.~~

~~15.~~14. Senior management must conduct and record a business risk assessment. In particular, Senior management must consider, on an ongoing basis, its risk appetite, and the extent of its exposure to *money laundering* and *the financing of terrorism* risks "in the round" or as a whole by reference to its organisational structure, its clients, the countries and territories with which its clients are connected, its range of services, and how it delivers those services. The assessment must consider the cumulative effect of risks identified, which may exceed the sum of each individual risk element. Senior management's assessment must be kept up to date. (Guidance on conducting the business risk assessment is set out in Section 2.3.1 below).

15. On the basis of its business risk assessment, Senior Management must establish a formal strategy to counter *money laundering* and the *financing of terrorism*. Where a Jersey law firm forms part of a group operating outside the Island, that strategy may protect both its global reputation and its Jersey business.

16. Senior management must record the results of its business risk assessment and keep the assessment under review.

17. Taking into account the conclusions of the business risk assessment, senior management must (i) organise and control the firm's affairs in a way that effectively mitigates the risks that it has identified, including areas that are complex; and (ii) be able to demonstrate the existence of adequate and effective *systems and controls* (including *policies and procedures*) to counter *money laundering* and the *financing of terrorism* (see Section 2.4).

18. Senior management must document its *systems and controls* (including *policies and procedures*) and clearly apportion responsibilities for countering *money laundering* and *the financing of terrorism*, and, in particular, responsibilities of the *MLCO* and *MLRO* (see Sections 2.5 and 2.6).

19. Senior management must assess both the effectiveness of, and compliance with, *systems and controls* (including *policies and procedures*), and take prompt action necessary to address any deficiencies (see Sections 2.4.1 and 2.4.2).

20. Senior management must consider what barriers (including cultural barriers) exist to prevent the operation of effective *systems and controls* (including *policies and procedures*) to counter *money laundering* and *the financing of terrorism*, and must take effective measures to address them (see Section 2.4.3).

21. Senior management must notify the *Commission* immediately in writing of any material failures to comply with the requirements of the *Money Laundering Order* or of this Handbook. Refer to Part 3 of the *AML/CFT Handbook* for further information.

2.3.1 Business Risk Assessment

AML/CFT Codes of Practice

22. A firm~~relevant person~~ must maintain appropriate policies and procedures to enable it, when requested by the JFSC, to make available to that authority a copy of its business risk assessment.

Guidance Notes

~~22.~~23. A firm may extend its existing risk management systems to address *money laundering* and *financing of terrorism* risks. The detail and sophistication of these systems will depend on the firm's size and the complexity of the business it undertakes. Ways of incorporating a firms' business risk assessment will be governed by the size of the firm and how regularly compliance staff and senior management are involved in day-to-day activities.

~~23.~~24. Senior management of a firm may demonstrate that it has considered its exposure to *money laundering* and *the financing of terrorism* risk by:

- involving all members of senior management in determining the risks posed by *money laundering* and *financing of terrorism* within those areas for which they have responsibility;
- considering organisational factors that may increase the level of exposure to the risk of *money laundering* and *the financing of terrorism*, e.g. business volumes and outsourced aspects of regulated activities or compliance functions;
- considering the nature, scale and complexity of its business, the diversity of its operations (including geographical diversity), the volume and size of any transactions, and the degree of risk associated with each area of its operation;
- considering who its clients are and what they do;
- considering whether any additional risks are posed by the countries or territories with which the firm or its clients are connected. Factors such as high levels of organised crime, increased vulnerabilities to corruption and inadequate frameworks to prevent and detect *money laundering* and *financing of terrorism* will impact the risk posed by relationships connected with such countries and territories;
- considering the risk that is involved in placing reliance on *obliged person*s to apply *reliance identification measures*;
- considering the characteristics of its service areas and assessing the associated vulnerabilities posed by each service area. For example:
    a. assessing how legal entities and structures might be used to mask the identities of the underlying beneficial owners; and
    b. considering how the firm establishes and delivers services to its clients. For example, risks are likely to be greater where relationships may be established remotely (non-face to face); and
- considering the accumulation of risk for more complex customers.

~~24.~~25. In the case of a law firm that is dynamic and growing, senior management may demonstrate that its business risk assessment is kept up to date where it is reviewed annually. In some other cases, this may be too often e.g. a firm with stable services or smaller well-established business. In all cases, senior management may demonstrate that its business risk assessment is kept up to date where it is reviewed when events (internal and external) occur that may materially change *money laundering* and the *financing of terrorism* risk.

2.3.1.1 Considering and Assessing Service Area Vulnerabilities and Warning Signs

Overview

~~25.~~26. As part of their business risk assessment, firms are required to assess their service area risks. This service area risk assessment must also be reflected when undertaking a client risk assessment and firms must also take steps to be aware of transactions with heightened *money laundering* risks.

~~26.~~27. The following sub-sections set out some key legal service area vulnerabilities drawn from *FATF* and law enforcement guidance and case studies, and some key warning signs that have been drawn up by the Law Society for England and Wales, as an indication of service area vulnerabilities. Further factors to consider when evaluating the risks posed by clients and service areas are set out in Section 3.3.4 of this Handbook.

Use of Client Accounts

~~27.~~28. Lawyers should not provide a banking service for their clients. However, it can be difficult to draw a distinction between holding client money for a legitimate transaction and acting more like a bank. For example, when the proceeds of a sale are left with a firm to make payments, these payments may be to mainstream lending companies, but these may also be to more obscure recipients, including private individuals, whose identity is difficult or impossible to check.

~~28.~~29. The following situations could give rise to cause for concern:

- a client deposits funds into a firm's client account, but then ends the transaction for no apparent reason;
- a client advises that funds are coming from one source and at the last minute the source changes; or
- a client unexpectedly requests that money received into a firm's client account be sent back to its source, to the client or to a third party.

~~29.~~30. Firms should think carefully before disclosing client account details as this allows money to be deposited into a client account without the firm's knowledge. If it is necessary to provide account details, firms should ask the client where the funds will be coming from. Will it be an account in their name, from Jersey or another jurisdiction? Firms should consider whether they are prepared to accept funds from any source that they are concerned about.

~~30.~~31. Circulation of client account details should be kept to a minimum. Clients should be discouraged from passing the details on to third parties and should be asked to use the account details only for previously agreed purposes.

Establish a Policy on Handling Cash

~~31.~~32. It is good practice to establish a policy of not accepting cash payments above a certain limit either at the firm's office or into the firm's bank account. Clients may attempt to circumvent such a policy by depositing cash directly into a client account at a bank. Firms may consider advising clients in such circumstances that they might encounter a delay in completion of the final transaction. Avoid disclosing client account details as far as possible and make it clear that electronic transfer of funds is expected.

Source of Funds

32.33. Accounts staff should monitor whether funds received from clients are from credible sources. For example, it is reasonable for monies to be received from a company if your client is a director of that company and has the authority to use company money for the transaction.

33.34. However, if funding is from a source other than a client, firm's may need to make further enquiries, especially if the client has not advised what they intend to do with the funds before depositing them into the firm's account. If it is decided to accept funds from a third party, perhaps because time is short, firms should ask how and why the third party is helping with the funding.

34.35. Enquiries do not need to be made into every source of funding from other parties. However firms must always be alert to warning signs and in some cases will need to seek more information.

35.36. In some circumstances, cleared funds will be essential for transactions and clients may want to provide cash to meet a completion deadline. Firms should assess the risk in these cases and ask more questions if necessary.

Private Client Work - Administration of Estates

36.37. A deceased person's estate is very unlikely to be actively utilised by criminals as a means for laundering their funds; however, there is still a low risk of *money laundering* for those working in this area.

37.38. When winding up an estate, there is no blanket requirement that firms should be satisfied about the history of all of the funds which make up the estate under administration; however firms should be aware of the factors which can increase *money laundering* risks and consider the following:

- where estate assets have been earned in a foreign jurisdiction, firms should be aware of the wide definition of criminal conduct in the *Proceeds of Crime Law*; and
- where estate assets have been earned or are located in a higher risk territory, firms may need to make further checks about the source of those funds.

38.39. Firms should be alert from the outset and monitor throughout so that any disclosure can be considered as soon as knowledge or suspicion is formed and problems of delayed consent are avoided (see Section 8.4 of this Handbook).

39.40. Firms should bear in mind that an estate may include criminal property. An extreme example would be where the firm knows or suspects that the deceased person was accused or convicted of acquisitive criminal conduct during their lifetime.

40.41. If firms know, or suspect that the deceased person improperly claimed welfare benefits/allowances or had evaded the due payment of tax during their lifetime, criminal property will be included in the estate and so a *money laundering* disclosure may be required.

41.42. Relevant local laws will apply before assets can be released. For example, a grant of probate will normally be required before UK assets can be released. Firms should remain alert to warning signs, for example if the deceased or their business interests are based in a higher risk jurisdiction.

42.43. If the deceased person is from another jurisdiction and a lawyer is dealing with the matter in the home country, firms may find it helpful to ask that person for information about the deceased to gain some assurances that there are no suspicious circumstances surrounding the estate. The issue of the tax payable on the estate may depend on the jurisdiction concerned.

Charities

43.44. While the majority of charities are used for legitimate reasons, they can be used as *money laundering* or *the financing of terrorism* vehicles.

44.45. Firms acting for charities should consider its purpose and the organisations it is aligned with. If money is being received on the charity's behalf from an individual or a company donor, or a bequest from an estate, firms should be alert to unusual circumstances, including large sums of money.

Property Transactions

45.46. Criminal conduct generates huge amounts of illicit capital and these criminal proceeds need to be integrated into personal lifestyles and business operations. Law enforcement advise that property purchases are one of the most frequently identified methods of laundering money. Property can be used either as a vehicle for laundering money or as a means of investing laundered funds.

46.47. Criminals will buy property both for their own use, e.g. as principal residencies or second homes, business or warehouse premises, and as investment vehicles to provide additional income. The Serious Organised Crime Agency in the UK advises that real property arises in over 85% of all confiscation cases and at least 25% of those investigated hold five or more properties both residential and commercial.

47.48. The purchase of real estate is commonly used as part of the last stage of *money laundering*. Such a purchase offers the criminal an investment which gives the appearance of financial stability. The purchase of a restaurant or hotel, for example, offers particular advantages, as it is often a cash-intensive business, which is the preferred currency of the criminals. Retail businesses provide a good front for criminal funds where legitimate earnings can be used as a front for the proceeds of crime.

Criminal Use of Conveyancing Services

48.49. Law enforcement advises that of all the services offered by legal practitioners, conveyancing is the most utilised function by criminal groups. Conveyancing is a comparatively easy and efficient means to launder money with relatively large amounts of criminal monies 'cleaned' in one transaction. In a stable or rising property market, the launderer will incur no financial loss except fees. Conveyancing transactions can also be attractive to money launderers who are attempting to disguise the audit trail of the proceeds of their crimes. As the property itself can be 'criminal property' for the purposes of the *Proceeds of Crime Law*, lawyers can still be involved in *money laundering* even if no money changes hands.

49.50. Corrupt lawyers may employ trainees to perform the conveyancing work from criminal groups, thereby distancing themselves from the criminal aspect of the business. Conveyancers should also be alert to instructions which are a deliberate attempt to avoid assets being dealt with in the way intended by the court or through the usual legal process. For example, lawyers may sometimes suspect that instructions are being given to avoid the property forming part of a bankruptcy, or forming part of assets subject to confiscation.

Ownership Issues

~~50.~~51. Properties owned by nominee companies or multiple owners may be used as *money laundering* vehicles to disguise the true owner and/or confuse the audit trail. Firms should be alert to sudden or unexplained changes in ownership.

~~51.~~52. One form of laundering, known as flipping, involves a property purchase, often using someone else's identity. The property is then quickly sold for a much higher price to the same buyer using another identity. The proceeds of crime are mixed with mortgage funds for the purchase. This process may be repeated several times.

~~52.~~53. Another potential cause for concern is where a third party is providing the funding for a purchase, but the property is being registered in someone else's name. There may be legitimate reasons for this, such as a family arrangement, but firms should be alert to the possibility of being misled about the true ownership of the property. Further *CDD* measures should be undertaken on the person providing the funding.

Methods of Funding

~~53.~~54. Many properties are bought with a combination of deposit, mortgage and/or equity from a current property. Usually, the lawyer acting for the purchaser will have information about how the client intends to fund the transaction. Lawyers should expect to be updated if those details change, for example, if a mortgage falls through and new funding is obtained.

~~54.~~55. Firms should remember that payments made through the mainstream banking system are not guaranteed to be clean.

~~55.~~56. Transactions that do not involve a mortgage or are not being financed wholly from the sale of a previous property have a higher risk of being fraudulent. Firms should be alert for large payments from private funds, especially if the client receives payments from a number of individuals or sources. If concerns arise;

- the client should be asked to explain the *source of funds*. Firms should assess whether the explanation appears to be valid – e.g. the money has been received from an inheritance;
- ensure that the client is the beneficial owner of the funds being used in the purchase.

~~56.~~57. Third parties often assist with purchases and firms may be asked to receive funds directly from third parties, for example relatives often assist first time buyers. Consideration will need to be given as to the extent of due diligence that needs to be undertaken on those third parties. Firms should consider whether there are any obvious warning signs and what needs to be known about:

- the client;
- the third party;
- their relationship; and
- the proportion of the funding being provided by the third party.

~~57.~~58. Firms should consider their obligations to the lender in these circumstances – firms are normally required to advise lenders if the buyers are not funding the balance of the price from their own resources.

Valuations

58.59. An unusual sale price can be an indicator of *money laundering*. Whilst lawyers acting in a property sale are not required to get independent valuations, if a firm becomes aware of a significant discrepancy between the sale price and what a property would reasonably be asked to sell for, consideration should be given to asking more questions.

59.60. Properties may also be sold below the market value to an associate, with a view to obscuring the title to the property while the original owner still maintains the beneficial ownership.

Mortgage Fraud

60.61. A firm may discover or suspect that a client is attempting to mislead a lender client to improperly inflate a mortgage advance – for example, by misrepresenting the borrower's income or because the seller and buyer are conspiring to overstate the sale price. Transactions which are not at arm's length may warrant particular consideration. However, until the improperly obtained mortgage advance is received, there is not any criminal property for the purposes of disclosure obligations to the *JFCU*.

61.62. If a firm suspects that a client is making a misrepresentation to a mortgage lender, the firm must either dissuade them from doing so or consider the ethical implications of continuing with the retainer. Even if a firm no longer acts for the client, it may still be under a duty to advise the mortgage lender.

62.63. Large scale mortgage fraud is more sophisticated and will normally involve several properties. It may be committed by criminal groups or by individuals. The buy-to-let market is particularly vulnerable to large scale mortgage fraud whether through new-build apartment complexes or large scale renovation properties. Occasionally commercial properties will be involved.

63.64. Fraudsters may use private sources of funding such as property clubs, especially when credit market conditions tighten. These lenders often have lower safeguards than institutional lenders, leaving them vulnerable to organised fraud. Property clubs can be targeted particularly in relation to overseas properties where the property either does not exist, or is a vacant piece of land, not a developed property.

64.65. Sometimes fraud is achieved by selling the property between related private companies. The transactions will involve inflated values and will not be at arm's length. Increasingly, offshore companies are used with the property sold several times within the group before approaching a lender for a mortgage at an inflated value.

65.66. Firms that discover or suspect that a mortgage advance has already been improperly obtained should consider advising the mortgage lender.

66.67. Firms acting in a connection with a re-mortgage who discover or suspect that a previous mortgage has been improperly obtained may need to advise the lender, especially if the re-mortgage is with the same lender. Consideration should also be given to making a disclosure to the *JFCU* as the improperly obtained mortgage advance represents criminal property.

67.68. If a client has made a deliberate misrepresentation on their mortgage application, it is likely that the crime/fraud exemption to legal professional privilege will apply (see Section 8 of this Handbook). This means that no waiver of confidentiality will be needed before a disclosure is made. However, such matters will need to be dealt with on a case-by-case basis.

Company and Commercial Work

68.69. The nature of company structures can make them attractive to money launderers because it is possible to obscure true ownership and protect assets for relatively little expense. For this reason, lawyers working with companies and in commercial transactions should remain alert throughout their retainers, with existing as well as new clients.

69.70. A common operating method amongst serious organised criminals is the use of front companies. These are often used to disguise criminal proceeds as representing the legitimate profits of fictitious business activities. They can also help to make the transportation of suspicious cargoes appear as genuine goods being traded. More often than not, they are used to mask the identity of the true beneficial owners and the source of criminally obtained assets. Corporate vehicles are also frequently used to help commit tax fraud, facilitate bribery/corruption, shield assets from creditors, facilitate fraud generally or circumvent disclosure requirements.

70.71. The lack of transparency concerning the ownership and control of corporate vehicles has proved to be a consistent problem for *money laundering* investigations. Corporations serving as directors and nominee directors can be used to conceal the identity of the natural persons who manage and control a corporate vehicle.

71.72. Several international reports have highlighted the extent to which private limited companies, shell companies, bearer shares, nominees, front companies and special purpose vehicles have been used in laundering operations. Case studies submitted to the *FATF* have indicated the following common elements in the misuse of corporate vehicles:

- multi-jurisdictional and/or complex structures of corporate entities and trusts;
- foreign payments without a clear connection to the actual activities of the corporate entity;
- use of offshore bank accounts without clear economic necessity;
- use of nominees;
- use of shell companies; and
- tax, financial and legal advisers were generally involved in developing and establishing the structure. In some case studies a lawyer was involved and specialised in providing illicit services for clients.

72.73. The more of the above elements that exist, the greater the likelihood and the risk that the identity of the underlying beneficial owner may be able to remain unidentifiable.

Shell Corporations

73.74. The shell corporation is a tool that appears to be widely used by criminals. Often purchased “off-the-shelf” it remains a convenient vehicle for laundering money and for concealing the identity of the beneficial owner of the funds. The company records are often more difficult for law enforcement to access because they are held behind a veil of professional privilege or the professionals who run the company act on instructions remotely and anonymously.

74.75. Shell companies are often used to receive deposits of cash which are the transferred to another jurisdiction, to facilitate false invoicing or to purchase real estate and other assets. They have also been used as the vehicle for the actual predicate offence of bankruptcy fraud on many occasions.

Bearer Shares

75.76. Bearer shares confer rights of ownership to a company upon the physical holder of the share. They are commonly and legitimately used in a number of countries. However, the high level of anonymity that bearer shares offer provides opportunities for misuse where the identity of the shareholder is not recorded when the share is issued and transferred, ownership of the share is effectively anonymous.

76.77. Such shares are open to two *money laundering* risks:

- financial assets can be acquired without the purchaser being identified; and
- the company owners and controllers may not be capable of being identified.

77.78. To guard against misuse, a number of jurisdictions have dematerialised or immobilised bearer shares when they are registered in an effort to ensure that the identity of the beneficial owners can be verified. Dematerialisation is achieved by requiring registration upon transfer or requiring registration in order to vote or collect dividends. While physical transfer of bearer shares is possible, it is believed to be rare.

Holding of Funds

78.79. Firms who choose to hold funds as stakeholder or escrow agent in commercial transactions should consider the checks to be made about the funds they intend to hold before the funds are received. Consideration should be given to conducting *CDD* measures on all those on whose behalf the funds are being held.

79.80. Particular consideration should be given to any proposal that funds are collected from a number of individuals whether for investment purposes or otherwise. This could lead to wide circulation of client account details and payments being received from unknown sources.

Private Equity

80.81. Law firms could be involved in any of the following circumstances:

- the start-up phase of a private equity business where individuals or companies seek to establish a private equity firm (and in certain cases, become authorised to conduct investment business);
- the formation of a private equity fund;
- ongoing legal issues relating to a private equity fund; or
- execution of transactions on behalf of a member of a private equity firm's group of companies (a private equity sponsor that will normally involve a vehicle company acting on its behalf (newco)).

81.82. Generally private equity work will be considered to be low risk for *money laundering* or the *financing of terrorism* for the following reasons:

- private equity firms are also covered by the *Money Laundering Order* and similar legislation in equivalent jurisdictions;
- investors are generally large institutions, some of which will also be regulated for *money laundering* purposes;
- there are generally detailed due diligence processes followed prior to investors being accepted;
- the investment is generally illiquid and the return of capital is unpredictable; and

› the terms of the investment in the fund generally strictly control the transfer of interests and the return of funds to investors.

~~82.~~83. Factors which may alter this risk assessment include:

› where the private equity firm, fund manager or an investor is located in a jurisdiction which is not regulated for *money laundering* to a standard which is equivalent to the *FATF* recommendations;

› where the investor is either an individual or an investment vehicle itself (a private equity fund of funds); and

› where the private equity firm is seeking to raise funds for the first time or is approaching a large investor base.

2.4 Adequate and Effective Systems and Controls

Overview

~~83.~~84. For *systems and controls* (including *policies and procedures*) to be adequate and effective in preventing and detecting *money laundering* and *the financing of terrorism*, they will need to be appropriate to the circumstances of the firm.

Statutory Requirements

~~84.~~85. *Article 11(1) of the Money Laundering Order requires a relevant person to establish and maintain appropriate and consistent policies and procedures in respect of the person's financial services business, and financial services business carried on by a subsidiary, in order to prevent and detect money laundering and the financing of terrorism.*

~~85.~~86. *Parts 3, 3A, 4 and 5 of the Money Laundering Order set out the measures that are to be applied in respect of customer due diligence, record keeping and reporting.*

~~86.~~87. *Article 11(2) of the Money Laundering Order requires that policies and procedures established and maintained under Article 11(1)are appropriate and consistent having regard to the degree of risk of money laundering and the financing of terrorism taking into account: (i) the level of risk identified in a national or sector-specific risk assessment in relation to money laundering carried out in respect of Jersey; and (ii) the type of customers, business relationships, products and transactions carried out with which the relevant person's business is concerned.*

~~87.~~88. *Article 11(3) lists a number of policies and procedures that must be established and maintained.*

~~88.~~89. *Article 11(9) of the Money Laundering Order requires a relevant person to take appropriate measures for the purpose of making employees whose duties relate to the provision of financial services (**relevant employees**) aware of policies and procedures under Article 11(1) and of legislation in Jersey to counter money laundering and the financing of terrorism. Article 11(10) of the Money Laundering Order requires a relevant person to provide relevant employees with training in the recognition and handling of transactions carried out by or on behalf of persons who are, or appear to be, engaged in money laundering or financing terrorism.*

~~89.~~90. *Article 11(11) of the Money Laundering Order requires a relevant person to establish and maintain policies and procedures for: (i) monitoring compliance with, and testing the effectiveness of, its policies and procedures; and (ii) monitoring and testing the effectiveness of measures to promote awareness and training of relevant employees.*

~~90.~~91. *When considering the type and extent of testing to be carried out under Article 11(11) of the Money Laundering Order, Article 11(12) requires a relevant person to have regard to the risk of money laundering or the financing of terrorism and matters that have an impact on that risk, such as the size and structure of the relevant person.*

~~91.~~92. *Article 11(8) of the Money Laundering Order requires that a relevant person operating through branches or subsidiaries, which carry on financial services business, must communicate its policies and procedures, maintained in accordance with Article 11(1), to those branches or subsidiaries. In addition, Article 11A requires group programmes for information sharing (see Section 2.7).*

AML/CFT Codes of Practice

~~92.~~93. A firm must establish and maintain appropriate and consistent *systems and controls* to prevent and detect money laundering and the *financing of terrorism*, that enable it to:

- apply the *policies and procedures* referred to in Article 11 of the *Money Laundering Order*;
- apply *CDD* measures – in line with Sections 3 to 7;
- report to the Joint Financial Crimes Unit (the ***JFCU***) when it knows, suspects or has reasonable grounds to know or suspect that another person is involved in *money laundering* or *the financing of terrorism*, including attempted transactions (in line with Section 8 of this Handbook);
- adequately screen *relevant employee*s when they are initially employed, make employees aware of certain matters and provide training - in line with Section 9 of this Handbook;
- keep complete records that may be accessed on a timely basis - in line with Section 10 of this Handbook);
- liaise closely with the *Commission* and the *JFCU* on matters concerning vigilance, *systems and controls* (including *policies and procedures*);
- communicate *policies and procedures* to overseas branches and subsidiaries, and monitor compliance therewith; and
- monitor and review instances where exemptions are granted to *policies and procedures*, or where controls are overridden.

~~93.~~94. In addition to those listed in Article 11(3) of the *Money Laundering Order*, a firm's *policies and procedures* must include *policies and procedures* for:

- client acceptance (and rejection), including approval levels for higher risk clients;
- the use of transactions limits and management approval for higher risk clients;
- placing reliance on *obliged person*s;
- applying exemptions from customer due diligence requirements under Part 3A of the *Money Laundering Order* and enhanced *CDD* measures under Articles 15, 15A and 15B;
- keeping documents, data or information obtained under *identifications measures* up to date and relevant, including changes in beneficial ownership and control;
- taking action in response to notices highlighting countries and territories in relation to which the *FATF* has called for the application of countermeasures or enhanced *CDD* measures; and
- taking action to comply with *Terrorist Sanctions Measures* and the *Directions Law*.

~~94.~~95. In maintaining the required *systems and controls* (including *policies and procedures*), a firm must check that the *systems and controls* (including *policies and procedures*) are operating effectively and test that they are complied with.

Guidance Notes

~~95.~~96. Whilst the *Money Laundering Order*, and consequently this Handbook, only brings within its scope the business activities of law firms where they are carrying on Schedule 2 business, the primary *money laundering* legislation and the general offences and penalties cover all persons and all business activities within Jersey. Consequently, law firms undertaking a significant proportion of Schedule 2 business may wish to consider applying the *systems and controls* to counter *money laundering* and the *financing of terrorism* across the whole of their business activities.

2.4.1 Effectiveness of Systems and Controls

Guidance Notes

~~96.~~97. A law firm may demonstrate that it checks that *systems and controls* (including *policies and procedures*) are adequate and operating effectively where senior management periodically considers the efficacy (capacity to have the desired outcome) of those *systems and controls* (including *policies and procedures*, and those in place at branches and in respect of subsidiaries) in light of:

- changes to its business activities or business risk assessment;
- information published from time to time by the *Commission* or *JFCU*, e.g. findings of supervisory and themed examinations and typologies;
- changes made or proposed in respect of new legislation, *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law* or guidance;
- resources available to comply with the *money laundering* legislation, the *Money Laundering Order* and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law*, in particular resources provided to the *MLCO* and *MLRO*, to apply enhanced *CDD* measures and to scrutinise transactions.

~~97.~~98. A law firm may demonstrate that it checks that *systems and controls* (including *policies and procedures*) are operating effectively where senior management periodically considers the effect of those *systems and controls* (including *policies and procedures*, and those in place at branches and in respect of subsidiaries) in lights of the information that is available to it, including:

- reports presented by the *MLCO* and others (e.g., where appropriate, risk management and internal audit functions) on compliance matters and *MLRO* on reporting;
- reports summarising findings from supervisory and themed examinations and action taken or being taken to address recommendations;
- the number and percentage of clients that have been assessed by the law firm as presenting a higher risk;
- the number of applications to establish business relationships or carry-out one-off transactions declined due to *CDD* issues, along with reasons;
- the number of business relationships terminated due to *CDD* issues, along with reasons;

- the number of "existing clients" that have still to be remediated under Section 4.7.2 of this Handbook;
- details of failures by an *obliged person* or client to provide information and evidence on demand and without delay under Articles 16, 16A and 17 B-D of the *Money Laundering Order* and action taken;
- the number of alerts generated by automated ongoing monitoring systems;
- the number of internal *SAR*s made to the *MLRO* (or *deputy MLRO*), the number of subsequent external *SAR*s submitted to the *JFCU*, and the timelines of reporting (by business area if appropriate);
- inquiries made by the *JFCU*, or production orders received, without issues having previously beening identified by *CDD* or reporting *policies and procedures*, along with reasons;
- results of testing awareness of *relevant employee*s with *policies and procedures* and legislation;
- the number and scope of exemptions granted to *policies and procedures*, including at branches and subsidiaries, along with reasons.

98.99. The level of *systems and controls*, and the extent to which monitoring needs to take place will be affected by:

- the firm's size;
- the nature and scale of its practice; and
- its overall risk profile.

99.100. Issues which may be covered in *systems and controls* include:

- the level of personnel permitted to exercise discretion on the risk-based application of the *Money Laundering Order* and this Handbook, and under what circumstances;
- *CDD* requirements to be met for simplified, standard and enhanced due diligence;
- when outsourcing of *CDD* obligations or reliance on third parties will be permitted, and on what conditions;
- how the firm will restrict work being conducted on a file where *CDD* has not been completed;
- the circumstances in which delayed *CDD* is permitted;
- when cash payments will be accepted;
- when payments will be accepted from or made to third parties;
- the manner in which disclosures are to be made to the *MLRO*; and
- the firm's policy for applying legal professional privilege (see Section 8.8 of this Handbook).

2.4.2 Testing of Compliance with Systems and Controls

Guidance Notes

~~100.~~101. A law firm may demonstrate that it has tested compliance with *systems and controls* (including *policies and procedures*) where senior management periodically considers the means by which compliance with its *systems and controls* (including *policies and procedures*) has been monitored compliance deficiencies identified and details of action taken or proposed to address any such deficiencies.

~~101.~~102. A law firm may demonstrate that it has tested compliance with *systems and controls* (including *policies and procedures*) where testing covers all of the *policies and procedures* maintained in line with Article 11(1) of the *Money Laundering Order* and paragraph 94~~100~~ above, and in particular:

- the application of simplified and enhanced *CDD* measures;
- reliance placed on *obliged person*s under Article 16 of the *Money Laundering Order*;
- action taken in response to notices highlighting countries and territories in relation to which the *FATF* has called for the application of countermeasures or enhanced *CDD* measures;
- action taken to comply with *Terrorist Sanctions Measures* and the *Directions Law*;
- the number or type of employees who have received training, the methods of training and the nature of any significant issues arising from the training.

2.4.3 Consideration of Cultural Barriers

Overview

~~102.~~103. The implementation of *systems and controls* (including *policies and procedures*) for the prevention and detection of *money laundering* and the *financing of terrorism* does not obviate the need for a firm to address cultural barriers that can prevent effective control. Human factors, such as the inter-relationships between different employees, and between employees and clients, can result in the creation of damaging barriers.

~~103.~~104. Unlike *systems and controls* (including *policies and procedures*), the prevailing culture of an organisation is intangible. As a result, its impact on the firm can sometimes be difficult to measure.

Guidance Notes

~~104.~~105. A firm may demonstrate that it has considered whether cultural barriers might hinder the effective operation of *systems and controls* (including *policies and procedures*) to prevent and detect *money laundering* and the *financing of terrorism* where senior management considers the prevalence of the following factors:

- an unwillingness on the part of fee earners or other employees to subject high value (and therefore important) clients to effective CDD measures for commercial reasons;
- pressure applied by senior management or fee earners outside Jersey upon employees in Jersey to transact without first conducting all relevant *CDD*;
- undue influence exerted by relatively large clients in order to circumvent *CDD* measures;

- excessive pressure applied on fee earners to meet aggressive revenue-based targets, or where employee or fee earner remuneration or bonus schemes are exclusively linked to revenue-based targets;
- an excessive desire on the part of fee earners to provide a confidential and efficient client service;
- design of the client risk classification system in a way that avoids rating any customer as presenting higher risk;
- the inability of employees to understand the commercial rationale for client relationships, resulting in a failure to identify non-commercial and therefore potential *money laundering* and the *financing of terrorism* activity;
- negative handling by senior management or fee earners of queries raised by more junior employees regarding unusual, complex or higher risk activity and transactions;
- an assumption on the part of more junior employees that their concerns or suspicions are of no consequence;
- a tendency for management to discourage employees from raising concerns due to lack of time and/or resources, preventing any such concerns from being addressed satisfactorily;
- dismissal of information concerning allegations of activities on the grounds that the client has not been successfully prosecuted or lack of public information to verify the veracity of allegations;
- the familiarity of fee earners or other employees with certain clients resulting in unusual, complex, or higher risk activity and transactions within such relationships not being identified as such;
- little weight or significance is attributed to the role of the *MLCO* or *MLRO*, and little co-operation between these post-holders and client-facing employees;
- actual practices applied by employees do not align with *policies and procedures*;
- employee feedback on problems encountered applying *policies and procedures* are ignored;
- non-attendance of partners or other members of management at training sessions on the basis of mistaken belief that they cannot learn anything new or because they have too many other competing demands on their time.

2.4.4 Outsourcing

Overview

~~105.~~106. In a case where a firm outsources a particular activity, it bears the ultimate responsibility for the duties undertaken in its name. This will include the requirement to ensure that the external party has in place satisfactory *systems and controls* (including *policies and procedures*), and that those *systems and controls* (including *policies and procedures*) are kept up to date to reflect changes in requirements.

~~106.~~107. Depending on the nature and size of a firm, the roles of *MLCO* and *MLRO* may require additional support and resources. Where a firm elects to bring in additional support, or to delegate areas of the *MLCO* or *MLRO* functions to external parties, the *MLCO* or *MLRO* will remain directly responsible for the respective roles, and senior management will remain responsible for overall compliance with the *money laundering* legislation and the *Money Laundering Order* (and by extension, also this Handbook).

AML/CFT Codes of Practice

~~107.~~108. A firm must consider the effect that outsourcing has on *money laundering* and the *financing of terrorism* risk, in particular where a *MLCO* or *MLRO* is provided with additional support from other parties, either from within group or externally.

~~108.~~109. A firm must assess possible *money laundering* or the *financing of terrorism* risk associated with outsourced functions, record its assessment, and monitor any risk on an on-going basis.

~~109.~~110. Where an outsourced activity is a financial services or Schedule 2 activity, then a firm must ensure that the provider of the outsourced services has in place *policies and procedures* that are consistent with those required under the *Money Laundering Order* and, by association, this Handbook.

~~110.~~111. In particular, a firm must ensure that knowledge, suspicion, or reasonable grounds for knowledge or suspicion of *money laundering* or *the financing of terrorism* activity are reported by the third party to the firm's *MLRO* (or *deputy MLRO*).

2.5 The Money Laundering Compliance Officer (MLCO)

Overview

~~111.~~112. The *Money Laundering Order* requires a firm to appoint an individual as *MLCO*, and tasks that individual with the function of monitoring its compliance with legislation in Jersey relating to *money laundering* and *the financing of terrorism* and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law*, and reporting thereon to senior management. The objective of this requirement is to require firms to clearly demonstrate the means by which they ensure compliance with the requirements of the same.

~~112.~~113. The *Money Laundering Order* also requires a firm to maintain adequate procedures for: (i) monitoring compliance with, and testing the effectiveness of, *policies and procedures*; and (ii) monitoring and testing the effectiveness of measures to raise awareness and training. When considering the type and extent of compliance testing to be carried out, a firm shall have regard to the risk of *money laundering* and *the financing of terrorism* and matters that have an impact on risk, such as size and structure of the firm's business.

~~113.~~114. The *MLCO* may have a functional reporting line, e.g. to a group compliance function.

~~114.~~115. The *Money Laundering Order* does not rule out the possibility that the *MLCO* may also have other responsibilities. To the extent that the *MLCO* is also **responsible** for the development of *systems and controls* (including *policies and procedures*) as well as monitoring subsequent compliance with those *systems and controls* (including *policies and procedures*), some additional independent assessment of compliance will be needed from time to time to address this potential conflict. Such an independent assessment is unlikely to be needed where the role of the *MLCO* is limited to actively monitoring the development and implementation of such *systems and controls*.

~~On 4 February 2008 (subsequently updated on 26 January 2009), the *Commission* issued a Notice under Article 10 of the *Money Laundering Order*. As a result of this notice, a firm that is not also a *regulated person* is not required to give the *Commission* written notice of the appointment, or termination, of its *MLCO*.~~

Statutory Requirements

~~115.~~116. *Article 7 of the Money Laundering Order requires a relevant person to appoint a MLCO to monitor whether the enactments in Jersey relating to money laundering and the financing of terrorism and AML/CFT Codes of Practice are being complied with. The same person may be appointed as both MLCO and MLRO.*

~~116.~~117. *Article 7(2A) of the Money Laundering Order requires a relevant person to ensure that the individual appointed is of an appropriate level of seniority and has timely access to all records that are necessary or expedient.*

~~117.~~118. *Article 7(6) of the Money Laundering Order requires a relevant person to notify the Commission in writing within one month when a person is approved as, or ceases to be a MLCO. However, Article 10 provides that the Commission may grant exemptions from this notification requirement by way of notice.*

AML/CFT Codes of Practice

~~118.~~119. A law firm must appoint a *MLCO* that:

- is employed by the firm;
- is based in Jersey; and
- has sufficient experience and skills.

~~119.~~120. A law firm must ensure that the *MLCO*;

- has appropriate independence, in particular from client-facing, business development and system and control development roles;
- reports regularly and directly to senior management and has a sufficient level of authority within the firm so that the senior management reacts to and acts upon reports made by the *MLCO*;
- has sufficient resources, including sufficient time and (if appropriate) a deputy *MLCO* and compliance support staff; and
- is fully aware of both their and the firm's obligations under the *money laundering* legislation, the *Money Laundering Order* and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law*.

~~120.~~121. In the event that the position of *MLCO* is expected to fall vacant, to comply with the statutory requirement to have an individual appointed to the office of *MLCO* at all times, a firm must take action to appoint an appropriate member of senior management to the position on a temporary basis.

~~121.~~122. If temporary circumstances arise where the firm has a limited or inexperienced compliance resource, it must ensure that this resource is supported as necessary.

~~122.~~123. When considering whether it is appropriate to appoint the same person as *MLCO* and *MLRO*, a firm must have regard to:

- the respective demands of the two roles, taking into account the size and nature of the firm's activities; and
- whether the individual will have sufficient time and resources to fulfil both roles effectively.

Guidance Notes

~~123.~~124. A firm may demonstrate that its *MLCO* is monitoring whether enactments and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law* are being complied with where he or she:

- regularly monitors and tests compliance with *systems and controls* (including *policies and procedures*) in place to prevent and detect *money laundering* and *the financing of terrorism* – supported as necessary by a compliance or internal audit function;
- reports periodically, as appropriate, to senior management on compliance with the firm's *systems and controls* (including *policies and procedures*) and issues that need to be brought to its attention; and
- responds promptly to requests for information made by the *Commission* and the *JFCU*.

~~124.~~125. In a case where the *MLCO* is also **responsible** for the development of *systems and controls* (including *policies and procedures*) in line with evolving requirements, a firm may demonstrate that the *MLCO* has appropriate independence where such *systems and controls* are subject to periodic independent scrutiny.

2.6 The Money Laundering Reporting Officer (MLRO)

Overview

~~125.~~126. Whilst the *Money Laundering Order* requires one individual to be appointed as *MLRO*, it recognises that, given the size and complexity of operations of many firms, it may be appropriate to designate additional persons (***deputy MLROs***) to whom *SAR*s may be made.

~~On 4 February 2008 (subsequently updated on 26 January 2009), the *Commission* issued a Notice under Article 10 of the *Money Laundering Order*. As a result of this notice, a firm that is not also a *regulated person* is not required to give the *Commission* written notice of the appointment, or termination of appointment, of its *MLRO*.~~

Statutory Requirements

~~126.~~127. *Article 8 of the Money Laundering Order requires a firm to appoint a MLRO. The MLRO's function is to receive and consider internal SARs in accordance with internal reporting procedures. The same person may be appointed as both MLCO and MLRO.*

~~127.~~128. *Article 8(2A) of the Money Laundering Order requires a relevant person to ensure that the individual appointed is of an appropriate level of seniority and has timely access to all records that are necessary or expedient.*

~~128.~~129. *Article 8(4) of the Money Laundering Order requires a relevant person to notify the Commission in writing within one month when a person is appointed as, or ceases to be a MLRO. However, Article 10 provides that the Commission may grant exemptions from this notification requirement by way of notice.*

~~129.~~130. *Article 9 of the Money Laundering Order allows a relevant person to designate one or more persons (deputy MLROs), in addition to the MLRO, to whom internal SARs may be made.*

AML/CFT Codes of Practice

~~130.~~131. A firm must appoint a *MLRO* that:

- is employed by the firm;

- is based in Jersey; and
- has sufficient experience and skills.

~~131.~~132. A firm must ensure that the *MLRO*:

- has appropriate independence, in particular from client-facing and business development roles;
- has a sufficient level of authority within the firm;
- has sufficient resources, including sufficient time, and (if appropriate) is supported by *deputy MLRO*s;
- is able to raise issues directly with senior management;
- maintains a record of all enquiries received from law enforcement authorities and records relating to all internal and external suspicious activity reports (see Section 10 of this Handbook);
- is fully aware of both their and the business' obligations under the *money laundering* legislation and the *Money Laundering Order* (and by extension, also this Handbook);
- ensures that relationships are managed effectively post disclosure to avoid tipping-off any third parties; and
- acts as the liaison point with the *Commission* and the *JFCU* and in any other third party enquiries in relation to *money laundering* or the *financing of terrorism*.

~~132.~~133. Where a firm has appointed one or more *deputy MLRO*s, it must ensure that the requirements set out above for the *MLRO* are also applied to any *deputy MLRO*s.

~~133.~~134. Where a firm has appointed one or more *deputy MLRO*s, it must ensure that the *MLRO*:

- keeps a record of all *deputy MLRO*s;
- provides support to, and routinely monitors the performance of, each *deputy MLRO*; and
- considers and determines that *SAR*s are being handled in an appropriate and consistent manner.

~~134.~~135. In the event that the position of *MLRO* is expected to fall vacant, to comply with the statutory requirement to have an individual appointed to the office of *MLRO* at all times, a firm must take action to appoint an appropriate member of senior management to the position on a temporary basis.

~~135.~~136. If temporary circumstances arise where a firm has a limited or inexperienced reporting resource, the firm must ensure that this resource is supported as necessary.

Guidance Notes

~~136.~~137. A firm may demonstrate that its *MLRO* (and any *deputy MLRO*) is receiving and considering *SAR*s in accordance with Article 21 of the *Money Laundering Order* where, inter alia, its *MLRO*:

- maintains a record of all requests for information from law enforcement authorities and records relating to all internal and external *SAR*s (Section 8);

- manages relationships effectively post disclosure to avoid tipping off any external parties; and
- acts as the liaison point with the *Commission* and the *JFCU* and in any other external party enquiries in relation to *money laundering* or *the financing of terrorism*.

~~137.~~138. A firm may demonstrate routine monitoring of the performance of any *deputy MLRO*s by requiring the *MLRO* to review:

- samples of records containing internal *SAR*s and supporting information and documentation;
- decisions of the *deputy MLRO* concerning whether to make an external *SAR*; and
- the bases for decisions taken.

2.7 Financial Groups

Overview

~~138.~~139. A Financial Group of which a firm is a member must maintain a group programme for the sharing of AML/CFT information. In addition, as explained in Section 1.4.3, where a company incorporated in Jersey carries on a *financial services business* through an overseas branch, it must comply with *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law* in respect of that business, irrespective of whether it also carries on *financial services business* in or from within Jersey.

~~139.~~140. As explained in Section 1.4.2 and 1.4.3, in practice, the above may not apply to all law firms carrying on Schedule 2 business on the basis that many~~all~~ law firms currently registered under the *Supervisory Bodies Law* are either sole practitioners or Jersey customary law partnerships (and therefore not legal persons).

Statutory Requirements

~~140.~~141. *Article 11A of the Money Laundering Order applies to a financial group of which a law firm is a member.*

~~141.~~142. *Article 11A of the Money Laundering Order requires a financial group to maintain a programme to prevent and detect money laundering and the financing of terrorism that includes:*

- policies and procedures by which a law firm within a financial group, which carries on financial services business or equivalent business, may disclose information to a member of the same financial group, but only where such disclosure is appropriate for the purpose of preventing and detecting money laundering or managing money laundering risks;

- adequate safeguards for the confidentiality and use of any such information;
- the monitoring and management of compliance with, and the internal communication of, such policies and procedures (including the appointment of a compliance officer for the financial group); and
- the screening of employees.

~~142.~~143. Under Article 11A(3) of the Money Laundering Order "information" includes the following:

- information or evidence obtained from applying identification measures;
- customer, account and transaction information; and
- information relating to the analysis of transactions or activities that are considered unusual.

AML/CFT Codes of Practice

~~143.~~144. A person that is a Jersey incorporated company must ensure that any subsidiary applies measures that are at least equivalent to *AML/CFT Codes of Practice* in respect of any *financial services business* carried on outside Jersey by that subsidiary.

~~144.~~145. A person who:

- is a legal person registered, incorporated or otherwise established under Jersey law, but who is not a Jersey incorporated company; and
- carries on a *financial services business* in or from within Jersey,

must apply measures that are at least equivalent to *AML/CFT Codes of Practice* in respect of any *financial services business* carried on by that person through an overseas branch/office.

~~145.~~146. Where overseas legislation prohibits compliance with an *AML/CFT* Code (or measures that are at least equivalent) then the *AML/CFT* Codes do not apply and the *Commission* must be informed that this is the case. In such circumstances, a firm must take other reasonable steps to effectively deal with the risk of *money laundering* and *the financing of terrorism*.