

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 by 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 business risks managed. For those 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 accountancy 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 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 trader¹.
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 *systems and controls*, training and awareness; and
 - › the appointment of a Money Laundering Compliance Officer (**MLCO**) and Money Laundering Reporting Officer (**MLRO**).
5. This Handbook describes the requirements for a 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 firm as its “**policies and procedures**”.

2.2 Measures to Prevent Money Laundering and the 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, a director or manager or officer 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 or compliance 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 whose duties relate to the provision of relevant services 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 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 (see Section 2.3.1 below).

Moved (insertion) [1]

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 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.

Moved up [1]: <#>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 (see Section 2.3.1 below).¶

2.3.1 Business Risk Assessment

AML/CFT Codes of Practice

1. A firm 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. Professional firms are likely to already have in place *policies and procedures* to minimise professional, client and legal risk. A firm may extend its existing risk management systems to address *AML/CFT* 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. 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 the *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 its 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 and 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 the *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 persons* 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 clients.
24. In developing a risk-based approach, firms need to ensure that it is readily comprehensible to senior management, other *relevant employees* and relevant third parties e.g. *auditors* and the *Commission*.
25. In the case of a 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 Client and Service Risks to the Business

Overview

26. The business risk assessment relating to clients and services will depend on the firm's size, type of clients and the practice area it engages in.
27. Firms should consider the different types of risk to which they are exposed within the different service areas as set out below. The risks should be considered within the context that a firm may be used to launder funds or assets through the firm or, alternatively, that the client or its counterparties may launder criminal funds or assets, but in a way that does not touch the accountancy firm.

Accountancy, Audit and Insolvency Service Risk

28. Those providing accountancy, auditing or *insolvency services* will primarily need to consider their business risk assessment in respect of the nature of their client base, the business sectors in which their clients operate and the geographical location of their clients. The standing of clients and adherence to sound corporate governance principles will also have an impact including those clients that have previously been prosecuted or fined for criminal or regulatory offences.
29. The business risk assessment should take account of the following risks:
 - › setting up, winding up, or effecting recovery for high cash turnover businesses for clients which may provide a front for criminal money;
 - › being used in an active sense to launder money through the handling of cash or assets or through payments that are made to, or received from, third parties, particularly with a cross-border element;
 - › becoming concerned in an arrangement which facilitates *money laundering* through the provision of investment services;
 - › becoming a party to serious fraud on the part of senior management or failing to recognise the warning signs relating to management fraud; and
 - › the potential for *money laundering* and the *financing of terrorism* attaching to the client and/or those who trade with or otherwise interact with clients.
 - › Those providing *accountancy services* should also consider the risks when:
 - providing assistance in setting up trusts or company structures which could be used to obscure beneficial ownership of monies and assets settled into trust; and
 - handling the financial affairs, or setting up companies, trusts or other structures for politically exposed persons whose assets and wealth may be derived from the proceeds of corruption (see Section 7.6 of this Handbook).
30. Specialisation within a sector that undertakes higher risk activity from a *money laundering* and the *financing of terrorism* perspective will affect the business risk assessment. Examples of higher risk sectors and sensitive business areas for *money laundering* and the *financing of terrorism* purposes are:
 - › financial services and money services businesses;
 - › high cash turnover businesses: bars and clubs, taxi firms, launderettes, takeaway restaurants, market traders;
 - › gaming and gambling businesses;
 - › real estate and construction;
 - › computers and high technology, telecommunications and mobile phone businesses; and
 - › arms and armaments.
31. Firms such as *financial services businesses*, money services businesses and estate agents that are covered by the *Money Laundering Order* should have taken steps to mitigate their risks by implementing robust internal controls.

Taxation Service Risk

32. Tax practitioners are not required to be experts in criminal law, but they are expected to be aware of the offences which can give rise to the proceeds of crime. For example, the boundaries between deliberate understatement or other tax evasion and simple cases of error or genuine differences in the interpretation of tax law. The main areas where offences may arise which might enhance the risks of the tax practitioner becoming concerned in an arrangement are:
- › tax evasion, including making false returns (including supporting documents), accounts or financial statements or deliberate failure to submit returns;
 - › deliberate refusal to correct known errors;
 - › fraudulent or dishonest conduct; and
 - › fraudulent evasion of Value Added Tax (**VAT**) by clients operating within the European Union including the possession and dealing in goods on which VAT has been evaded (e.g. Missing Trader Intra Community/Carousel fraud).

2.4 Adequate and Effective Systems and Controls

Overview

33. 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

34. *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.*
35. *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.*
36. *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 with which the relevant person's business is concerned.*
37. *Article 11(3) lists a number of policies and procedures that must be established and maintained.*
38. *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 whose duties relate to the provision of financial services 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.*

39. 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.
40. When considering the type and extent of testing to be carried out under Article 11(11), Article 11(12) of the Money Laundering Order 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.
41. Article 11(8) 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

42. 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 employees* 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.
43. 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 transaction limits and management approval for higher risk clients;
 - › placing reliance on *obliged persons*;
 - › 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 *identification 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*.
44. 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

45. Whilst the *Money Laundering Order*, and consequently this Handbook, only brings within its scope the business activities of 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, firms 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, regardless of whether they are defined as Schedule 2 business.

2.4.1 Effectiveness of Systems and Controls

Guidance Notes

46. A 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.
47. A 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 light 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 the *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 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;
 - › details of failures by an *obliged person* or client to provide information and evidence on demand and without delay under Articles 16, 16A and 17B-D of the *Money Laundering Order* and action taken;
 - › the number of alerts generated by automated ongoing monitoring systems;
 - › the number of internal *SARs* made to the *MLRO* (or *deputy MLRO*), the number of subsequent external *SARs* 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 been identified by *CDD* or reporting *policies and procedures*, along with reasons;
 - › results of testing awareness of *relevant employees* 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.
48. 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, scale and complexity of its operations;
 - › the number of different business types it is involved in;
 - › the types of services it offers and how it sells those services;
 - › the type of business transactions it becomes involved in or advises on; and
 - › its overall risk profile.
49. 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 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, including payment of fees, will be accepted from, or made to, third parties; and
- › the manner in which disclosures are to be made to the *MLRO*.

2.4.2 Testing of Compliance with Systems and Controls

Guidance Notes

50. A 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.
51. A 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 50 above, and in particular:
- › the application of simplified and enhanced *CDD* measures;
 - › reliance placed on *obliged persons* 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

52. 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.
53. 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

54. 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 client due diligence;
 - › 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 employees to provide a confidential and efficient client service;
- › design of the client risk classification system in a way that avoids rating any client 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 criminal activities on the grounds that the customer 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 cooperation between these post-holders and customer-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; and
- › non-attendance of senior 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

55. 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 to ensure that those *systems and controls* (including *policies and procedures*) are kept up to date to reflect changes in requirements.
56. 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, this Handbook).

AML/CFT Codes of Practice

57. 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.
58. 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.
59. Where an outsourced activity is a financial services or Schedule 2 activity, 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.
60. In particular, a firm must ensure that knowledge, suspicion, or reasonable grounds for knowledge or suspicion of *money laundering* or financing 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

61. The Money Laundering Order requires a firm to appoint an individual as *MLCO*, and task 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.
62. 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.
63. The *MLCO* may have a functional reporting line, e.g. to a group compliance function.
64. 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* (and *policies and procedures*) as well as monitoring subsequent compliance with those *systems and controls* (and *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*.

Statutory Requirements

65. *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.*
66. *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.*

67. *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

68. A firm must appoint a *MLCO* that:
- › is employed by the firm;
 - › is based in Jersey;
 - › has sufficient experience and skills.
69. A 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 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 and the *Money Laundering Order* and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law*.
70. 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.
71. If temporary circumstances arise where the firm has a limited or inexperienced compliance resource, it must ensure that this resource is supported as necessary.
72. 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

73. 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*.

2.6 The Money Laundering Reporting Officer (MLRO)

Overview

74. 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 *SARs* may be made.

Statutory Requirements

75. *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.*
76. *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.*
77. *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.*
78. *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

79. A firm must appoint a *MLRO* that:
- › is employed by the firm;
 - › is based in Jersey; and
 - › has sufficient experience and skills.
80. 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 MLROs*;
 - › 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;
 - › is fully aware of both *his* 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*;
 - › 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*.
81. Where a firm has appointed one or more *deputy MLROs*, it must ensure that the requirements set out above for the *MLRO* are also applied to any *deputy MLROs*.

82. Where a firm has appointed one or more *deputy MLROs*, it must ensure that the *MLRO*:
- › keeps a record of all *deputy MLROs*;
 - › provides support to and routinely monitors the performance of each *deputy MLRO*; and
 - › considers and determines that *SARs* are being handled in an appropriate and consistent manner.
83. 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.
84. If temporary circumstances arise where a firm has a limited or inexperienced *money laundering* reporting resource, the firm must ensure that this resource is supported as necessary.

Guidance Notes

85. A firm may demonstrate that its *MLRO* (and any *deputy MLRO*) is receiving and considering *SARs* 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 *SARs* (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 enquiries in relation to *money laundering* or the *financing of terrorism*.
86. A firm may demonstrate routine monitoring of the performance of any *deputy MLROs* by requiring the *MLRO* to review:
- › samples of records containing internal *SARs* 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

87. 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.

Statutory Requirements

88. *Article 11A of the Money Laundering Order applies to a financial group of which a relevant person is a member.*
89. *Article 11A (2) 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 relevant person 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 risk;*
 - › *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*
90. 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;*
 - › *information relating to the analysis of transactions or activities that are considered unusual.*

AML/CFT Codes of Practice

91. 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.
92. 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.
93. Where overseas legislation prohibits compliance with an *AML/CFT Code of Practice* (or measures that are at least equivalent) then the *AML/CFT Codes of Practice* 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*.