2 CORPORATE GOVERNANCE

2.1 Overview of section

1. Corporate governance is the system by which enterprises are directed and controlled and their risks managed. For supervised persons, money laundering and the financing of terrorism are risks that must be managed in the same way as other business risks.
2. Under the general heading of corporate governance, this section considers:
   - › board responsibilities for the prevention and detection of *money laundering* and the *financing of terrorism*
   - › requirements for systems and controls, training and awareness
   - › the appointment of a ***MLCO*** and ***MLRO***.
3. The *AML/CFT Handbook* describes a *supervised person's* general framework to combat *money laundering* and the *financing of terrorism* as its *systems and controls*. The *AML/CFT Handbook* refers to the way in which those systems and controls are implemented into the day-to-day operation of a *supervised person* as its *policies and procedures*.
4. Where a *supervised person* is not a company but is, for example, a partnership, references in this section to "the Board" should be read as meaning the senior management function of that person, including the Board of a legal arrangement's governing body. In the case of a *sole trader*, "the Board" will be the *sole trader*. In the case of an overseas company carrying on a *supervised business* in Jersey through a branch, "the Board" should be read as including the local management function of that branch in Jersey.

2.2 Measures to prevent money laundering and the financing of terrorism

Statutory requirements (paraphrased wording)

5. *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 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.*
6. *Article 37 enables the Minister for External Relations and Financial Services to prescribe by Order the measures that must be taken (including measures not to be taken) by a relevant person. These measures are established in the Money Laundering Order.*

2.3 Board responsibilities

Overview

7. The key responsibilities of the Board, set out in further detail below, are to:
   - › identify the supervised person'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 fulfilling these responsibilities.

8. The Board is assisted in fulfilling these responsibilities by a *MLCO* and *MLRO*. Larger or more complex *supervised persons* 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 (paraphrased wording)

9. *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.*

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

11. *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

12. The Board must conduct and record a business risk assessment in respect of the *supervised person*. In particular, the Board must consider, on an on-going basis, the *supervised person's* risk appetite and the extent of the *supervised person's* exposure to *money laundering* and the *financing of terrorism* risks "in the round" or as a whole by reference to the *supervised person's* organisational structure, *customers*, the countries and territories with which those *customers* are connected, the products and services the *supervised person* provides and how those products and services are delivered. The assessment must consider the cumulative effect of risks identified, which may exceed the sum of each individual risk element. The Board's assessment must be kept up to date. (See Section 2.3.1).

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

14. Taking into account the conclusions of the business risk assessment and strategy, the Board must:

› organise and control its affairs in a way that effectively mitigates the risks that it has identified, including areas that are complex; and

› 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).

15. The Board 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).

16. The Board 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).

17. The Board 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).

18. The Board must notify the *JFSC* immediately in writing of any material failures to comply with the requirements of the Money Laundering Order or the *AML/CFT Handbook*.

2.3.1 Business risk assessment

AML/CFT Codes of Practice

19. A *supervised 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

20. When considering a risk appetite for the supervised person's business, the Board may wish to examine the following factors (note the below list is not exhaustive):

    - are they prepared to accept only a certain proportion of business rated at each risk level? For example, the Board may only have an appetite for very high-risk customers to form 5% of their overall fee income or assets under management
    - are there any country connections or customer risk levels with which the Board are not prepared to engage?
    - how do the particular characteristics of the supervised person (e.g. business sector, type of products and services offered) potentially expose it to greater ML and/or TF risk?
    - has a national risk appetite been published by the Island of Jersey? What types of customers and activity are considered to be outside of the national risk appetite?

21. It is important for the risk appetite to be sufficiently clear so that the Board can articulate it when considering whether to establish a business relationship or carry out a one-off transaction with a customer. For example, it should not be so vague that it can be used to justify the acceptance of any business, no matter the risk level.

22. Equally, a clear risk appetite should not be wilfully ignored in order to, for example, accept business from a very high-risk customer who is offering an attractive fee proposition.

23. It is the responsibility of the Board to ensure that business relationships and one-off transactions are maintained in accordance with the agreed risk appetite.

24. A *supervised person* may extend its existing risk management systems to address *ML/TF* risks. The detail and sophistication of these systems will depend on the *supervised person's* size and the complexity of the business it undertakes. Ways of incorporating a *supervised person's* business risk assessment will be governed by the size of the *supervised person* and how regularly compliance staff and the Board are involved in day-to-day activities.

25. The Board of a *supervised person* may demonstrate that it has considered its exposure to *money laundering* and the *financing of terrorism* risk by:

    - involving all members of the Board 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. 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 customers are and what they do e.g. do its customers engage in higher-risk activities
- considering whether any additional risks are posed by the countries and territories with which its customers 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 characteristics of the products and services that it offers and assessing the associated vulnerabilities posed by each product and service. For example:
    - a. products that allow a *customer* to "pool" third party funds will tend to be more vulnerable - because of the anonymity provided by the co-mingling of assets or funds belonging to several third parties by the *customer*
    - b. products such as standard current accounts are more vulnerable because they allow payments to be made to and from external parties, including cash transactions
    - c. conversely, those products that do not permit external party transfers or where redemption is permitted only to an account from which the investment is funded will be less vulnerable
    - d. products and services which make use of new and developing technologies, such as virtual assets, may pose a risk due to the increased anonymity which can be afforded by the asset to their users. There may also be a lack of experience in providing these new products, meaning the control environment may not be as effective.
- considering the risk that is involved in placing reliance on *obliged persons* to apply *reliance identification measures*
- considering how it establishes and delivers products and services to its *customers*. For example, risks are likely to be greater where relationships may be established remotely (non-face to face), or may be controlled remotely by the *customer* (straight-through processing of transactions)
    - a supervised person may employ new and developing technologies to establish business relationships with their customers, for example through an E-ID application. As discussed further in Section 4.3.5 of this Handbook, the risks of using such technology to obtain evidence of identity should be considered, noting the particular characteristics of each application. This should be recorded in the Business Risk Assessment
- considering the accumulation of risk for more complex *customers*.

26. When conducting a business risk assessment care should be taken not to focus too much on any single factor. All factors (including those identified by a National Risk Assessment or similar), as well as the wider picture (and cumulative risk) should be considered.
27. Care should also be taken not to rely on a 'template' business risk assessment i.e. one previously prepared within the business or supplied by an external provider. The assessment should be customised to fully reflect and consider the unique types of customers serviced by the business, the geographical areas to which it has exposure, and the specific products and services provided by the business.
28. With reference to new and developing technologies, the Board should have a due diligence process in place to analyse and understand their risks, then apply a framework for how they will be monitored and managed going forward.
29. In developing a risk-based approach, *supervised persons* need to ensure that the Business Risk Assessment is readily comprehensible by the Board, other *relevant employees* and relevant third parties e.g. *auditors* and the *JFSC*.
30. In the case of a *supervised person* that is dynamic and growing, the Board 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 *supervised person* with stable products and services. In all cases, the Board 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.
31. When reviewing a business risk assessment, the Board should ensure it captures all relevant risks and considers how effective the business' control environment is at managing those risks. Effectiveness can be evidenced by considering the findings of control testing such as periodic reviews and reviewing data collected by the supervised person.
32. Where gaps or deficiencies are identified during a business risk assessment review, an action plan should be drawn up so they can be addressed. The action plan should form an integral part of the business risk assessment.
33. Where a *supervised person* is subject to a regulatory code of practice (such as the Trust Company Business Code of Practice) there is also an obligation for a wider, operational business risk assessment to be conducted. When preparing an *AML/CFT* business risk assessment or *customer* risk assessment, factors in this operational business risk assessment may be relevant. Therefore, a combined *AML/CFT* and operational business risk assessment may be appropriate.
34. Risks that are not normally considered to be specific *ML/TF* risks may also be relevant to an *AML/CFT* business risk assessment, such for example, credit risk, tax risk, investor eligibility risk, cyber security etc.
35. It is likely that the business risk assessment will be conducted by the *supervised person* prior to any *customer* risk assessment. When *a customer* risk assessment is prepared the business risk assessment may need to be updated (for example, to take into account new risk factors or the *supervised person's* changing risk tolerance/appetite).

2.4 Adequate and effective systems and controls

Overview

36. 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 *supervised person*.

Statutory requirements (paraphrased wording)

37. *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 financing of terrorism.*

38. *Parts 3, 3A, 4 and 5 of the Money Laundering Order set out the measures that are to be applied in respect of CDD, record-keeping and reporting.*

39. *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.*

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

41. *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 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.*

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

43. *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 financing of terrorism that exists in respect of the relevant person's business, and matters that have an impact on that risk, such as the size and structure of the relevant person.*

44. *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 2.8 of this Handbook).*

AML/CFT Codes of Practice

45. A *supervised person* 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 of this Handbook
- report to 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 JFSC and the JFCU on matters concerning vigilance, systems and controls (including policies and procedures)
- communicate policies and procedures to overseas branches and subsidiaries (subject to Article 10A(9) see section 1.4.2), and monitor compliance therewith and
- monitor and review instances where exemptions are granted to policies and procedures, or where controls are overridden.

46. In addition to those listed in Article 11(3) of the Money Laundering Order, a *supervised person's policies and procedures* must include *policies and procedures* for:
    - customer acceptance (and rejection), including approval levels for higher risk customers
    - the use of transaction limits and management approval for higher risk customers
    - 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
    - taking action to comply with *Terrorist Sanctions Measures* and the Directions Law.
47. In maintaining the required *systems and controls* (including *policies and procedures*), a *supervised person* must check that the *systems and controls* (including *policies and procedures*) are operating effectively and test that they are complied with.

2.4.1 Effectiveness of systems and controls

Guidance notes

48. A *supervised person* may demonstrate that it checks that *systems and controls* (including *policies and procedures*) are adequate and operating effectively where the Board 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 *JFSC* 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 *Anti-Money Laundering and Counter-Terrorism Legislation* 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.

49. A *supervised person* may demonstrate that it checks that *systems and controls* (including *policies and procedures*) are operating effectively where the Board 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 *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 *customers* that have been assessed by the *supervised person* as presenting a higher risk
- the number of applications to establish business relationships or carry-out one-off transactions which have been 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 *customers*" that have still to be remediated under Section 4.7.2 of this Handbook
- details of failures by an *obliged person* or *customer* 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 on-going 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 timeliness 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 of 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.

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

- the supervised person'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 delivers those services

- the type of business transactions it becomes involved in or advises on
- its overall risk profile.

51. Areas which are required under the *Money Laundering Order* to be covered in *systems and controls* include (but are not limited to):
    - the manner in which disclosures are to be made to the *MLRO*
    - the circumstances in which delayed *CDD* is permitted
    - when outsourcing of *CDD* obligations or reliance on third parties will be permitted, and on what conditions
    - *CDD* requirements to be met for simplified, standard and enhanced due diligence
    - how the *supervised person* will restrict work being conducted for a *customer* where *CDD* has not been completed
52. Issues which may also 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
    - when cash payments will be accepted
    - when payments will be accepted from or made to third parties
    - the *supervised person's* policy for applying legal professional privilege (*LPP*). Note that *LPP* is only applicable to lawyers – see Section 15.7.1 of this Handbook for specific guidance.

2.4.2 Testing of compliance with systems and controls

Guidance notes

53. A *supervised person* may demonstrate that it has tested compliance with *systems and controls* (including *policies and procedures*) where the Board 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.
54. A *supervised person* 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 the *AML/CFT Code of Practice* at paragraph 46 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*, and
    - 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

55. 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 remove the need for a *supervised person* to address cultural barriers that can prevent effective control. Human factors, such as the inter-relationships between different employees, and between employees and *customers*, can result in the creation of damaging barriers.

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

Guidance notes

57. A *supervised person* 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 the Board considers the prevalence of the following factors:

- an unwillingness on the part of employees to subject high value (and therefore important) *customers* to effective *CDD* measures for commercial reasons
- pressure applied by management or *customer* relationship managers outside Jersey upon employees in Jersey to transact without first conducting all relevant *CDD*
- undue influence exerted by relatively large *customers* in order to circumvent *CDD* measures
- excessive pressure applied on employees to meet aggressive revenue-based targets, or where employee or management 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 *customer* service
- design of the *customer* risk classification system in a way that avoids rating any *customer* as presenting a higher risk
- the inability of employees to understand the commercial rationale for business relationships, resulting in a failure to identify non-commercial and therefore potential *money laundering* and *financing of terrorism* activity
- negative handling by managerial staff 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 line managers 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 employees with certain *customers* resulting in unusual 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* is ignored
- non-attendance of senior employees at training sessions on the basis of a 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

58. In a case where a *supervised person* outsources a particular activity, it bears the ultimate responsibility for the duties undertaken in its name. This will include the requirement to determine 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. See the table below for details of which *CDD* activities may be outsourced.

<table>
<tr><th>CDD (always the ultimate responsibility of the supervised person)</th><th colspan="2">Activities which may be outsourced</th></tr>
<tr><td rowspan="7">Identification measures</td><td colspan="2">Risk assessment</td></tr>
<tr><td colspan="2">ID customer</td></tr>
<tr><td colspan="2">ID third parties</td></tr>
<tr><td>ID person acting for customer</td><td>Verify authority to act</td></tr>
<tr><td rowspan="2">Where customer not individual:</td><td>Understand ownership/control structure</td></tr>
<tr><td>ID beneficial owners/controllers</td></tr>
<tr><td colspan="2">Obtain information on purpose/nature</td></tr>
<tr><td rowspan="2">On-going monitoring</td><td colspan="2">Scrutinising transactions/activity</td></tr>
<tr><td colspan="2">Keep documents/information up-to-date</td></tr>
</table>

59. Depending on the nature and size of a *supervised person*, the roles of the *MLCO* and *MLRO* may require additional support and resourcing. Where a *supervised person* 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 their respective role, and the Board will remain responsible for overall compliance with the *Anti-Money Laundering and Counter-Terrorism Legislation* (and by extension, also this Handbook). Note that the *AML/CFT Codes of Practice* at Paragraphs 82 and 95 below provide that the role of the *MLCO* and *MLRO* must be undertaken by an employee of the *supervised person* based in Jersey, unless the specific circumstances set out in those paragraphs apply.

60. The JFSC has also issued an Outsourcing Policy and guidance note for *supervised persons*, which outlines its own set of requirements and obligations in respect of outsourcing.

AML/CFT Codes of Practice

61. All *supervised persons* must comply with the JFSC's Outsourcing Policy and guidance note.

62. A *supervised person* 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.

63. A *supervised person* 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.

64. Where an outsourced activity is a *supervised business* activity, then a *supervised person* must be satisfied 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.

65. In particular, a *supervised person* must be satisfied that knowledge, suspicion, or reasonable grounds for knowledge or suspicion of *money laundering* or *financing of terrorism* activity will be reported by the provider of the outsourced service to the *MLRO* (or *deputy MLRO*) of the *supervised person*.

2.5 Supervisory Risk Data Questionnaires

Overview

66. Since 2018, the JFSC has collected data from supervised persons on an annual basis in order to support our implementation of a risk-based approach to supervision. This includes:

- organisational/footprint data
- AML/CFT compliance data and
- data regarding a supervised person's customers.

67. This data is used in order to:

- improve our understanding of the activities undertaken by supervised persons and modify our risk-based approach accordingly and
- assist in the preparation of National Risk Assessments for Jersey.

68. To collect the above-referenced data, the JFSC will issue one or more Supervisory Risk Data Questionnaires (**Risk Questionnaires**) to supervised persons. The content of a Risk Questionnaire will differ based on the business sector of the supervised person. At the discretion of the JFSC, some sectors or parts thereof may not be included in a particular Risk Questionnaire exercise.

69. A set time period will be provided, by the end of which all supervised persons receiving a Risk Questionnaire are required to complete and return it to the JFSC.

AML/CFT Code of Practice

70. When in receipt of a Risk Questionnaire from the JFSC, a supervised person must complete and return said questionnaire by the deadline provided.

Guidance Notes

71. In order to prepare for a Risk Questionnaire, a supervised person may consider reviewing relevant guidance notes issued by the JFSC in previous data collection exercises. The supervised person can then update its systems and controls (including policies and procedures) so the required data is collected during the usual course of business.

72. For each data collection exercise, the JFSC will provide specific guidance on how to complete the Risk Questionnaire. This includes guidance for the organisational/footprint part of the questionnaire and the sector-specific parts. A supervised person should read the relevant guidance in full before completing a Risk Questionnaire.

73. A supervised person should consider storing the required data in a format which can be easily reviewed, extracted and transferred to a Risk Questionnaire. It may also be appropriate to ensure any supporting documentation which was used in completing a Risk Questionnaire can be easily accessed if required.

2.6 The Money Laundering Compliance Officer (MLCO)

Overview

74. The *Money Laundering Order* requires a *supervised person* 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. The objective of this requirement is to require *supervised persons* to clearly demonstrate the means by which they ensure compliance with the requirements of the same.

75. The Money Laundering Order also requires a *supervised person* to maintain adequate procedures for:

    a. monitoring compliance with, and testing the effectiveness of, *policies and procedures* and

    b. 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 *supervised person* 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 *supervised person's* business.

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

77. 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 (paraphrased wording)

78. *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 financing of terrorism and AML/CFT Codes of Practice are being complied with. The same person may be appointed as both MLCO and MLRO.*

79. *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.*

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

81. *Article 7 of the Money Laundering Order recognises that a relevant person that is also a regulated person may have notified the JFSC of the appointment or cessation of a MLCO under other legislation. If so, a duplicate notification is not required under the Money Laundering Order.*

AML/CFT Codes of Practice

82. A supervised person must appoint a MLCO that:

- is employed by the *supervised person* or an enterprise in the same financial group as the *supervised person*
  - In the case of a supervised person that: carries on the business of being a functionary, recognized fund, or unclassified fund or is a Category B insurance permit holder, a managed bank, or other managed entity; has no employees of its own; and is administered by a person carrying on a supervised business, it is acceptable for an employee of the administrator to be appointed by the supervised person as its MLCO
- is based in Jersey
  - In the case of a supervised person that is a Category A insurance business permit holder with no employees of its own in Jersey, it is acceptable to appoint an employee outside Jersey. In the case of a supervised person that is carrying on a money service business and has no employees of its own in Jersey, it is acceptable for the supervised person to appoint an employee outside Jersey as its MLCO, provided the employee is based in an equivalent jurisdiction; and
- has sufficient experience and skills.

83. A *supervised person* must ensure that the *MLCO*:

- has appropriate independence, in particular from *customer*-facing, business development and *systems and controls* development roles
- reports regularly and directly to the Board and has a sufficient level of authority within the *supervised person* so that the Board 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
- is fully aware of both their and the *supervised person's* obligations under the *Anti-Money Laundering and Counter-Terrorism Legislation* and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law*.

84. 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 supervised person must take action to appoint a member of the Board (or other appropriate member of senior management) to the position on a temporary basis.

85. If temporary circumstances arise where the supervised person has a limited or inexperienced money laundering compliance resource, it must ensure that this resource is supported as necessary.

86. When considering whether it is appropriate to appoint the same person as *MLCO* and *MLRO*, a *supervised person* must have regard to:

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

Guidance notes

87. A *supervised person* 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 they:

- regularly monitor and test 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
- report periodically, as appropriate, to the Board on compliance with the *supervised person's systems and controls* (including *policies and procedures*) and issues that need to be brought to its attention
- respond promptly to requests for information made by the *JFSC* and the *JFCU*.

88. 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 *supervised person* may demonstrate that the *MLCO* has appropriate independence where such *systems and controls* are subject to periodic independent scrutiny.

2.7 The Money Laundering Reporting Officer (MLRO)

Overview

89. 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 enterprises, it may be appropriate to designate additional persons (*deputy MLROs*) to whom *SARs* may be made.

Statutory requirements (paraphrased wording)

90. *Article 8 of the Money Laundering Order requires a relevant person 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.*

91. *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.*

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

93. *Article 8 of the Money Laundering Order recognises that a relevant person that is also a regulated person may have notified the JFSC of the appointment or cessation of a MLRO under other legislation. If so, a duplicate notification is not required under the Money Laundering Order.*

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

AML/CFT Codes of Practice

95. A *supervised person* must appoint a *MLRO* that:

- is employed by the *supervised person* or enterprise in the same financial group as the *supervised person*
  - In the case of a supervised person that: carries on the business of being a functionary, recognized fund, or unclassified fund, or is a Category B insurance permit holder, a managed bank, or other managed entity; has no employees of its own; and is administered by a person carrying on supervised business that is a supervised person, it is acceptable for an employee of the administrator to be appointed by the supervised person as its MLRO.
- is based in Jersey
  - In the case of a supervised person that is a Category A insurance business permit holder with no employees of its own in Jersey, it is acceptable to appoint an employee outside Jersey In the case of a supervised person that is carrying on a money service business and has no employees of its own in Jersey, it is acceptable for the supervised person to appoint an employee outside Jersey as its MLRO, provided the employee is based in an equivalent jurisdiction; and
- has sufficient experience and skills.

96. A *supervised person* must ensure that the *MLRO*:

- has appropriate independence, in particular from *customer*-facing and business development roles
- has a sufficient level of authority within the *supervised person*
- has sufficient resources, including sufficient time, and (if appropriate) is supported by *deputy MLROs*
- is able to raise issues directly with the Board, and
- is fully aware of both their and the supervised person's obligations under the Anti-Money Laundering and Counter-Terrorism Legislation and AML/issued under the Supervisory Bodies Law.

97. Where a *supervised person* has appointed one or more *deputy MLROs* the requirements set out above for the *MLRO* must also be applied to any *deputy MLROs*.

98. Where a *supervised person* 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*

- considers and determines that *SARs* are being handled in an appropriate and consistent manner.

99. 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 *supervised person* must take action to appoint a member of the Board (or other appropriate member of senior management) to the position on a temporary basis.

100. If temporary circumstances arise where a *supervised person* has a limited or inexperienced *money laundering* reporting resource, it must ensure that this resource is supported as necessary.

Guidance notes

101. A *supervised person* 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, among other things, its *MLRO*:

- maintains a record of all requests for information from law enforcement authorities and records relating to all internal and external *SARs* (see Section 8 of this Handbook)
- manages relationships effectively post disclosure to avoid tipping off any external parties
- acts as the liaison point with the *JFSC* and the *JFCU* and in any other external enquiries in relation to *money laundering* or the *financing of terrorism*.

102. A *supervised person* 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*
- the bases for decisions taken.

2.8 Financial groups

Overview

103. A *Financial Group* of which a *supervised person* is a member must maintain a group programme for the sharing of *AML/CFT* information.

104. In addition, as explained in Section 1.4.3, where a company incorporated in Jersey (a *supervised person)* carries on a *supervised 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 *supervised business* in or from within Jersey.

105. In practice, the above only applies to *supervised persons* that meet the definition of a *financial group*, this includes a requirement that a parent company or other legal person exercise control over every member of that group for the purposes of applying group supervision.

Group supervision refers to (a) the core principles for effective banking supervision published by the Basel Committee on Banking Supervision; (b) the Objectives and Principles of Securities Regulation issued by the International Organisation of Securities Commissions; or (c) the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.

Statutory requirements (paraphrased wording)

106. *Article 11A of the Money Laundering Order applies to a financial group of which a relevant person is a member.*

107. *Article 11A(2) of the Money Laundering Order requires a financial group to maintain a programme to prevent and detect money laundering and 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 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)*
- *The screening of employees.*

108. *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

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

110. A *supervised* person who:

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

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

111. A person who:

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

must ensure that any subsidiary applies measures that are at least equivalent to the *AML/CFT Codes of Practice* in respect of any *supervised business* carried on outside Jersey by that person.

112. 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 *JFSC* must be informed that this is the case. In such circumstances, a *supervised person* must take other reasonable steps to effectively deal with the risk of *money laundering* and the *financing of terrorism*.