ANTI-MONEY LAUNDERING

GUIDANCE FOR THE ACCOUNTANCY SECTOR

March 2018

Introduction

Accountants are key gatekeepers for the financial system, facilitating vital transactions that underpin the UK economy. As such, they have a significant role to play in ensuring their services are not used to further a criminal purpose. As professionals, accountants must act with integrity and uphold the law, and they must not engage in criminal activity.

This guidance is based on the law and regulations as of 26 June 2017. It covers the prevention of money laundering and the countering of terrorist financing. It is intended to be read by anyone who provides audit, accountancy, tax advisory, insolvency, or trust and company services in the United Kingdom and has been approved and adopted by the UK accountancy AML supervisory bodies.

The guidance has been prepared jointly by the CCAB bodies:

Institute of Chartered Accountants in England and Wales

Association of Chartered Certified Accountants

Institute of Chartered Accountants of Scotland

Chartered Accountants Ireland

The Chartered Institute of Public Finance and Accountancy

It has been approved and adopted by the UK accountancy supervisory bodies:

Institute of Chartered Accountants in England and Wales – www.icaew.com/

Association of Accounting Technicians – www.aat.org.uk/

Association of Taxation Technicians – www.att.org.uk/

Association of International Accountants – www.aiaworldwide.com/

Institute of Certified Bookkeepers – www.bookkeepers.org.uk/

Chartered Institute of Management Accountants – www.cimaglobal.com/

Institute of Financial Accountants – www.ifa.org.uk/

International Association of Bookkeepers – www.iab.org.uk/

Association of Chartered Certified Accountants – www.accaglobal.com/uk/en.html

Chartered Institute of Taxation – www.tax.org.uk/

Insolvency Practitioners Association – www.insolvency-practitioners.org.uk/

Insolvency Service – www.gov.uk/government/organisations/insolvency-service

HM Revenue & Customs – www.gov.uk/government/organisations/hm-revenue-customs

Institute of Chartered Accountants in Scotland – www.icas.com

Chartered Accountants Ireland - https://www.charteredaccountants.ie/

CONTENTS

1 ABOUT THIS GUIDANCE

- What is the purpose of this guidance?
- Who is the guidance for?
- What is the legal status of this guidance?

1.1 What is the purpose of this guidance?

1.1.1 This *guidance* has been prepared to help accountants (including tax advisers and insolvency practitioners) comply with their obligations under UK legislation to prevent, recognise and report money laundering. Compliance with it will ensure compliance with the relevant legislation (including that related to counter terrorist financing) and professional requirements.

1.1.2 The term 'must' is used throughout to indicate a mandatory legal or regulatory requirement. *Businesses* may seek an alternative interpretation of the UK anti-money laundering and terrorist financing (AML) regime, but they must be able to **justify** their decision to their *anti-money laundering supervisory authority*.

1.1.3 Where the law or regulations require no specific course of action, 'should' is used to indicate good practice sufficient to satisfy statutory and regulatory requirements. *Businesses* should consider their own particular circumstances when determining whether any such 'good practice' suggestions are indeed appropriate to them. Alternative practices can be used, but *businesses* must be able to **explain** their reasons to their *anti-money laundering supervisory authority*, including why they consider them compliant with law and regulation.

1.1.4 The UK anti-money laundering regime applies only to defined services carried out by designated *businesses*. This *guidance* assumes that many *businesses* will find it easier to apply certain AML processes and procedures to all of their services, but this is a decision for the *business* itself. It can be unnecessarily costly to apply anti-money laundering provisions to services that do not fall within the *UK AML regime*.

1.1.5 This *guidance* refers, in turn, to guidance issued by bodies other than *CCAB*. When those bodies revise or replace their guidance, the references in this document should be assumed to refer to the latest versions.

1.1.6 *Businesses* may use AML guidance issued by other trade and professional bodies, including the *Joint Money Laundering Steering Group (JMLSG),* where that guidance is better aligned with the specific circumstances faced by the *business*. Where the *business* relies on alternative guidance, they must (in accordance with 1.1.2 of this *guidance*) be in a position to justify this reliance to their *anti-money laundering supervisory authority*.

1.1.7 The law which comprises the *UK AML regime* is contained in the following legislation and relevant amending statutory instruments:

- The Proceeds of Crime Act 2002 (POCA) as amended by the Serious Organised Crime and Police Act 2005 (SOCPA);
- The Terrorism Act 2000 (TA 2000) (as amended by the Anti-Terrorism Crime and Security Act 2001 (ATCSA) and the Terrorism Act 2006 (TA 2006));
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the 2017 Regulations);
- Terrorist Asset-Freezing Act 2010;

- Anti-terrorism, Crime and Security Act 2001;
- Counter-terrorism Act 2008, Schedule 7;
- The Criminal Finances Act 2017.

1.1.8 *POCA* and *TA 2000* contain the offences that can be committed by individuals or organisations. The *2017 Regulations* set out the systems and controls that *businesses* are obliged to possess, as well as the related offences that can be committed by *businesses* and key individuals within them.

1.2 Who is this guidance for?

1.2.1 This *guidance* is addressed to *businesses* covered by Regulations 8(2)(c) and 8(2)(e) of the *2017 Regulations*. This means anyone who, in the course of business in the UK, acts as:

- Regulation 8(2)(e):
  - A trust or company service provider (Regulation 12(2)).
- Regulation 8(2)(c):
  - An *auditor* (Regulation 11(a));
  - An *external accountant* (Regulation 11(c));
  - An *insolvency practitioner* (Regulation 11(b));
  - A *tax adviser* (Regulation 11(d)).

For the purposes of this *guidance* the services listed above are collectively referred to as *defined services*. The scope of what would be considered carrying on business in the UK is broad, and would include certain cross border business models where day to day management takes place from UK registered office or UK head office.

1.2.2 Regulation 11(c) of the *2017 Regulations* defines an *external accountant* as someone who provides *accountancy services* to other persons by way of business. There is no definition given for the term *accountancy services*, however for the purposes of this *guidance* it includes any service which involves the recording, review, analysis, calculation or reporting of financial information, and which is provided under arrangements other than a contract of employment.

1.2.3 This *guidance* does not cover any other services, guidance for which may be available from other sources. *Businesses* supervised by HMRC that provide both accountancy services and trust or company services should generally follow this *guidance* but also have regard to the HMRC 'Anti-money laundering guidance for trust or company services providers'. *Businesses* solely providing trust or company services and supervised by HMRC should follow the HMRC guidance.

1.2.4 Guidance related to secondees and subcontractors can be found in APPENDIX B.

1.3 What is the legal status of this guidance?

1.3.1 Because this *guidance* has been approved by HM Treasury, the UK courts must take account of its contents when deciding whether a *business* subject to it has committed an offence under the *2017 Regulations,* or Section 330-331 of *POCA*. This *guidance* is not intended to be exhaustive. If in doubt, seek appropriate advice or consult your *anti-money laundering supervisory authority*.

If an *anti-money laundering supervisory authority* is called upon to judge whether a *business* has complied with its general ethical or regulatory requirements, it is likely to

be influenced by whether or not the *business* has applied the provisions of this *guidance*.

2 MONEY LAUNDERING DEFINED

- What is money laundering?
- What is the legal and regulatory framework?

2.1 What is money laundering?

2.1.1 Money laundering is defined very widely in UK law. It includes all forms of using or possessing criminal property (as well as facilitating the use or possession) regardless of how it was obtained.

2.1.2 Criminal property may take any form, including:

- Money or money's worth;
- Securities;
- A reduction in a liability; and
- Tangible or intangible property.

Money laundering can involve the proceeds of offending in the UK but also of conduct overseas that would have been an offence had it taken place in the UK. There is no need for the proceeds to pass through the UK. For the purposes of this *guidance* money laundering also includes terrorist financing. There are no materiality or *de minimis* exceptions to money laundering or terrorist financing (*MLTF*) offences.

2.1.3 Money laundering activity can include:

- A single act (for example, possessing the proceeds of one's own crime);
- Complex and sophisticated schemes involving multiple parties;
- Multiple methods of handling and transferring criminal property; or
- Concealing criminal property or entering into arrangements to assist others to conceal criminal property.

2.1.4 *Businesses* need to be alert to the risks posed by:

- *Client*s;
- Suppliers;
- Employees; and
- The customers, suppliers, employees and associates of *client*s.

2.1.5 Neither the *business* nor its *client* needs to have been party to money laundering for a reporting obligation to arise (see Section six of this *guidance*).

2.2 What is the legal and regulatory framework?

2.2.1 The primary money laundering offences are defined by *POCA*, as amended by *SOCPA*. Inside or outside the *regulated sector* someone commits a money laundering offence if they:

- Conceal, disguise, convert, transfer or remove criminal property from England and Wales, Scotland or Northern Ireland (Section 327 of POCA);
- Enter into, or become involved in, an *arrangement* which they know or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person (Section 328 of POCA); or

- Acquire, use or possess *criminal property* for which adequate consideration was not provided.

Any of these offences is punishable by up to 14 years' imprisonment and/or an unlimited fine.

2.2.2 None of these offences is committed if:

- The persons involved did not know or suspect that they were dealing with the proceeds of crime; or
- A report of the suspicious activity is made promptly to:
  - A *Money Laundering Reporting Officer* (*MLRO)* (i.e. an internal Suspicious Activity Report *(SAR)*); or
  - The National Crime Agency *(NCA)* under the provisions of Section 338 of *POCA* (as an external *SAR*) and the SAR is made before the offence takes place so that the necessary *consent* to proceed (referred to as a defence against money laundering by the NCA) is obtained beforehand; or
- There is a reasonable excuse for not reporting (this is likely to be defined narrowly, in terms of personal safety or security, and so very rare); or
- The conduct which gave rise to the *criminal property* is, (a) reasonably believed to have happened in a location where it was legal (i.e., outside the UK), and (b) would have carried a maximum sentence of less than 12 months had it occurred in the UK. The requirements of this overseas conduct exception are complex, onerous and stringent; specialist legal advice may be needed.

2.2.3 The following offences apply **only within the *regulated sector***:

- Failure to report (Section 330 of *POCA*) a suspicion of money laundering (see above regarding 'reasonable excuse'). Remember: there is no *de minimis* threshold value for reporting.
- Disclosing that a suspicious activity report *(SAR)* has been made, or is being contemplated, in a way that is likely to prejudice any subsequent investigation. For further information on these so-called **'tipping off'** offences (Section 333 of POCA) see Section six of this *guidance*.

2.2.4 There are equivalent offences under the Terrorism Act 2000 (*TA 2000*) with no overseas conduct exemption or *de minimis* threshold amount.

2.2.5 Summaries of the relevant Sections of *POCA* can be found in APPENDIX A.

3 RESPONSIBILITY & OVERSIGHT

- What are the responsibilities of a *business*?
- How should sole practitioners implement these requirements?
- What are the responsibilities of *senior management*/*MLRO*?
- How might the *MLRO* role be split?
- What policies, procedures and controls are required?

3.1 What are the responsibilities of a business?

3.1.1 For *businesses* providing *defined services*, the *2017 Regulations* require anti-money laundering systems and controls that meet the requirements of the UK anti-money laundering regime. The 2017 Regulations impose a duty to ensure that *relevant employees* (see Section eight of this *guidance*) are kept aware of these systems and controls and are trained to apply them properly. *Businesses* are explicitly required to:

- Monitor and manage their own compliance with the *2017 Regulations*; and
- Make sure they are always familiar with the requirements of the 2017 Regulations to ensure continuing compliance.

3.1.2 If a *business* fails to meet its obligations under the *2017 Regulations*, civil penalties or criminal sanctions can be imposed on the *business* and any individuals deemed responsible. This could include anyone in a senior position who neglected their own responsibilities or agreed to something that resulted in the compliance failure.

3.1.3 The primary money laundering offences defined under *POCA* (see 2.2 of this *guidance*) can be committed by anyone inside or outside the *regulated sector* but *POCA* imposes specific provisions on the regulated sector.

3.1.4 *Businesses* must have systems and controls capable of: assessing the risk associated with a *client*; performing CDD; monitoring existing *client*s; keeping appropriate records; and enabling staff to make an internal *SAR* (i.e. to their *MLRO*).

3.1.5 *Relevant employees* must be trained appropriately so that they understand both their own personal AML obligations and the business-wide systems and controls that have been developed to prevent *MLTF*.

3.1.6 The AML skills, knowledge, expertise, conduct and integrity of *relevant employees* must be assessed.

3.1.7 Effective internal risk management systems and controls must be established and the relevant *senior management* responsibilities clearly defined.

3.2 How should sole practitioners implement these requirements?

3.2.1 Because it would not be appropriate to the size and nature of the business, a sole practitioner who has no *relevant employees* need not:

- appoint a board member to be responsible for the *business'* compliance with the UK anti-money laundering regime, as the sole practitioner will be held responsible;
- appoint a *nominated officer* because the sole practitioner will be responsible for submitting external reports to the *NCA*;
- establish an independent audit function for AML policies, controls and procedures.

3.3 What are the responsibilities of Senior Management/MLRO?

3.3.1 The *2017 Regulations* define *senior management* as: an officer or employee of the *business* with sufficient knowledge of the business' *MLTF* risk exposure, and with sufficient authority, to take decisions affecting its risk exposure.

3.3.2 The *2017 Regulations* require that the approval of *Senior Management* must be obtained:

- for the policies, controls and procedures adopted by the *business*. (Regulation 19(2)(b));
- before entering into or continuing a business relationship with a Politically Exposed Person *(PEP)*, a family member of a *PEP* or a known close associate of a *PEP* (Regulation 35(5)(a)).

3.3.3 Members of *senior management* undertaking such responsibilities should receive Continuing Professional Development (CPD) appropriate to their role.

3.3.4 Regulation 21(1)(a) of the 2017 Regulations requires that, where appropriate to the size and nature of the *business*, the *business* appoints a board member or member of *senior management* who must be responsible for the *business'* compliance with the UK anti-money laundering regime. The role requires the individual to have:

- an understanding of the *business*, its service lines and its *client*s;
- sufficient seniority to direct the activities of all members of staff (including senior members of staff);
- the authority to ensure the *business'* compliance with the regime;
- the time, capacity and resources to fulfil the role.

3.3.5 Regulation 21(3) of the *2017 Regulations* requires a *business* to appoint a *nominated officer,* who must be responsible for receiving internal *SARs* and making external *SARs* to the *NCA* (as the UK's FIU). The person appointed must have:

- sufficient seniority to enforce their decisions;
- the authority to make external reports to the *NCA* without reference to another person;
- the time, capacity and resources to review internal *SAR*s and make external *SAR*s in a timely manner.

3.3.6 Within 14 days of the appointment of either the responsible board member/*senior management* and/or the *nominated officer*, the *business' anti-money laundering supervisory authority* must be informed of the identity of the individual(s).

3.3.7 Depending on the size, complexity and structure of a *business*, these two roles may be combined in a single individual provided that person has sufficient seniority, authority, governance responsibility, time, capacity and resources to do both roles properly. This *guidance* primarily describes the situation in which one individual fulfils the combined role, referred to in this *guidance* as the *MLRO*, with alternative arrangements covered in 3.4 of this *guidance*. The role of the *MLRO* is not defined in legislation but has traditionally included responsibility for internal controls and risk management around *MLTF*, in accordance with sectoral guidance. *Businesses* with an *MLRO* should periodically review the *MLRO*'s brief to ensure that:

- it reflects current law, regulation, guidance, best practice and the experience of the business in relation to the effective management of *MLTF* risk; and

- the *MLRO* has the seniority, authority, governance responsibility, time, capacity and resources to fulfil the brief.

3.3.8 The *business* should ensure that there are sufficient resources to undertake the work associated with the *MLRO*'s role. This should cover normal working, planned and unplanned absences and seasonal or other peaks in work. Arrangements may include appointing deputies and delegates. When deciding upon the number and location of deputies and delegates, the business should have regard to the size and complexity of the *business'* service lines and locations. Particular service lines or locations may benefit from a deputy or delegate with specialised knowledge or proximity. Where there are deputies, delegates or both (or when elements of *business*' AML policies, controls and procedures are outsourced), the *MLRO* retains ultimate responsibility for the *business'* compliance with the UK anti-money laundering regime.

3.3.9 All *MLROs*, deputies and delegates should undertake CPD appropriate to their roles.

3.3.10 The *MLRO* should:

- have oversight of, and be involved in, *MLTF* risk assessments;
- take reasonable steps to access any relevant information about the *business*;
- obtain and use national and international findings to inform their performance of their role;
- create and maintain the business's risk based approach to preventing *MLTF*;
- support and coordinate management's focus on *MLTF* risks in each individual business area. This involves developing and implementing systems, controls, policies and procedures that are appropriate to each business area;
- take reasonable steps to ensure the creation and maintenance of *MLTF* documentation;
- develop Customer Due Diligence (*CDD*) policies and procedures;
- ensure the creation of the systems and controls needed to enable staff to make internal *SARs* in compliance with *POCA*;
- receive internal *SARs* and make external *SARs* to the *NCA*;
- take remedial action where controls are ineffective;
- draw attention to the areas in which systems and controls are effective and where improvements could be made;
- take reasonable steps to establish and maintain adequate arrangements for awareness and training;
- receive the findings of relevant audits and compliance reviews (both internal and external) and communicate these to the board (or equivalent managing body).

- report to the board (or equivalent managing body) at least annually, providing an assessment of the operations and effectiveness of the *business'* AML systems and controls. This should take the form of a written report. These written reports should be supplemented with regular ad hoc meetings or comprehensive management information to keep senior management engaged with AML compliance and up-to-date with relevant national and international developments in AML, including new areas of risk and regulatory practice. The board (or equivalent managing body) should be able to demonstrate that it has given proper consideration to the reports and ad hoc briefings provided by the *MLRO* and then take appropriate action to remedy any AML deficiencies highlighted.

3.4 How might the MLRO role be split?

3.4.1 Where the *MLRO* role as described above is split between two or more individuals, the allocation of the duties should be clear to the individuals assigned the duties, all *relevant employees* and the business' *anti-money laundering supervisory authority*.

3.4.2 *Businesses* may use their discretion as to how to assign duties between two or more individuals, depending on the size, complexity and structure of their business (subject to the basic legal requirements described in this *guidance*).

3.4.3 The matters listed in 3.3.10 of this *guidance* should be allocated to these individuals or others with the appropriate skills, knowledge and expertise. Regardless of the allocation of these duties, the individual identified in 3.3.4 of this *guidance* is ultimately responsible for the business' compliance with the UK anti-money laundering regime, including the actions of the *nominated officer*.

3.5 What policies, procedures and controls are required?

3.5.1 The *2017 Regulations* place certain requirements on *businesses* regarding *CDD* (Chapter two) and 'record keeping, procedures and training' (Chapter three). The following topics, all of which form part of the *MLTF* framework, need to be considered:

- risk based approach, risk assessment and management;
- *CDD*;
- record keeping;
- internal control;
- ongoing monitoring;
- reporting procedures;
- compliance management;
- communication.

3.5.2 The *2017 Regulations* provide different amounts of detail about the policies and procedures required in each area. *Businesses* must implement and document policies, controls and procedures that are proportionate to the size and nature of the *business*. These should be subject to regular review and update, and a written record of this exercise maintained.

3.5.3 *Businesses* with overseas subsidiaries or branches that are carrying out any of the activities listed in 1.2.1 of this *guidance* must establish group wide policies and procedures equivalent to those in the UK. If the law of the overseas territory does not permit this then the *business* must inform its *anti-money laundering supervisory authority* and implement additional risk based procedures. Steps taken to communicate policies, controls and procedures to the group must also be recorded.

Risk assessment and management

3.5.4 Every *business* must have appropriate policies and procedures for assessing and managing *MLTF* risks. To focus resources on the areas of greatest risk, a risk based approach should be adopted. It is the ultimate responsibility of the board member or member of *senior management* responsible for compliance to identify the risks and then develop risk based procedures for taking on new *client*s. A risk assessment should be conducted at least annually, but with new and changing risks considered as and when they are identified. Resources like the Financial Action Task Force (*FATF*) mutual evaluations and Transparency International's corruption perception index can be useful when determining the *MLTF* risk faced by a given *business*. Information from the business' *anti-money laundering supervisory authority* must be taken into account. Further information on the risk based approach, types and categories of risk can be found in Section four of this *guidance*.

Customer Due Diligence (*CDD*)

3.5.5 Responsibility for developing *CDD* policies and procedures rests with the *MLRO*. These procedures should ensure that *relevant employees* are able to make informed decisions about whether or not to establish a *business relationship* or undertake an *occasional transaction*, in the light of the *MLTF* risks associated with the *client* and transaction To ensure that the correct procedures are being followed, *relevant employees* must be made aware of their obligations under the *2017 Regulations* and given appropriate training.

3.5.6 Many *businesses* already have procedures to help them avoid conflicts of interest and ensure they comply with professional requirements for independence. The requirements of the *2017 Regulations* can either be integrated into these procedures, to form a consolidated approach to taking on a new *client*, or addressed separately. For more on *CDD* see Section five of this *guidance*.

Reporting

3.5.7 Under *POCA* the reporting of knowledge or suspicion of money laundering is a legal requirement. It is the responsibility of the *MLRO* to develop and implement internal policies, procedures and systems that are able to satisfy the *POCA* reporting requirements. Those policies must set out clearly, (a) what is expected of an individual who becomes aware of, or suspects, money laundering, and (b) how they report their concerns to the *MLRO.* All *relevant employees* must be trained in these procedures.

More information on reporting suspicious activity can be found in Section six of this *guidance.*

Record keeping

3.5.8 All records created as part of the *CDD* process, including any non-engagement documents relating to the *client* relationship and ongoing monitoring of it, must be retained for five years after the relationship ends. All records related to an *occasional transaction* must be retained for five years after the transaction is completed. A disengagement letter could provide documentary evidence that a business relationship has terminated, as could other forms of communication such as an unambiguous email making it clear that the *business* does not wish to engage or is ceasing to act.

3.5.9 Although no comparable retention period is specified for information and communications relating to internal and external *SARs*, a business may wish to retain these securely for five years as well.

3.5.10 *Senior management* must ensure that the *relevant employees* are made aware of these retention policies and that they remain alert to the importance of following them. There is more information on record keeping in Section seven of this *guidance*.

Training and awareness

3.5.11 The *2017 Regulations* require all *relevant employees* to be made aware of the law relating to *MLTF* and data protection and given regular training in how to recognise and deal with suspicious activity which may be related to *MLTF*.

The *MLRO* should establish training capable of ensuring that *relevant employees*:

- Are aware of their legal and regulatory duties;
- Understand how to put those requirements into practice in their roles; and
- Are continuously updated about changes in, (a) the *business'* AML policies, systems and controls, and (b) the *MLTF* risks faced.

3.5.12 A formal training plan can help make sure that *relevant employees* receive the right training to enable them to comply with their AML obligations.

3.5.13 Training should be tailored to suit the particular role of the individual.

3.5.14 A business that fails to provide training for *relevant employees* could be in breach of the regulations and at risk of prosecution. It would also risk failing to comply with Section 338 of *POCA*, which requires *Businesses* in the regulated sector to disclose any suspicions of money laundering. Although Section 330 of *POCA* could provide a 'reasonable excuse' defence against a failure to disclose for the individual, the regulations are still likely to have been breached by the *business* because adequate training was not provided. For further information on training and awareness refer to Section eight of this *guidance*.

Employee screening

3.5.15 *Businesses* should consider the skills, knowledge, expertise, conduct and integrity of all *relevant employees* both before, and during the course of, their appointment, proportionate to their role in the business and the *MLTF* risks they are likely to encounter. An employee is relevant if his or her work is relevant to compliance with the *2017 Regulations* or is otherwise capable of contributing to the *business*' identification, mitigation, prevention or detection of *MLTF*. Most *businesses* may already undertake such an assessment as part of their recruitment, appraisal, training, independence, fit and proper and compliance procedures. However, it is important that *businesses* have a mechanism for evidencing *MLTF* knowledge within such procedures for example, a test for which the results are recorded can evidence knowledge and expertise. Similarly, regular recorded ethics training can be useful in assessing integrity.

Monitoring policies and procedures

3.5.16 The *MLRO* and appropriate *senior management* should together monitor the effectiveness of policies, procedures and processes so that improvements can be made when inefficiencies are found. Risks should be monitored and any changes must be reflected in changes to policies and procedures; keeping them up-to-date, in line with the risk assessment of the *business.* For more information, see Section four of this *guidance*.

3.5.17 In their efforts to improve AML policies, controls and procedures, and better understand where problems can arise, *senior management* should encourage *relevant employees* to provide feedback. When changes are made to policies, procedures or processes these should be properly communicated to *relevant employees* and supported by appropriate training where necessary.

3.5.18 *Businesses* must introduce a system of regular, independent reviews to understand the adequacy and effectiveness of the *MLTF* systems and any weaknesses identified. Independent does not necessarily mean external, as some *businesses* will have internal functions (typically audit, compliance or quality functions) that can carry out the reviews. Any recommendations for improvement should be monitored. Existing monitoring programmes and their frequency can be extending to include AML. The reviews should be proportionate to the size and nature of the *business.* A sole practitioner with no *relevant employees* need not implement regular, independent reviews unless required by their *UK AML supervisory authority*.

3.5.19 As part of their improvement efforts the *senior manager* responsible for compliance and the *MLRO* should monitor publicly-available information on best practice in dealing with *MLTF* risks. For example, thematic reviews by regulators can be useful ways to improve understanding of good and poor practice, while reports on particular enforcement actions can illuminate common areas of weakness in AML policies, controls and procedures.

4 RISK BASED APPROACH

- What is the role of the risk based approach?
- What is the role of *senior management*?
- How should the risk analysis be designed?
- What is the risk profile of the *business*?
- How should procedures take account of the?
- What are the different types of risk?
- How important is documentation?

4.1 What is the role of the risk based approach?

4.1.1 The risk based approach is fundamental to satisfying the *FATF* recommendations, the EU directive and the overall UK *MLTF* regime. It requires governments, supervisors and *Businesses* alike to analyse the *MLTF* risks they face and make proportionate responses to them. It is the foundation of any business' AML policies, controls and procedures, particularly its *CDD* and staff training procedures.

4.1.2 The risk based approach recognises that the risks posed by *MLTF* financing activity will not be the same in every case and so it allows the *business* to tailor its response in proportion to its perceptions of risk. The risk based approach requires evidence-based decision-making to better target risks. No procedure will ever detect and prevent all *MLTF*, but a realistic analysis of actual risks enables a *business* to concentrate the greatest resources on the greatest threats.

4.1.3 The risk based approach does not exempt low risk *client*s, services and situations from *CDD*, however the appropriate level of *CDD* is likely to be less onerous than for those thought to present a higher level of risk.

4.1.4 This section provides guidance on the analyses the *business* will need to perform to properly underpin a risk based approach. Guidance on applying the risk based approach to particular AML procedures and controls can be found in the relevant sections of this *guidance* dedicated to those procedures.

4.2 What is the role of senior management?

4.2.1 *Senior management* is responsible for managing all of the risks faced by the *business*, including *MLTF* risks. Senior managers should ensure that *MLTF* risks are analysed, and their nature and severity identified and assessed, in order so as to produce a risk profile. *Senior management* should then act to mitigate those risks in proportion to the severity of the threats they pose.

4.2.2 Where a risk is identified, the *business* must design and implement appropriate procedures to manage it. The reasons for believing these procedures to be appropriate should be supported by evidence, documented and systems created to monitor effectiveness. A *business'* risk based approach should evolve in response to the findings of the systems monitoring the effectiveness of the AML policies, controls and procedures.

4.2.3 The risk analysis can be conducted by the *MLRO*, but must be approved by *senior management* including the senior manager responsible for compliance (if a different person to the *MLRO*). This is likely to include formal ratification of the outcomes, including the resulting policies and procedures, but may also include close *senior management* involvement in some or all of the analysis itself.

4.2.4 The risk profile and operating environment of any *business* changes over time. The risk analysis must be refreshed regularly by periodic reviews, the frequency of which should reflect the *MLTF* risks faced and the stability or otherwise of the business environment. In addition, whenever *senior management* sees that events have affected *MLTF* risks, the risk analysis should also be refreshed by an event-driven review. A fresh analysis may require AML policies, controls and procedures to be amended, with consequential impacts upon, for example, the training programs for *relevant employees*.

4.3 How should a risk analysis be designed?

4.3.1 One possible first step is to consider the *MLTF* risks faced by each different part of the *business*. The *business* may already have general risk analysis processes, and these could form the basis of its *MLTF* risk analysis.

4.3.2 When designing an analysis process the *business* should look not only at itself but at its *client*s and markets as well. Consider factors that lower risks as well as those that increase them; a *client* subject to an effective *AML regime* poses a lower risk than one not. *Businesses* should take into account the findings of the most recent UK National Risk Assessment, together with any guidance issued by the relevant *anti-money laundering supervisory authority*.

4.3.3 Total *MLTF* risks include the possibility that the *business* might:

- Be used to launder money (e.g. by holding criminal proceeds in a *client* money account or by becoming involved in an arrangement that disguises the beneficial ownership of criminal proceeds);
- Be used to facilitate *MLTF* by another person (e.g. by creating a corporate vehicle to be used for money laundering or by introducing a money launderer to another regulated entity);
- Suffer consequential legal, regulatory or reputational damage because a *client* (or one or more of its associates) is involved in money laundering.

4.3.4 Risks should be grouped into categories, such as '*client*', 'service' and 'geography'. Some risks will not easily fit under any one heading but that should not prevent them from being considered properly. Nor should a *business* judge overall risk simply by looking at individual risks in isolation. When two threats are combined they can produce a total risk greater than the sum of the parts. A particular industry and a particular country may each be thought to pose only a moderate risk. But when they are brought together, perhaps by a particular *client* or transaction, then the combined risk could possibly be high. *Businesses* must not take a 'tick-box' approach to assessing *MLTF* risk in relation to any individual *client* but must, instead, take reasonable steps to assess all information relevant to its consideration of the risk.

4.4 What is the risk profile of the business?

4.4.1 A *business* with a relatively simple *client* base and a limited portfolio of services may have a simple risk profile. In which case, a single set of AML policies, controls and procedures may suffice right across its operations. On the other hand, many *Businesses* will find that their risk analysis reveals quite different *MLTF* risks in different aspects of the *business*. *Accountancy services*, for example, may face significantly different risks to insolvency, bankruptcy and recovery services. A risk analysis allows resources to be targeted, and procedures tailored, to address those differences properly.

4.4.2 When a *business* decides to have different procedures in different parts of its operations, it should consider how to deal with *client*s whose needs straddle departments or functions, such as:

- A new *client* who is to be served by two or more parts of the *business* with different AML policies, controls and procedures;
- An existing *client* who is to receive new services from a part of the *business* with its own distinct AML policies, controls and procedures.

4.4.3 The *risk based approach* can also take into account the *business'* experience and knowledge of different commercial environments. If, for example, it has no experience of a particular country, it could treat it as a normal or high risk even though other *Businesses* might consider it low risk. Similarly, if it expects to deal with only UK individuals and entities, it may treat as high risk any *client* associated with a non-UK country.

4.5 How should procedures take account of the risk based approach?

4.5.1 Before establishing a *client* relationship or accepting an engagement a *business* must have controls in place to address the risks arising from it. The risk profile of the *business* should show where particular risks are likely to arise, and so where certain procedures will be needed to tackle them.

4.5.2 Risk based approach procedures should be easy to understand and easy to use for all *relevant employees* who will need them. Sufficient flexibility should be built in to allow the procedures to identify, and adapt to, unusual situations.

4.5.3 The nature and extent of AML policies, controls and procedures depend on:

- The nature, scale, complexity and diversity of the *business*;
- The geographical spread of *client* operations, including any local AML regimes that apply; and
- The extent to which operations are linked to other organisations (such as networking businesses or agencies).

4.5.4 *Businesses* should have different *client* risk categories such as: low, normal, and high. The procedures used for each category should be suitable for the risks typically found in that category. For example, if it is normal for a *business* to deal with *client*s from a high risk country, the *business'* procedures for what they regard as normal *client*s must be designed to be address the risks associated with the high risk country. Some low and high risk indicators can be found in APPENDIX E.

4.5.5 Regardless of the risk categorisation, *businesses* will still be expected to undertake monitoring of the *client* relationship. Such monitoring must be done on a risk based approach, with levels of monitoring varying depending on the *MLTF* risk associated with individual *client*s.

4.5.6 Taking into account key risk categories, a *business* may be able to draw up a simple matrix in order to determine a *client*'s risk profile. Such risk categories may include a *client*'s legal form, the country in which the *client* is established or incorporated, and the industry sector in which the *client* operates. In addition, *businesses* should also consider the nature of the service being offered to a *client* and the channels through which the services/transactions are being delivered.

4.5.7 Elevated risks could be mitigated by:

- Conducting enhanced levels of due diligence – i.e., increasing the level of *CDD* that is gathered.
- Carrying out periodic *CDD* reviews on a more frequent basis.
- Putting additional controls around particular service offerings or *client*.

4.6 What is client risk?

4.6.1 A *business* should consider the following question, "Does the *client* or its beneficial owners have attributes known to be frequently used by money launderers or terrorist financiers?"

4.6.2 *Client* risk is the overall *MLTF* risk posed by a *client* based on the key risk categories, as determined by a *business*.

4.6.3 The *client*'s risk profile may also inform the extent of the checks that need to be performed on other associated parties, such as the *client*'s beneficial owners.

4.6.4 Undue *client* secrecy and unnecessarily complex ownership structures can both point to heightened risk because company structures that disguise ownership and control are particularly attractive to people involved in *MLTF*.

4.6.5 In cases where a *client* (an individual) or beneficial owner of a *client* is identified as a *PEP*, an enhanced level of due diligence must be performed on the *PEP*. Further details on the approach to be taken in such circumstances are set out in 5.3.11 - 5.3.22 of this guidance.

4.7 What is service risk?

4.7.1 A *business* should consider the following question "Do any of our products or services have attributes known to be used by money launderers or terrorist financiers?"

4.7.2 Service risk is the perceived risk that certain products or services present an increased level of vulnerability in being used for *MLTF* purposes.

4.7.3 *Businesses* should consider carrying out additional checks when providing a product or service that has an increased level of *MLTF* vulnerability.

4.7.4 Services and products in which there is a serious risk that the *business* itself could commit a money laundering offence should also be treated as higher risk. For example, wherever the *business* may commit an offence under Section 327 – 329 of *POCA*. (See APPENDIX A.)

4.7.5 Before a *business* begins to offer a service significantly different from its existing range of products or services, it should assess the associated *MLTF* risks and respond appropriately to any new or increased risks.

4.8 What is geographic risk?

4.8.1 A *business* should consider the following question "Are our *client*s established in countries that are known to be used by money launderers or terrorist financiers?"

4.8.2 Geographic risk is the increased level of risk that a country poses in respect of *MLTF*.

4.8.3 When determining geographic risk, factors to consider may include the perceived level of corruption, criminal activity, and the effectiveness of *MLTF* controls within the country.

4.8.4 *Businesses* should make use of publicly available information when assessing the levels of *MLTF* of a particular country, e.g. information published by civil society organisations

such as Transparency International and public assessments of the *MLTF* framework of individual countries (such as *FATF* mutual evaluations).

4.8.5 Although some countries may carry a higher level of *MLTF* risk, those *businesses* that have extensive experience within a given country may reach a geographical risk classification that differs to those that that only have a limited exposure.

4.9 What is sector risk?

4.9.1 A *business* should consider the following question "Do our *client*s have substantial operations in sectors that are favoured by money launderers or terrorist financiers?"

4.9.2 Sector risks are the risks associated with certain sectors that are more likely to be exposed to increased levels of *MLTF*.

4.9.3 *Businesses* should consider the sectors in which their *client* has significant operations, and take this into account when determining a *client*'s risk profile. When considering what constitutes a high risk sector, *Businesses* should take into account the findings of the most recent UK National Risk Assessment, together with any guidance issued by the relevant *anti-money laundering supervisory authority*.

4.10 What is delivery channel risk?

4.10.1 A *business* should consider the following question "Does the fact that I am not dealing with the *client* face to face pose a greater *MLTF* risk?"

4.10.2 Certain delivery channels can increase the *MLTF* risk, because they can make it more difficult to determine the identity and credibility of a *client*, both at the start of a *business relationship* and during its course.

4.10.3 For example, delivery channel risk could be increased where services/products are provided to *client*s who have not been met face-to-face, or where a *business relationship* with a *client* is conducted through an intermediary.

4.10.4 *Businesses* should consider the risks posed by a given delivery channel when determining the risk profile of a *client*, and whether an increased level of *CDD* needs to be performed.

4.11 Why is documentation important?

4.11.1 *Businesses* must be able to demonstrate to their *anti-money laundering supervisory authority* how they assess and seek to mitigate *MLTF* risks. This assessment must be documented, and made available to the *anti-money laundering supervisory authority* on request. The documentation should demonstrate how the risk assessment informs their policies and procedures.

5 CUSTOMER DUE DILIGENCE (*CDD*)

- What is the purpose of *CDD*?
- When should *CDD* be carried out?
- How should *CDD* be applied?
- What happens if *CDD* cannot be performed?

5.1 What is the purpose of *CDD*?

5.1.1 Criminals often seek to mask their true identity by using complex and opaque ownership structures. The purpose of *CDD* is to know and understand a *client*'s identity and business activities so that any *MLTF* risks can be properly managed. Effective *CDD* is, therefore, a key part of AML defences. By knowing the identity of a *client*, including who owns and controls it, a *business* not only fulfils its legal and regulatory requirements it equips itself to make informed decisions about the *client*'s standing and acceptability.

5.1.2 *CDD* also helps a *business* to construct a better understanding of the *client*'s typical business activities. By understanding what is normal practice it is easier to detect abnormal events, which, in turn, may point to *MLTF* activity.

CDD principles

5.1.3 The *2017 Regulations* outline the required components of good *CDD*. *Businesses* must apply them, (a) at the start of a new *business relationship* (including a company formation), (b) at appropriate points during the lifetime of the relationship and (c) when an *occasional transaction* is to be undertaken. The required components are:

- Identifying the ***client*** (i.e., knowing who the *client* is) and then verifying their identity (i.e., demonstrating that they are who they claim to be) by obtaining documents or other information from independent and reliable sources;
- Identifying **beneficial owner(s)** so that the ownership and control structure can be understood and the identities of any individuals who are the owners or controllers can be known and, on a risk sensitive basis, reasonable measures should be taken to verify their identity; and
- Gathering information on the intended purpose and nature of the ***business relationship***.

5.1.4 When determining the degree of *CDD* to apply, the *business* must adopt a risk based approach, taking into account the type of *client*, *business relationship*, product or transaction, and ensuring that the appropriate emphasis is given to those areas that pose a higher level of risk (see Section four of this *guidance*). For this reason it is important that risks are assessed at the outset of a *business relationship* so that a proportionate degree of *CDD* can be brought to bear.

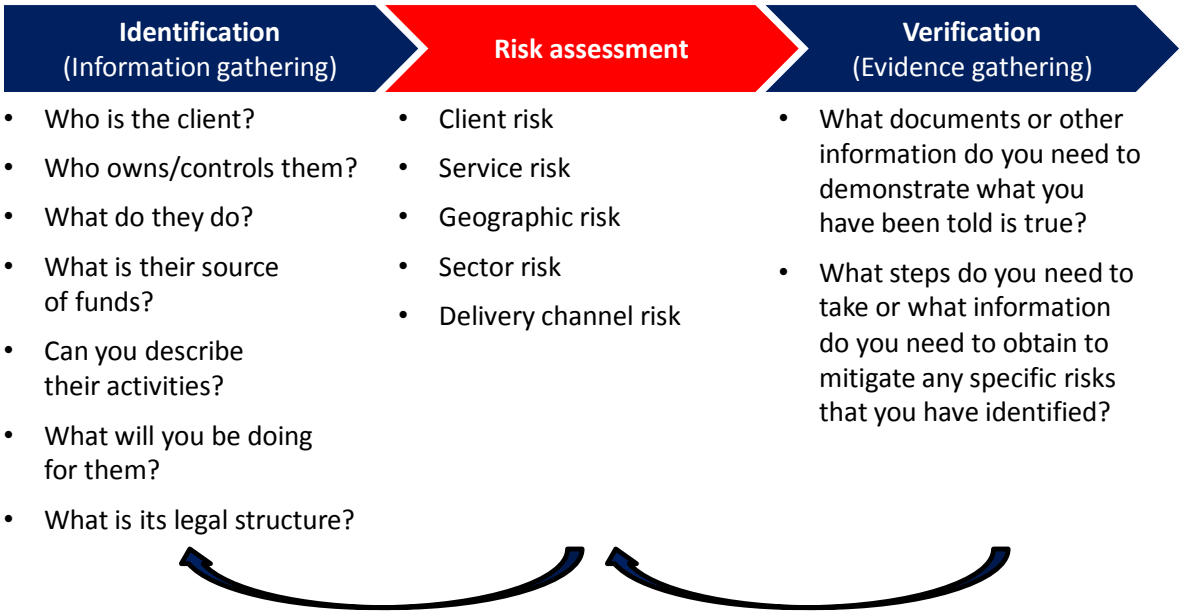
5.1.5 Where the work to be performed falls within the scope of *defined services*, the *business* must ensure that *CDD* is applied to new and existing *clients* alike. For existing *clients*, *CDD* information gathered previously should be reviewed and updated where it is necessary, timely and risk-appropriate to do so.

5.1.6 The *2017 Regulations* stipulate that *CDD* must also be performed where there is either a suspicion of *MLTF*, or any doubts about the reliability of the identity information, or documents obtained previously for verification purposes.

5.1.7 Where there is such knowledge or suspicion the *business* needs to consider not only whether the existing *CDD* information is sufficient and up-to-date, but also whether an external *SAR* should be made to the *NCA*.

5.1.8 While the *2017 Regulations* prescribe the level of *CDD* that should be applied in certain situations (ie. simplified or enhanced – for more on this see 5.3 of this *guidance*), they do not describe how to do this on a risk-sensitive basis. Nonetheless, a *business* is expected to be able to demonstrate to its *anti-money laundering supervisory authority* that the measures it applied were appropriate in accordance with its own risk assessment. Section four of this *guidance* outlines broadly the key areas to be considered when developing a risk based approach including (amongst other factors) the purpose, regularity and duration of the business relationship.

Stages of CDD



5.1.9 The arrows in the diagram above represent feedback loops by which an initial risk assessment or verification may highlight a need for more information to be gathered or a fresh risk assessment performed.

5.1.10 The **identification** phase requires the gathering of information about a *client's* identity and the purpose of the intended *business relationship*. Appropriate identification information for an individual would include full name, date of birth and residential address. This can be collected from a range of sources, including the *client*. In the case of corporates and other organisations, identification also extends to establishing the identity of anyone who ultimately owns or controls the *client*. These people are the Beneficial Owners (BOs), and further detail on how to deal with them can be found in 5.1.14 of this *guidance.*

5.1.11 The next stage of *CDD* is **risk assessment**. This should be performed in accordance with the risk based approach guidance contained in Section four of this *guidance*, and must reflect the purpose, regularity and duration of the *business relationship,* as well as the size of transactions to be undertaken by the *client* and the *business'* own risk assessment. An initial risk assessment is based on the information gathered during stage one (identification), but this may prompt the gathering of additional information as indicated by the left-hand feedback loop. The right-hand feedback loop shows that additional risk assessment may be required in the light of stage three (**verification**).

5.1.12 Once an initial **risk assessment** has been carried out, evidence is required to verify the identity information gathered during the first stage. This is called *client* **verification**.

Verification involves validating (with an independent, authoritative source), that the identity is genuine and belongs to the claimed individual or entity. For an individual, verification may require sight of a passport (with a photocopy taken). For corporates and others, in addition to the *client* itself, reasonable verification measures for any individual beneficial owners (BOs) must also be considered on a risk sensitive basis.

5.1.13 Further guidance on the type of information that should be gathered and the documents that can be used to verify it, can be found in 5.3.35 of this *guidance*.

Beneficial ownership

Definition

5.1.14 A beneficial owner can only be a natural person i.e., an individual (other than in the case of a trust, see below).

5.1.15 Regulations 5 and 6 of the *2017 Regulations* defines the meaning of 'beneficial owner' for a range of different *client* types. The table below gives a summary of how beneficial ownership could be established for a variety of entities:

Client type	Voting Rights	Shares	Capital or profits	Other means of ownership/control
Companies whose securities are listed on a EEA regulated investment market or equivalent				No requirement to establish beneficial ownership
Bodies corporate (including LLPs and LPs)	>25%	>25%		Any individual who exercises ultimate control over the management of the body corporate, or who controls the body corporate
Partnerships other than LLPs and LPs	entitled to or controls >25%		entitled to or controls >25%	Any individual who exercises ultimate control over the partnership management (or in the case of a Scottish partnership, significant influence)
Trusts				The beneficiaries (or where some/all have not yet been determined, the class of persons in whose main interest the trust is set up or operates) The settlor and trustee(s) Any other individual who has control over the trust (e.g., a protector or trust controller).

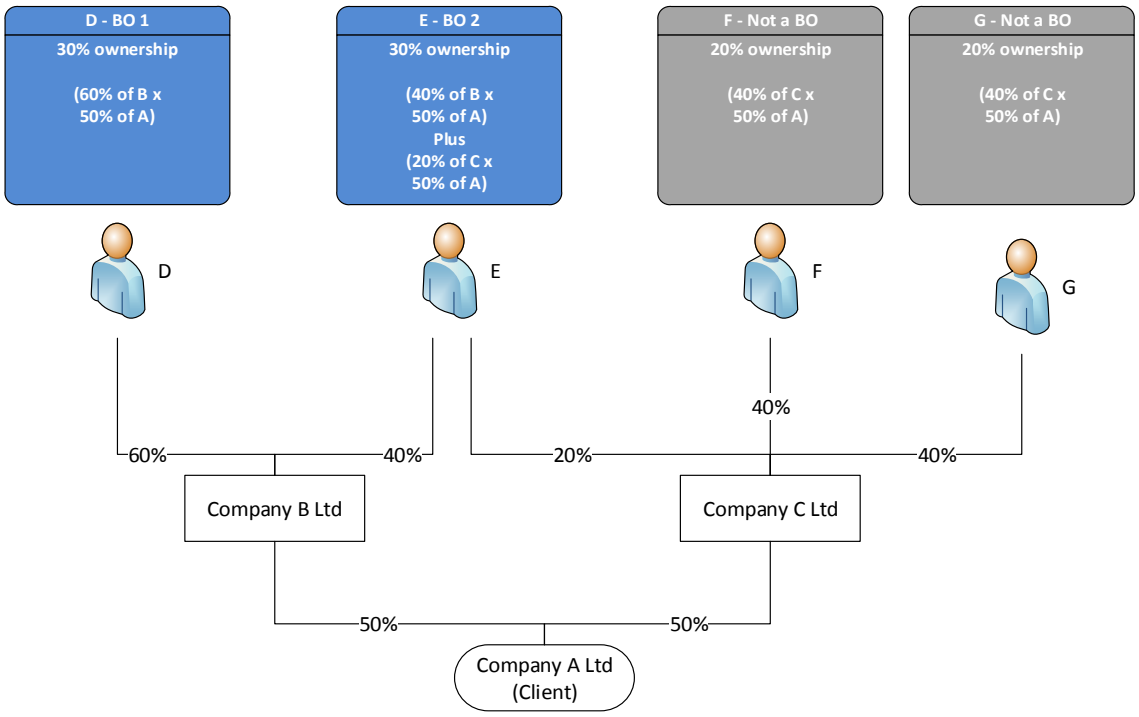
Client type	Voting Rights	Shares	Capital or profits	Other means of ownership/control
Other legal entities				Any individual who benefits from the property of the entity where no individual beneficiaries are identified, the class of persons in whose main interest the entity or arrangement was set up or operates, any individual who exercises control over the entity/arrangement.
Estates of deceased individuals				The executor or administrator of the estate
All other cases Where all possible means of identifying the beneficial owner of a body corporate have been exhausted and recorded				The individual who ultimately owns or controls the client, or on whose behalf a transaction is being conducted the senior individual responsible for management (noting the reasons why the business was unable to obtain adequate information on the beneficial owner, and considering whether it may be appropriate to cease acting, or file a SAR).

5.1.16 *Businesses*, in accordance with their legal obligations, need to be diligent in their enquiries about beneficial ownership, taking into account that the information they need may not always be readily available from public sources. A flexible approach to information gathering will be needed as it will often involve direct enquiries with *clients* and their advisers as well as searches of public records in the UK and overseas. There may be situations in which someone is considered to be the beneficial owner by virtue of control even though their ownership share is less than 25%.

Determining BOs in respect of complex structures

5.1.17 In many situations determining beneficial ownership is a straightforward matter. Cases in which the *client* is part of a complex structure will need to be looked at more closely. The diagrams below illustrate types of structures, including indirect ownership and aggregation, which should be taken into account when determining beneficial ownership.

EXAMPLE 1



The *client* is Company A Ltd, a private company. Unless persons F or G exercise the relevant control through other means (such as through 25% voting rights or other means of control) and based on a 25% ownership threshold, the BOs are person D and person E.

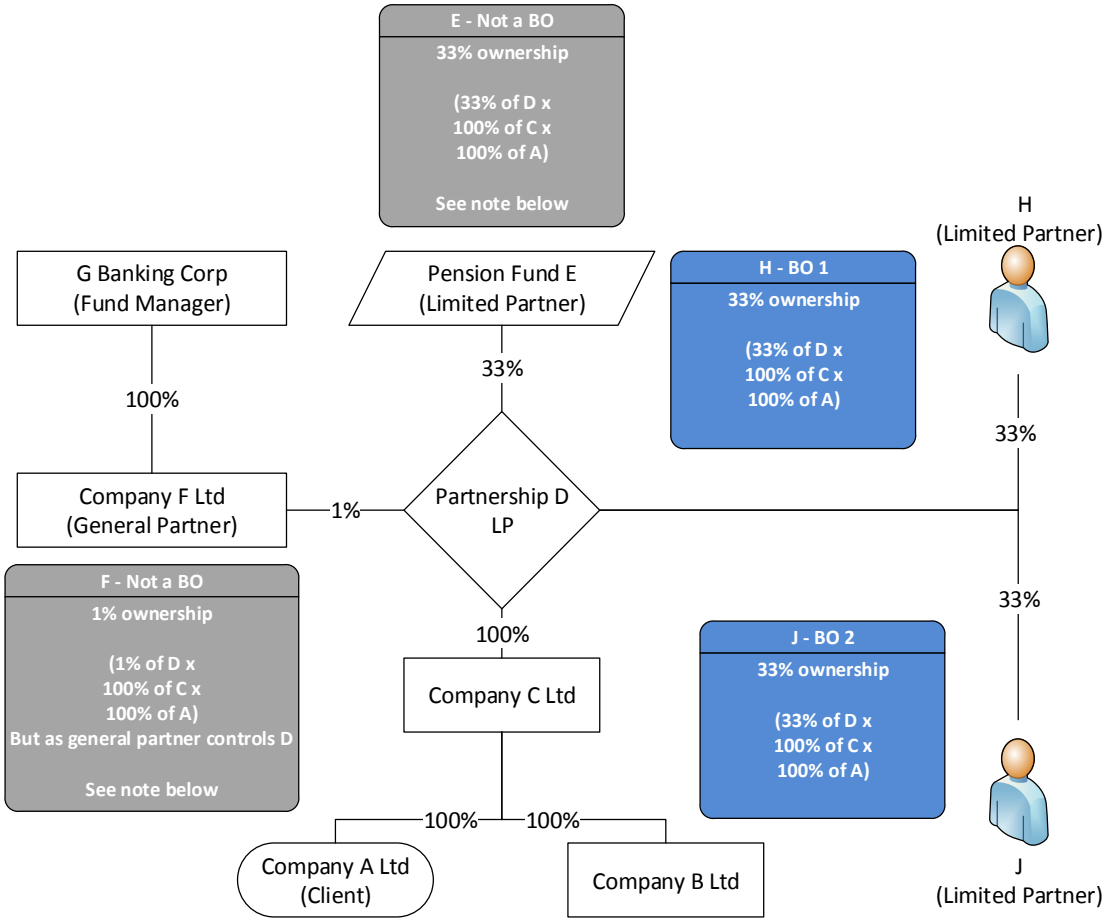
In determining the beneficial owner position, we would need to understand the ownership of Companies B & C (also private companies), but they themselves do not meet the definition of a BO as they are not natural persons.

Person D: is a beneficial owner due to their indirect shareholding of 30% via Company B.

Person E: is a beneficial owner due to their indirect shareholding of 30% via Company B and C.

Persons F & G are not beneficial owners as they only own 20% each via Company C.

EXAMPLE 2



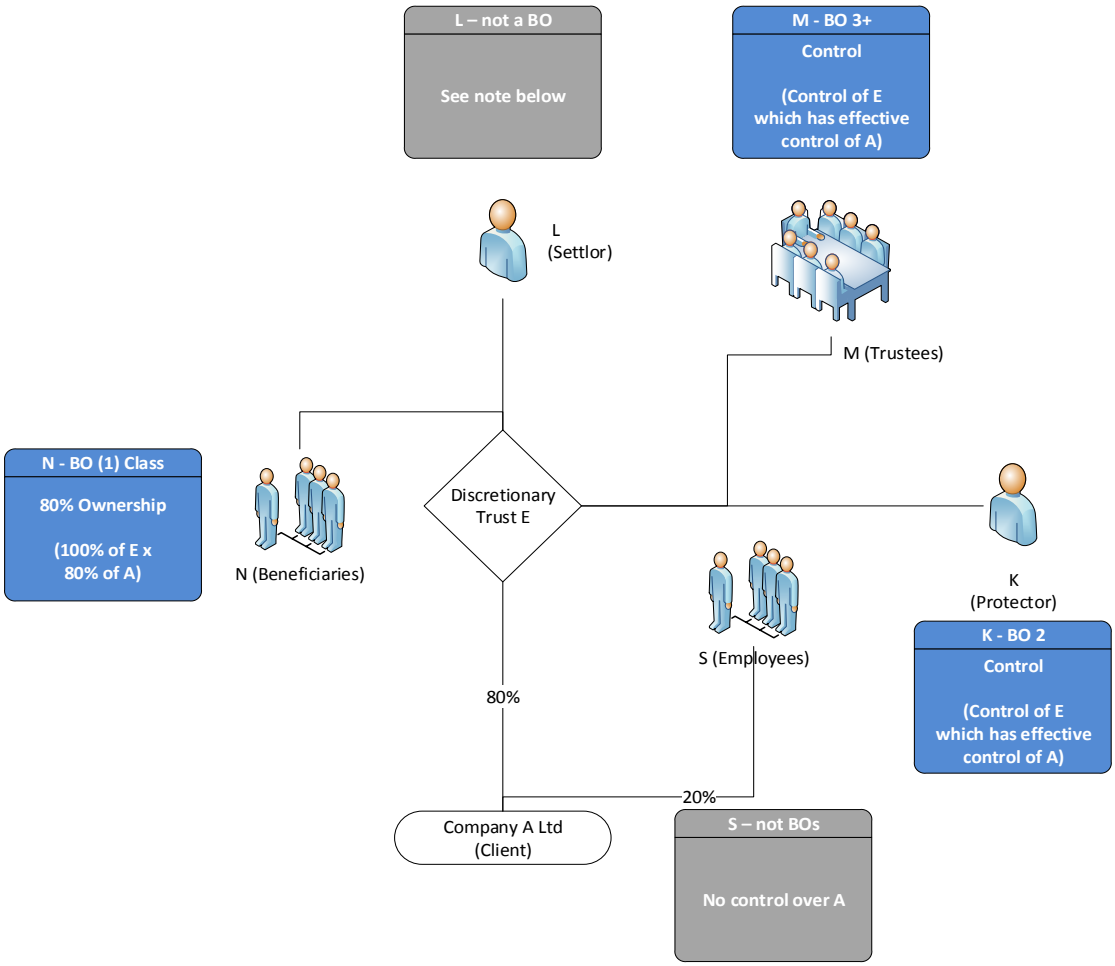
Our *client* is Company A Ltd, a private company. Unless E or F exercise the relevant control through other means (such as through 25% voting rights or other means of control) and based on a 25% threshold, the BOs are person H and person J.

In determining the beneficial owner position, we would need to understand the structure of Company C, Partnership D, Pension Fund E, Company F and G Banking Corp but they themselves do not meet the definition of a BO as they are not natural persons.

Persons H & J: are beneficial owners based on a 25% threshold due to their indirect shareholding of 33% each via Partnership D.

Whilst not beneficial owners in their own right, Pension Fund E and Company F present avenues of ownership and control which should be considered further. Pension Fund E has a 33% ownership interest in Company A. Company F, as General Partner, controls the operations of Partnership D (which owns 100% of Company A). Company F is ultimately owned by G Banking Corp. In some situations, pension schemes and banks may qualify for Simplified Due Diligence (SDD), in which case consideration will stop at the point that we can confirm they are eligible for such treatment. Depending on the risk assessment we may need to further investigate the ownership and control structure to ensure there are no further BOs.

Example 3



The *client* (Company A Ltd) is a body corporate, therefore:

- Its BOs are the natural persons who: (a) exercise ultimate control over its management; (b) own or control more than 25% of its voting rights; (c) own or control more than 25% of its shares; or (d) otherwise controls it (for example through the right to appoint or remove a majority of the directors). There is no need to consider who benefits from dividends or capital distributions.
- There is no need to use the BO rules related to other types of *client*, such as trusts.

In our case, all of the shares in Company A have equal voting rights. 80% of them are owned by Discretionary Trust E, which allows Discretionary trust E to control the activities of Company A. The remaining shares are owned by employees of Company A, none of whom have any connection to anyone else in the ownership and control structure.

Discretionary trust E is not a natural person, so it cannot be a BO.

The activities of Discretionary trust E are controlled by its trustees (M). Thus, each trustee is a BO of Company A.

In our case the trust's protector (K) acts as a check on the powers of the trustees and is also responsible for appointing new trustees. They are therefore regarded as having significant influence and control over E. Protector K is a BO of Company A.

In our case the settlor (L) has no involvement following settlement of assets into the trust, nor do they exercise significant influence or control over the trustees or the

protector. L has no other connection to A. L is not a BO of Company A, since they will not be exercising significant influence or control over E.

The employee-shareholders do not have enough votes, acting either individually or together, to control Company A, none of them is a BO of Company A.

Although the trustees and the protector must act in the interest of the beneficiaries, they (N) have no authority over the trustees or protector. Thus, the beneficiaries will not be BOs of Company A, unless they exercise significant influence or control over E or A.

Notes:

- There may be situations where it is appropriate to know the identity of person L, for example to understand the source of Company A's capital. The MLRO should make the decision to seek such information as a risk-sensitive response to a particular set of circumstances.
- There may be situations where it is appropriate to identify the class of beneficiaries of trust E or even individuals receiving distributions from the trust, for example where distributions from Company A appear excessive it may be appropriate to establish that the beneficiary or beneficiaries require substantial funds. This may occur where a beneficiary is paying for a wedding or for large medical bills. The MLRO should make the decision to seek such information as a risk-sensitive response to a particular set of circumstances.
- If the trust E becomes a client, the settlor and the class of beneficiaries will need to be identified, in line with the rules for a discretionary trust.

5.2 When should CDD be carried out?

When establishing a business relationship

5.2.1 *CDD* should normally be completed before entering into a *business relationship* or undertaking an *occasional transaction*. For guidance on the situation when *CDD* cannot be performed before the commencement of a *business relationship*, see 5.4 of this *guidance*.

5.2.2 A *business relationship* is defined by the *2017 Regulations* (Regulation 4) as:

> 'A business, professional or commercial relationship between a relevant (ie. regulated) person and a customer, which arises out of the business of the relevant person and is expected by the relevant person, at the time when contact is established, to have an element of duration.'

Thus generic advice, provided with no expectation of any client follow-up or continuing relationship (such as generic reports provided free of charge or available for purchase by anyone), is unlikely to constitute a *business relationship*, although may potentially be an *occasional transaction*.

5.2.3 Under Regulation 27 (2) of the *2017 Regulations*, for a transaction to be 'occasional' it must occur outside of a *business relationship* and have a value more than €15,000. Such a thing is not common in *accountancy services*, but should it occur then the business must, (a) understand why the *client* requires the service, (b) consider any other parties involved, and (c) establish whether or not there is any potential for *MLTF*. If the *client* returns for another transaction the *business* should consider whether this establishes an ongoing relationship.

5.2.4 *CDD* procedures must also be carried out at certain other times, such as when there is a suspicion of *MLTF*, or where there are doubts about the available identity information, perhaps following a change in ownership/control or through the participation of a PEP (see 5.3.11 of this *guidance*).

Ongoing monitoring of the client relationship

5.2.5 Established *business relationships* should be subject to *CDD* procedures throughout their duration. This ongoing monitoring involves the scrutiny of *client* activities (including enquiries into sources of funds if necessary) to make sure they are consistent with the *business'* knowledge and understanding of the *client* and its operations, and the associated risks.

Event-driven reviews

5.2.6 *Businesses* need to make sure that documentation, data and information obtained for *CDD* purposes is kept up-to-date. Events prompting a *CDD* information update must include:

- a change in the *client's* identity
- a change in beneficial ownership of the *client*
- a change in the service provided to the *client*
- information that is inconsistent with the *business'* knowledge of the *client*

An event driven review may also be triggered by:

- the start of a new engagement;
- planning for recurring engagements;

- a previously stalled engagement restarting;
- a significant change to key office holders;
- the participation of a *PEP* (see 5.3.11 of this *guidance*)
- a significant change in the *client's* business activity (this would include new operations in new countries); and
- there is knowledge, suspicion or cause for concern (for example where you doubt the veracity of information provided). If a *SAR* has been made, care must also be taken to avoid making any disclosures which could constitute *tipping off*.

Periodic reviews

5.2.7 *Businesses* should use routine periodic reviews to update their *CDD*. The frequency of up-dating should be risk based, making use of the *business'* risk assessment covered in Section 4 of this *guidance*, and reflecting the *business'* knowledge of the *client* and any changes in its circumstances or the services it requires.

Ongoing procedures

5.2.8 The *CDD* procedures required for either event-driven or periodic reviews may not be the same as when first establishing a new *business relationship*. Given how much existing information could already be held, ongoing *CDD* may require the collection of less new information than was required at the very outset.

5.3 How should *CDD* be applied?

Applying *CDD* by taking a risk based approach

5.3.1 Regulation 28(12) of the *2017 Regulations* requires adequate *CDD* measures to reflect the *business'* risk assessment (Section four of this *guidance*). This is important not only to ensure that there is good depth of knowledge in higher risk cases but also to avoid disproportionate effort in lower or normal risk cases and to minimise inconvenience for a potential *client*. No system of checks will ever detect and prevent all *MLTF*, but a risk-sensitive approach of this kind will provide a realistic assessment of the risks. A non-exhaustive list of risk factors can be found in APPENDIX E.

5.3.2 Extensive information on how to apply *CDD* in this way is contained in the guidance on risk-sensitive client verification provided by the *JMLSG*, which considers a wide range of entity types. For information on the more frequently encountered entity types see APPENDIX C.

Simplified due diligence (SDD)

5.3.3 SDD can be applied when a *client* is low risk, in accordance with the *businesses*' risk assessment criteria.

5.3.4 *CDD* measures are still required but the extent and timing may be adjusted to reflect the assessment of low risk, for example in determining what constitutes reasonable verification measures. Ongoing monitoring for unusual or suspicious transactions is still required.

5.3.5 The *business'* internal procedures should set out clearly what constitutes reasonable grounds for a client to qualify for SDD and must take into account at least the risk factors in APPENDIX E and relevant information made available by its *anti-money laundering supervisory authority*.

5.3.6 In any case, when a client or potential client has been subjected to SDD, and a suspicion of *MLTF* arises nonetheless, the SDD provisions must be set aside and the appropriate due diligence procedures applied instead (with due regard given to any risk of *tipping off*).

Enhanced due diligence (EDD)

5.3.7 A risk based approach to *CDD* will identify situations in which there is a higher risk of *MLTF*. The regulations specify that 'enhanced' due diligence (Regulation 33 of the *2017 Regulations*) must be applied in the following situations:

- where there is a high risk of *MLTF*;
- in any *occasional transaction* or *business relationship* with a person established in a high-risk third country;
- if a business has determined that a client or potential client is a *PEP*, or a *family member* or *known close associate* of a *PEP;*
- in any case where a *client* has provided false or stolen identification documentation or information on establishing a *business relationship*;
- in any case where a transaction is complex and unusually large, there is an unusual pattern of transactions which have no apparent economic or legal purpose;
- in any other case which by its nature can present a higher risk of *MLTF.*

5.3.8 The *business'* internal procedures should set out clearly what constitutes reasonable grounds for a *client* to qualify for EDD and must take into account at least the high risk factors in APPENDIX E.

5.3.9 EDD procedures must include:

- as far as reasonably possible, examining the background and purpose of the engagement; and
- Increasing the degree and nature of monitoring of the *business relationship* in which the transaction is made to determine whether that transaction or that relationship appear to be suspicious.

5.3.10 EDD measures (as detailed in Regulation 33 (5) of the *2017 Regulations*) may also include one or more of the following measures:

- seeking additional independent, reliable sources to verify information, including identity information, provided to the *business*;
- taking additional measures to understand better the background, ownership and financial situation of the *client*, and other parties relevant to the *engagement*;
- taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the *business relationship*;
- Increasing the monitoring of the *business relationship*, including greater scrutiny of transactions.

Politically exposed person (PEP)

5.3.11 As set out above, the *2017 Regulations* specify that *PEPs* (as well as certain *family members* and *known close associates*) must undergo EDD. The nature, and extent of, such EDD measures must vary depending on the extent of any heightened *MLTF* risk associated with individual *PEPs*. *Businesses* must treat *PEPs* on a case-by-case basis, and apply EDD on the basis of their assessment of the *MLTF* risk associated with any individual *PEPs*.

5.3.12 So as to assess this risk, it is important to identify *PEPs* so that the *business* can properly consider the risks associated with any *engagement* involving them. Appropriate risk management systems and procedures to determine whether potential *clients* (or their beneficial owners) are *PEPs*, or *family members/known close associates* of a *PEP*. These must be based on the risk assessment process detailed in Section four of this *guidance*, and relevant information provided by the *business' anti-money laundering supervisory authority*. Domestic *PEPs* are included within the definition of *PEPs*. *Businesses* should, however, consider factors including the country which has entrusted a *PEP* with a prominent public function when determining the level of *MLTF* risk associated with an individual *PEP*. *PEPs* entrusted with prominent public functions by countries with characteristics such as low levels of corruption; strong state institutions; and credible anti-money laundering defences are likely to pose less of an *MLTF* risk than *PEPs* from higher-risk countries.

5.3.13 An individual identified as a *PEP* solely because of their public function in the UK must still be treated as a *PEP*. However if the *business* is not aware of any factors that would place the individual in a higher risk category, the individual may be categorised as a low risk *PEP*. Regulation 18 of the *2017 Regulations* and the risk factors guidance produced by the European Supervisory Authorities set out factors that might point to potential higher risk. Such factors might also include, for example:

- known involvement in publicised scandals e.g., regarding expenses;
- undeclared business interests;
- the acceptance of inducements to influence policy.

5.3.14 In lower-risk situations a *business* should apply less onerous EDD requirements (such as, for example, making fewer enquiries of a *PEP's family members* or *known close associates;* and taking less intrusive and less exhaustive steps to establish the *sources of wealth/funds* of *PEPs*). Conversely, and in higher-risk situations, *Businesses* should apply more stringent EDD measures. This represents part of the risk based approach that *businesses* should take to *MLTF* compliance, as described more fully elsewhere in this *guidance*.

5.3.15 *Businesses* must treat individuals as *PEPs* for at least 12 months after they cease to hold a prominent public function. This requirement does not apply to *family members* or *known close associates. Family members* and *known close associates* of *PEPs* should be treated as ordinary *clients* (and subject only to *CDD* obligations) from the point that the *PEP* ceases to discharge a prominent public function. *Businesses* should only apply EDD measures to *PEPs* for more than 12 months after they have ceased to hold a prominent public function when the *business* has determined that they present a higher risk of *MLTF*.

5.3.16 To establish whether someone is a *family member* or *known close associate* of a *PEP, businesses* are expected to refer only to information that is either in the public domain or already in their possession. The *2017 Regulations* provide that the definition of a *family member* must include the spouses/civil partners of *PEPs*, the children of *PEPs* (and their spouse or civil partner) and the parents of *PEPs*. This is not an exhaustive list – in determining whether other *family members* should be subject to EDD, *businesses* should consider the levels of *MLTF* risk associated with the relevant *PEP*. In lower-risk situations, a business should not apply EDD to additional *family members* other than those contained within the definition set out in the *2017 Regulations*.

5.3.17 The *2017 Regulations* state that only directors, deputy directors and board members (or equivalent) of international organisations should be treated as *PEPs*. Middle-ranking and junior officials do not fall within the definition of a *PEP*.

5.3.18 Since the term 'international organisation' is not defined by the *2017 Regulations*, careful consideration should be given to the type, reputation and constitution of a body before excluding its representatives from EDD. Bodies such as the United Nations and NATO can confidently be considered to fall within the definition. The context of the *engagement* and role of the *PEP* in respect of it should also be considered. The regulations are clear that only directors, deputy directors and board members (or equivalent of international organisations should be treated as PEPs.

5.3.19 *Businesses* are required to use risk-sensitive measures to help them recognise *PEPs*. This can be as simple as asking the *client* themselves or searching the internet for public information relating to the *PEP*. *Businesses* likely to provide services regularly to *PEPs* should consider subscribing to a specialist database. *Businesses* that use such databases must understand how they are populated and will need to ensure that those flagged by the database fall within the definition of a *PEP*, *family member* or *known close associate* as set out by the *2017 Regulations*. During the life of a relationship, and to the extent that it is practical, attempts should be made to keep abreast of developments that could transform an existing *client* into a *PEP*.

5.3.20 *Businesses* wanting to enter into, or continue, a *business relationship* with a *PEP* must carry out EDD, which includes:

- *senior management* approval for the relationship;
- adequate measures to establish sources of wealth and funds; and
- enhanced monitoring of the ongoing relationship.

As set out above, the nature and extent of EDD measures must vary depending on the levels of *MLTF* risk associated with individual *PEPs*.

5.3.21 The Financial Conduct Authority (FCA) has published detailed guidance on how businesses that it supervises for *MLTF* purposes should identify and treat *PEPs*. *Businesses* may find this guidance useful in determining the approach that they should take to identifying and applying EDD to *PEPs*.

5.3.22 Recital 33 of the *EU Directive* (which the *2017 Regulations* bring into UK law)makes it clear that refusing a *business relationship* with a person solely on the basis that they are a *PEP* is a contrary to the spirit and letter of the *EU Directive*, and of the *FATF* standards. *Businesses* must instead mitigate and manage any identified *MLTF* risks, and should refuse *business relationships* only when such risk assessments indicate that they cannot effectively mitigate and manage these risks.

Financial sanctions and other prohibited relationships

5.3.23 *Businesses* must comply with any sanctions, embargos or restrictions in respect of any person or state to which the UN, UK or EU has decided to apply such measures (a list is published by HM Treasury). *Businesses* may be directed to not enter into *business relationships*, carry out *occasional transactions* or proceed with any arrangements already in progress, and have an obligation to report sanctions breaches to HM Treasury's Office of Financial Sanctions Implementation (OFSI) (separately to the making of an external *SAR* to the *NCA*, where appropriate). Depending on the circumstances, sanctions imposed by overseas countries may also apply to UK *businesses*.

5.3.24 Financial sanctions can be a complex and changeable area. Detailed discussion of it is beyond the scope of this *guidance*. *Businesses* should make use of the guidance published by OFSI. OFSI also offer a free e-alerts service to help *businesses* stay up-to-date with developments in financial sanctions. *Businesses* should note that *2017 Regulations* set out specific reporting obligations for certain b*usinesses*, including *external accountants*, *auditors*, and *tax advisers*. A *business* that fails to comply with its reporting obligations will be committing an offence, which may result in a criminal prosecution or a monetary penalty. For further information on the reporting obligations refer to the OFSI guide to financial sanctions. *Businesses* unsure of their legal obligations should seek legal advice.

Reliance on other parties

5.3.25 *Businesses* are permitted to rely on certain other parties (subject to their agreement) to complete all or part of *CDD*.

5.3.26 This is permitted only if the other party is a member of the *regulated sector* in the UK, or subject, in an EEA or non-EEA state, to an equivalent regulatory regime which includes compliance supervision requirements equivalent to the *EU Directive*.

5.3.27 *Businesses* should note that where one party places reliance on another they must enter into an agreement (that should be in writing) to ensure that the other party will provide the *CDD* documentation immediately on request. An arrangement of this kind can be useful and efficient when the two parties are able to build a relationship of trust, but it should not be entered into lightly. Liability for inadequate *CDD* remains with the relying party. *Businesses* placing reliance on another should satisfy themselves with the level of *CDD* being undertaken.

Parties seeking reliance

5.3.28 A *business* relying on a third party in this way is not required to apply standard *CDD*, but it must still carry out a risk assessment and perform ongoing monitoring. That means it should still obtain a sufficient quantity and quality of *CDD* information to enable it to meet its monitoring obligations.

5.3.29 In addition, the *business* seeking to rely on a third party remains liable for any *CDD* failings irrespective of the terms of the *CDD* agreement.

5.3.30 If relying on a third party, *businesses* must obtain copies of all relevant information to satisfy *CDD* requirements. They should also enter into a written arrangement that confirms that the party being relied on will provide copies of identification and verification documentation immediately on request.

Parties granting reliance

5.3.31 A *business* should consider whether it wishes to be relied upon to perform *CDD* for another party. Before granting consent, a *business* that is relied upon must ensure that its *client* (and any other third party whose information would be disclosed) is aware that the disclosure may be made to the other party and has no objection to the disclosure. It should make sure that:

- it has adequate systems for keeping proper *CDD* records;
- it can make available immediately on request:
  - any information about the *client*/BO gathered during *CDD*; and/or
  - copies of any information provided during *client*/BO identity/verification or documentation obtained during *CDD*.
- It can keep those *CDD* records securely for five years after the end of the *business relationship*.

Group engagements

5.3.32 When a relevant *business* contracts with a group of companies that are under the control of a parent undertaking, all of which could be considered *clients*, it may wish to consider applying *CDD* in a proportionate, risk-sensitive way by treating the group as a single entity.

Subcontracting

5.3.33 Where a relevant *business*, A, is engaged by another *business*, B, to help with work for one of its *clients* or some other underlying party, C, then A should consider whether its *client* is in fact B, not C. For example, where there is no *business relationship* formed, nor is there an engagement letter between A and C, it may be that *CDD* on C is not required but should instead be completed for B.

5.3.34 On the other hand, where there is significant contact with the underlying party, or where a *business relationship* with it is believed to have been established, then C may also be deemed a *client* and *CDD* may be required for both C and B. In this situation, A may wish to take into account information provided by B and the relationship it has with C when determining what *CDD* is required under its risk based approach. It should be noted that the same considerations are relevant in networked arrangements, where work is referred between member firms.

Evidence gathering

5.3.35 The *2017 Regulations* do not prescribe what information sources a *business* should consult to perform *CDD* effectively. There are many possibilities, including direct discussions with the *client* and collecting information from its websites, brochures and reports, as well as public domain sources. It is particularly important to make sure that the *client* is who they say they are. Since the purpose of *client* verification is to check the *client* identity information already gathered, it is important that the information used at this stage is drawn from independent sources and any identity evidence used should be from an authoritative source.

5.3.36 In higher risk cases *businesses* must consider whether they need to take extra steps to increase the depth of their *CDD* knowledge. These might include more extensive internet and media searches covering the *client*, key counterparties, the business sectors and countries and requests for additional identity evidence. Subscription databases can be a quick way to access this kind of public domain information, and they will often reveal links to known associates (companies and individuals) as well.

5.3.37 *Client* verification means to verify on the basis of documents or information obtained from a reliable source which is independent of the person whose identity is being verified. Documents issued or made available by an official body can be regarded as being independent.

5.3.38 It is important that verification procedures are undertaken on a risk-sensitive basis. Refer to APPENDIX C for a non-exhaustive list of documents that can be used for verification purposes. Further help can be found in the *JMLSG* guidance.

Copies of documents

Certification

5.3.39 *Businesses* should consider how they will demonstrate the provenance of document copies. When the original was seen by a *relevant employee* it should be sufficient for that person to endorse the copy to that effect, including the date on which it was seen. When the copy originates from outside the *business*, the standing of the person who certified it should be considered and *relevant employees* should be aware of the risks associated with certified copies (for example, that such documents may be falsified). It may be necessary to stipulate acceptable sources for certified copies; for example, *businesses* may decide to restrict acceptance to those persons in the permitted categories for reliance (see 5.3.26 of this *guidance*).

Annotation

5.3.40 Where a document is not an original but could be mistaken for one, it should be annotated to that effect. This is particularly true for documents sourced from the internet, such as downloads from Companies House, from the website of a regulator, stock exchange or government department, or from any other suitable source. Documents of this kind should carry an indication of the source and when the download

took place – sometimes in the automatic page footers/headers – and these would satisfy this requirement. Where necessary and taking a risk based approach, such documents (whether downloaded or otherwise) should be validated with an authoritative source such as a government agency.

Use of electronic data

5.3.41 A number of subscription services give access to identity-related information. Many of them can be accessed on-line and are often used to replace or supplement paper-based verification checks. Companies House registers of persons of significant control may be used but may not be relied upon in the absence of other supporting evidence.

5.3.42 Before using any electronic service, question whether the information is reliable, comprehensive and accurate. Consider the following:

- **Does the system draw on multiple sources?** A single source (e.g., the electoral register) is not usually sufficient. A system that combines negative and positive data sources is generally the more robust.
- **Are the sources checked and reviewed regularly?** Systems that do not update their data regularly are generally more prone to inaccuracy.
- **Are there control mechanisms to ensure data quality and reliability?** Systems should have built-in data integrity checks which, ideally, are sufficiently transparent to prove their effectiveness.
- **Is the information accessible?** It should be possible to either download and store search results in electronic form, or print a hardcopy that contains all the details required (name of provider, original source, date, etc.).
- **Does the system provide adequate evidence that the client is who they claim to be?** Consideration should be given as to whether the evidence provided by the system has been obtained from an official source, e.g., certificate of incorporation from the official company registry.

5.4 What happens if CDD cannot be performed?

When delays occur

5.4.1 The *business* should still gather enough information to form a general understanding of the *client's* identity so that it remains possible to assess the risk of *MLTF*.

5.4.2 The *2017 Regulations* do recognise that *CDD* will sometimes need to be completed while the *business relationship* is established, rather than before. But delays of this kind are only permissible when there is little risk of *MLTF* and it is necessary to avoid interrupting the normal conduct of business. Such exceptions will be rare (see 5.4.6 of this *guidance*).

5.4.3 When most of the information needed has been collected before the *business relationship* has begun, it may be acceptable to have a short extension (to allow for information collection to be completed) provided the cause of the delay is administrative or logistical, not the *client's* reluctance to cooperate. To ensure the reasons are valid, and should not give rise to suspicions of *MLTF*, it is recommended that each extension be considered individually and agreed by the *MLRO*.

5.4.4 Extensions to the *CDD* schedule should be specific, well-defined and time-limited. There should be no granting of general extensions (such as for particular *client* types).

5.4.5 No *client engagement* (including transfers of *client* money or assets) should be completed until *CDD* has been completed in accordance with the *business'* own procedures.

5.4.6 Provided that *CDD* is completed as soon as practicable, verification procedures may be completed during the establishment of a *business relationship* if it is necessary not to interrupt the normal course of business and there is little risk of *MLTF*. In some situations it may be necessary to carry out *CDD* while commencing work because it is urgent. Such situations could include:

- some insolvency appointments;
- appointments that involve ascertaining the *client's* legal position or defending them in legal proceedings;
- response to an urgent cyber incident; or
- when it is critically important to preserve or extract data or other assets without delay.

5.4.7 It is recommended that these categories are considered carefully and defined by the *MLRO* to ensure that the reasons for any extension are appropriate.

Cessation of work and suspicious activity reporting

5.4.8 If a prospective or existing *client* refuses to provide *CDD* information, the work must not proceed and any existing relationship with the *client* must be terminated. However in many cases inability to complete *CDD* is not a circumstance where an insolvency practitioner can resign and so an appropriate risk based approach should be adopted where the *client's* management are not cooperative. Consideration must also be given to whether or not a *SAR* should be submitted to the *NCA* under *POCA* or *TA 2000* (see Section six of this *guidance*).

6 SUSPICIOUS ACTIVITY REPORTING

- What must be reported?
- When and how should an external *SAR* be made to the *NCA*?
- What is *consent* and why is it important?
- What should happen after an external *SAR* has been made?

6.1 What must be reported?

The reporting regime

6.1.1 *Businesses* must have internal reporting procedures that enable *relevant employees* to disclose their knowledge or suspicions of *MLTF*. A *nominated officer* must be appointed to receive these disclosures (this *guidance* assumes that this role will be filled by the *MLRO*). In the regulated sector it is an offence for someone who knows or suspects that *MLTF* has taken place (or has reasonable grounds) not to report their concerns to their *MLRO* (or, in exceptional circumstances, straight to the *NCA*).

6.1.2 The *MRLO* has a duty to consider all such internal *SARs*. If the *MLRO* also suspects *MLTF* when an external *SAR* must be made to the *NCA*. Typically the *MLRO's* knowledge or suspicions will arise (directly or indirectly) out of the internal *SARs* they receive.

6.1.3 Similar 'failure to disclose' provisions are found in The *TA* 2000.

6.1.4 The key elements required for a SAR (suspicion, crime, proceeds) are set out below.

Suspicion

6.1.5 There is very little guidance on what constitutes 'suspicion' so the concept remains subjective. Some pointers can be found in case law, where the following observations have been made. Suspicion is:

- a state of mind more definite than speculation but falling short of evidence-based knowledge;
- a positive feeling of actual apprehension or mistrust;
- a slight opinion, without sufficient evidence.

Suspicion is not:

- a mere idle wondering;
- a vague feeling of unease.

6.1.6 A *SAR* must be made where there is knowledge or suspicion of money laundering, but there is no requirement to make speculative *SARs*. If, for example, a suspicion is formed that someone has failed to declare all of their income for the last tax year, to assume that they had done the same thing in previous years would be speculation in the absence of specific supporting information. Similarly, the purchase of a brand new Ferrari by a *client's* financial controller is not, in itself, suspicious activity. However, inconsistencies in accounts for which the financial controller is responsible could raise speculation to the level of suspicion.

6.1.7 A *SAR* is also required when there are 'reasonable grounds' to know or suspect. This is an objective test; i.e., the standard of behaviour expected of a reasonable person in the same position. Claims of ignorance or naivety are no defence.

6.1.8 It is important for individuals to make enquiries that would reasonably be expected of someone with their qualifications, experience and expertise, and as long as the enquiries fall within the normal scope of the *engagement* or *business relationship*. In other words, they should exercise a healthy level of professional scepticism and judgement and, if unsure about what to do, consult their *MLRO* (or similar) in accordance with the *business'* own procedures. If in doubt, err on the side of caution and report to the *MLRO*.

6.1.9 The information or knowledge that gave rise to the suspicions must have come to the individual in the course of business in the *regulated sector*.

Crime

6.1.10 Criminal conduct is behaviour which constitutes a criminal offence in the UK or, if it happened overseas, would have been an offence had it taken place in any part of the UK.

6.1.11 There is an overseas conduct exception, set out in Section 330 (7A) of *POCA*, which describes the circumstances in which there is no requirement to report overseas matters of this kind:

- the conduct is reasonably believed to have taken place overseas; and
- it was lawful where it took place; and
- the maximum sentence had it happened in the UK would be less than 12 months.

(For offences under the Gaming Act 1968, the Lotteries and Amusements Act 1976 and Section 23 or 25 of the *FSMA 2000* the exemption still applies even if the UK sentence is more than 12 months.)

Because these tests are complex and burdensome, *MLROs* may seek legal advice to resolve any doubts.

6.1.12 There is no similar overseas conduct exemption for reporting suspicions of terrorist financing.

6.1.13 In most cases of suspicious activity the reporter will have a particular type of criminal conduct in mind, but this is not always the case. Some transactions or activities so lack a commercial rationale or business purpose that they give rise to a general suspicion of *MLTF*. UK law defines money laundering widely; any criminal conduct that results in criminal property is classified as money laundering. Individuals are not required to become experts in the wide range of criminal offences that lead to money laundering, but they are expected to recognise any that fall within the scope of their work. Exercise professional scepticism and judgement at all times.

6.1.14 An innocent error or mistake would not normally give rise to criminal proceeds (unless a strict liability offence). If a *client* is known or believed to have acted in error, they should have the situation explained to them. They must then promptly bring their conduct within the law to avoid committing a money laundering offence. Where there is uncertainty because certain legal issues lie outside the competence of the practitioner, the *client* should be referred to an appropriate specialist or legal professional.

Proceeds

6.1.15 Criminal proceeds can take many forms. Cost savings (as a result of tax evasion or ignoring legal requirements) and other less obvious benefits can be proceeds of crime.

Where criminal property is used to acquire more assets, these too become criminal property. It is important to note that there is no question of a de minimis value.

6.1.16 If someone knowingly engages in criminal activity with no benefit, then they may have committed some offence other than money laundering (it will often be fraud) and there is no obligation to make a *SAR*. *Businesses* should nonetheless consider whether they are under some other professional reporting obligations, such as those referred to in 6.4.20 of this *guidance*.

A checklist for the *SAR* reporting process can be found in APPENDIX D.

OFFENCE: failure to disclose

6.1.17 Individuals should make sure that any information in their possession which is part of the required disclosure is passed to the *MLRO* as soon as practicably possible.

6.1.18 Where, as a result of an internal *SAR*, the *MLRO* obtains knowledge or forms a suspicion of *MLTF*, they must as soon as practicable make an external *SAR* to the *NCA*. The *MLRO* may commit a *POCA* Section 331 offence if they fail to do so.

Some examples

Example 1 – Shoplifting	
The *business* acts for a retail *client* and you are aware of some instances of shoplifting.	
Report	If you: • know or suspect the identity of the shoplifter; • know or suspect the location of the shoplifted goods; • have information that may assist in the identification of the identity of the shoplifter; or • have information that may assist in locating the shoplifted goods.
Do not report	If you have none of the information listed above.
No further work is required to find out any of the listed details.	

Example 2 – Overpaid invoices	
Some customers of your *client* have overpaid their invoices. The *client* retains overpayments and credits them to the profit and loss account.	
Report	If you: • know or suspect that the *client* intends to dishonestly retain the overpayments. Reasons for such a belief may include: ○ The *client* omits overpayments from statements of account. ○ The *client* credits the profit and loss account without making any attempt to contact the overpaying party.

Example 2 – Overpaid invoices	

Do not report	If you:
	• believe that the *client* has no dishonest intent to permanently deprive the overpaying party. Reasons for such a belief may include:
	  ○ Systems operated by the *client* to notify the customer of overpayments.
	  ○ Evidence that requested repayments are processed promptly.
	  ○ Evidence that the *client* has attempted to contact the overpaying party.
	  ○ The *client* has sought and is following legal advice in respect of the overpayments.

Example 3 – Illegal dividends	
Your *client* has paid a dividend based on draft accounts. Subsequent adjustments reduce distributable reserves to the extent that the dividend is now illegal.	
Report	If there is suspicion of fraud.
Do not report	If there is no such suspicion. The payment of an illegal dividend is not a criminal offence under the Companies Act.

Example 4 – Invoices lacking commercial rationale	
Your *client* plans to expand its operations into a new country of operation. They have engaged a consultancy firm to oversee the implementation although it is not clear what the firm's role is. Payments made to the consultancy firm are large in comparison to the services provided and some of the expenses claimed are for significant sums to meet government officials' expenses. The country is one where corruption and facilitation payments are known to be widespread. You ask the Finance Director about the matter and he thought that such payments were acceptable in the country in question.	
Report	If you suspect that bribes have been paid.
Do not report	If you do not suspect illegal payments.
Money laundering offences include conduct occurring overseas which would constitute an offence if it had occurred in the UK.	

Example 5 – Concerted price rises
Your *client's* overseas subsidiary is one of three key suppliers of goods to a particular market in Europe. The subsidiary has recently significantly increased its prices and margins and its principal competitors have done the same. There has been press speculation that the suppliers acted in concert, but publicly they have cited

increased costs of production as driving the increase. Whilst this explains part of the reason for the increase, it is not the only reason because of the increase in margins. On reviewing the accounting records, you see significant payments for consultancy services and seek an explanation. Apparently, they relate to an assessment of the impact of the price increase on the market as well as some compensation for any losses the competitors suffered on their business outside of Europe. Some of the increased profits have flowed back to the UK parent company. There is not a criminal cartel offence under local law but there is under UK law.	
Report	If you suspect a price fixing cartel.
Do not report	If you do not suspect criminal activity.

Example 6 – Breaches of overseas laws	
You suspect that one of your *client's* overseas subsidiaries has been in breach of a number of local laws. In particular, dividends have been paid to the parent company in breach of local exchange control requirements.	
Report	If you suspect that in order for the payment to have been made an act (such as fraud) that would have been a criminal offence had it occurred in the UK, has taken place.
Do not report if	If you decide that no act that would have been a criminal offence had it taken place in any part of the UK, has occurred.
Money laundering offences include conduct occurring overseas which would constitute an offence if it had occurred in the UK (carrying a custodial sentence of 12 months or more). The UK has no exchange control legislation.	

Failure to disclose: defences and exemptions

6.1.19 There are the following defences against failure to disclose:

- There is a reasonable excuse for not making the disclosure. However, it is anticipated that only relatively extreme circumstances – such as duress or threats to safety – would be accepted;
- The privileged circumstances exemption applies (see 6.2.22 of this *guidance*);
- The *relevant employee* concerned did not know about or suspect *MLTF* and had not received the training required by Regulation 21 of the *2017 Regulations*. As no training was provided, the *relevant employee* is not bound by the objective test – i.e., to always report when there are 'reasonable grounds' for knowledge or suspicion – but the *business* has committed an offence by failing to provide training.

OFFENCE: Tipping off

6.1.20 This offence is committed when a *relevant employee* in the *regulated sector* discloses that:

- a *SAR* has been made and this disclosure is likely to prejudice any subsequent investigation; or

- an investigation into allegations of *MLTF* is underway (or being contemplated) and this disclosure is likely to prejudice that investigation.

6.1.21 Considerable care must be taken when communicating with *client*s or third parties after any form of SAR has been made. Before disclosing any of the matters reported it is important to consider carefully whether to do so is likely to constitute an offence of *tipping off* or *prejudicing an investigation* (see 6.1.20 and 6.1.30 of this *guidance*). It is suggested that *businesses* keep records of these deliberations and the conclusions reached (see Section seven of this *guidance*).

6.1.22 No *tipping off* offence is committed under Section 333A of *POCA*, if the relevant person did not know or suspect that their disclosure was likely to prejudice any subsequent investigation.

6.1.23 There are a number of exceptions to this prohibition on disclosing the existence of a *SAR* or an actual or contemplated investigation. A person does not commit an offence if they make a disclosure:

- to a fellow *relevant employee* of the same undertaking; or
- to a *relevant professional adviser* in a different undertaking if both people are located in either an EEA state or a state with equivalent anti-money laundering requirements, and both undertakings share common ownership, management or control; or
- to an *anti-money laundering supervisory authority* as defined by the *2017 Regulations*; or
- for the purposes of the prevention, investigation or prosecution of a criminal offence in the UK or elsewhere, or an investigation under *POCA*, or the enforcement of any court order under *POCA*; or
- following notification that the moratorium period for a *consent SAR* has been extended beyond 31 days, to the subject of the report (provided the content of the *SAR* is not disclosed). *Businesses* may wish to seek legal advice.

6.1.24 An offence is not committed if a *relevant professional adviser* makes a disclosure to another within the same profession (e.g. accountancy) but from a different business, who is of the same professional standing (including with respect to their duties of professional confidentiality and protection of personal data), when that disclosure:

- relates to a single *client* or former *client* of both advisers; and
- involves a transaction or the provision of a service that involves both of them; and
- is made only for the purpose of preventing a money laundering offence; and
- is made to a person in an EU member state or a state imposing equivalent *MLTF* requirements.

6.1.25 No disclosure offence is committed if a *relevant employee* attempts to dissuade their *client* from conduct amounting to an offence. No *tipping off* offence is committed when enquiries are made of a *client* regarding something that properly falls within the normal scope of the *engagement* or *business relationship*. For example, if a *business* discovers an invoice that has not been included on a *client's* tax return, then the *client* should be asked about it.

6.1.26 Although normal commercial enquiries (perhaps to understand a particular transaction) would not generally lead to *tipping off*, care is required nonetheless. Enquiries should be confined to what is required by the ordinary course of business. No attempt should be made to investigate matters unless to do so is within the scope of the professional work commissioned. It is important to avoid making accusations or suggesting that anyone is guilty of an offence.

6.1.27 Continuing work may require that matters relating to the suspicions be discussed with the *client's senior management*. This may be of particular importance in audit relationships.

6.1.28 *Relevant employees* concerned about *tipping off* may wish to consult their *MLRO*. In particular, it is important that documents containing references to the subject matter of any *SAR* is not released to third parties without first consulting the *MLRO* and, in extreme cases, law enforcement. Examples of such documents include:

- public audit or other attestation reports;
- public reports to regulators;
- confidential reports to regulators (e.g., to the FCA under certain auditing standards);
- provision of information to sponsors or other statements in connection with rule 2.12 of the UK's stock exchange listing rules;
- reports under the Company Directors Disqualification Act 1986;
- reports under s218 of the Insolvency Act 1986;
- Companies Act statements on *auditor* resignations;
- professional clearance/etiquette letters;
- communications to *client*s of an intention to resign.

6.1.29 *MLROs* sometimes need advice when formulating instructions to the wider business. Legal advice can be sought from a suitably skilled and knowledgeable professional legal adviser. Recourse can be made to the helplines and support services provided by the professional bodies. Discussion with the *NCA* and law enforcement may also be valuable, but bear in mind that they cannot provide advice and they are not entitled to dictate the conduct of a professional relationship.

OFFENCE: Prejudicing an investigation

6.1.30 Revealing the existence of a law enforcement investigation can lead to an offence of *prejudicing an investigation*. There is a defence if the person who made the disclosure did not know or suspect that it would be prejudicial, or did not know or suspect the documents to be relevant, or did not intend to conceal any facts from the person carrying out the investigation.

6.1.31 Falsification, concealment or destruction of documents relevant to an investigation (or causing the same) can also fall within this offence. Again, there is a defence if it was not known or suspected that the documents were relevant, or there was no intention to conceal facts.

6.2 When and how should an external SAR be made to the NCA?

Is a report required?

6.2.1 There are no hard and fast rules for recognising *MLTF*. It is important for everyone to remain alert to the risks and to apply their professional judgement, experience and scepticism.

6.2.2 *Relevant employees* must ask themselves whether something they have observed in the course of business has the characteristics of *MLTF* and, therefore, warrants a *SAR*. Most *businesses* include in their standard anti-money laundering systems and controls to enable *relevant employees* to discuss, with suitable people, whether their concerns amount to reportable knowledge or suspicion. *Relevant employees* should take advantage of these arrangements.

6.2.3 Once there is the requisite knowledge or suspicion, or reasonable grounds for either, then the *relevant employee* must submit an internal *SAR* to their *MLRO* promptly (or, in exceptional circumstances, straight to the *NCA*).

6.2.4 Deciding whether or not something is suspicious may require further enquiries to be made with the *client* or their records (all within the normal scope of the assignment or *business relationship*). The UK anti-money laundering regime does not prohibit normal commercial enquiries to fulfil *client* duties, and these may help establish whether or not something is properly a cause for suspicion.

6.2.5 Investigations into suspected *MLTF* should not be conducted unless to do so would be within the scope of the *engagement*. Any information sought should be in keeping with the normal conduct of business. Normal business activities should continue (subject to the *business's* consideration of the risks involved), with any information or other matters that flow from included in a *SAR*. To perform additional investigations is not only unnecessary, it is undesirable since it would risk *tipping off* a money launderer.

6.2.6 *Relevant employees* may wish to consider the following questions to assist their decision.

Should I submit a report to the MLRO?

Step	Question
1	• Do I have knowledge or suspicion of criminal activity? or • Am I aware of an activity so unusual or lacking in normal commercial rationale that it causes a suspicion of *MLTF*?
2	• Do I know or suspect that a benefit arose from the activity in 1?
3	• Do I think that someone involved in the activity, or in possession of the proceeds of that activity, knew or suspected that it was criminal?
4	• Can I identify the person (or persons) in possession of the benefit? or • Do I know the location of the benefit? or • Do I have information that will help identify the person (or persons)? or • Do I have information that will help locate the benefits?

6.2.7 If in doubt, always report concerns to the *MLRO*.

Internal reports to the MLRO

6.2.8 Only sole practitioners, who employ no *relevant employees*, have a duty to submit *SARs* straight to the *NCA*.

6.2.9 Section 330 of *POCA* requires all *relevant employees* to make an internal *SAR* to their *MLRO* – reporting to a line manager or colleague is not enough to comply with the legislation. Someone seeking reassurance that their conclusions are reasonable can discuss their suspicions with managers or other colleagues, in line with the *business'* procedures.

6.2.10 When more than one *relevant employee* is aware of the same reportable matter a single *SAR* can be submitted to the *MLRO*, but it should contain the names of all those making the *SAR*. No internal *SAR* should be made in the name of a *relevant employee* who is unaware of the existence of the internal *SAR*. There is no prescribed format for internal *SARs* to be made to an *MLRO*.

Onward reports by the MLRO to the NCA

6.2.11 It is the *MLRO's* responsibility to decide whether the information reported internally needs to be reported to the *NCA*. The *MLRO* is also responsible for deciding whether, (a) *consent* is required from law enforcement for the *engagement* or any aspect of it to continue, and (b) how *client* business should be conducted while a *consent* decision is awaited. Registering with the NCA SAR Online System is recommended to facilitate timely reporting when an external SAR to be made to the *NCA* is necessary.

6.2.12 *MLROs* should approach external reporting with caution. When deciding what to do they should consider the following questions:

- Do I know or suspect (or have reasonable grounds for either) that someone is engaged in *MLTF*?
- Do I think that someone involved in the activity, or in possession of the proceeds of that activity, knew or suspected that it was criminal?
- From the contents of the internal *SAR*, can I identify the suspect or the whereabouts of any laundered property?
- Is an application for *consent* required (see 6.3 of this *guidance*)?
- Do I believe, or is it reasonable for me to believe, that the contents of the internal *SAR* will, or may, help identify the suspect or the whereabouts of any laundered property?
- Can I provide the information essential to an external *SAR* (see 6.2.15 of this *guidance*) without disclosing information acquired in privileged circumstances? The privilege reporting exemption is limited to relevant professional advisers and is available only to members of professional bodies, such as those listed in schedule 1 of the *2017 Regulations*, who also meet the requirements set out in Section 330 (14) of *POCA*. Further guidance on the privilege reporting exemption can be found in 6.2.22 of this *guidance*.

6.2.13 The *MLRO* may want to make reasonable enquiries of other *relevant employees* and systems within the *business*. These may confirm the suspicion, but they may also eliminate it, enabling the matter to be closed without the need for a *SAR*.

6.2.14 There is no prescribed format for an external *SAR* to the *NCA*. Various submission methods are available. The NCA SAR Online System is the *NCA's* preferred submission mechanism. It is available through the *NCA* website and allows *businesses* to make *SARs* in a secure online environment. The *NCA* accepts hard copy *SARs* but will not provide a reference number in response to these.

What information should be included in an external SAR?

6.2.15 Guidance can be found on the NCA website. The following should be regarded as essential information:

- Name of reporter;
- Date of report;
- The name of the suspect or information that may help identify them. This may simply be details of the victim if their identity is known. As many details as possible should be provided to the *NCA* to assist with the identification of the suspect;
- Details of who else is involved, associated, and how;
- The facts regarding what is suspected and why. The 'why' should be explained clearly so that it can be understood without professional or specialist knowledge;
- The relevant NCA glossary code (if applicable);
- The whereabouts of any criminal property, or information that may help locate it, such as details of the victim;
- The actions that the *business* is taking which require consent (see 6.3 of this *guidance*)?

6.2.16 All external *SARs* should be free of jargon and written in plain English.

6.2.17 It is also recommended that reporters:

- do not include confidential information not required by *POCA*;
- show the name of the *business*, individual or *MLRO* submitting the report only once, in the source ID field and nowhere else;
- do not include the names of the *relevant employees* who made the internal *SARs* to the *MLRO*;
- include other parties as 'subjects' only when the information is necessary for an understanding of the external *SAR* or to meet required disclosure standards; and
- highlight clearly any particular concerns the reporter might have about safety (whether physical, reputational or other). This information should be included in the 'reasons for suspicion/disclosure' field.

Confidentiality

6.2.18 A correctly made external *SAR* provides full immunity from action for any form of breach of confidentiality, whether it arises out of professional ethical requirements or a legal duty created by contract (e.g., a non-disclosure agreement).

6.2.19 There will be no such immunity if the external *SAR* is not based on knowledge or suspicion, or if it is intended to be 'defensive' i.e., for the purposes of regulatory compliance rather than because of a genuine suspicion.

Documenting reporting decisions

6.2.20 In order to control legal risks it is important that adequate records of internal *SARs* are kept. This is usually done by the *MLRO* and would normally include details of:

- all internal *SARs* made;
- how the *MLRO* handled matters, including any requests for further information;

- assessments of the information provided, along with any subsequent decisions about whether or not to await developments or seek extra information;
- the rationale for deciding whether or not to make an external *SAR*;
- any advice given to engagement teams about continued working and any *consent* requests made.

These records can be simple or sophisticated, depending on the size of the *business* and the volume of reporting, but they always need to contain broadly the same information and be supported by the relevant working papers. They are important because they may be needed later if the *MLRO* or some other person is required to justify and defend their actions.

6.2.21 For the *MLRO's* efficiency and ease of reference, a reporting index may be kept and each internal *SAR* given a unique reference number.

Reporting and the privileged circumstances exemption

6.2.22 Section 330 (10) of *POCA* contains a privileged circumstances reporting exemption. Members of relevant professional bodies (which are referred to as 'relevant professional advisers') who know about or suspect *MLTF* (or have reasonable grounds for either) are not required to submit a SAR if the information came to them in privileged circumstances (i.e. during the provision of legal advice and acting in respect of litigation). In these circumstances, and as long as the information was not provided with the intention of advancing a crime, then the information must not be reported. The privileged reporting exemption only covers *SARs* and should not be confused with legal professional privilege, which also extends to other documentation and advice.

6.2.23 In Section 330 (14) of *POCA*, *relevant professional adviser* is defined as an accountant, auditor or *tax adviser*:

- who is a member of a relevant professional body; and
- that body makes provision for:
  - testing professional competence as a condition of admission; and
  - imposing and maintaining professional and ethical standards for members along with sanctions for failures to comply.

However, there is no list of the professional bodies that meet these criteria. If *businesses* are in any doubt about whether these provisions apply to them, they should consult their own professional body or seek legal advice.

6.2.24 Whether or not the privilege reporting exemption applies to a given situation is a matter for careful consideration. The *business* may have been providing the *client* with a variety of services, not all of which would create the circumstances required for the exemption. Consequently, it is strongly recommended that careful records are kept about the provenance of the information under consideration when decisions of this kind are being made. Legal advice may be needed.

6.2.25 Set out below are some examples of work which may fall within privileged circumstances.

Advice on tax law to assist a *client* in understanding their tax position; Advice on the legal aspects of a take-over bid;	Assisting a *client* by taking witness statements from him or from third parties in respect of litigation;

Advice on duties of directors under the Companies Act; Advice to directors on legal issues relating to the Insolvency Act 1986; and Advice on employment law.	Representing a *client*, as permitted, at a tax tribunal; and When instructed as an expert witness by a solicitor on behalf of a *client* in respect of litigation.

6.2.26 Audit work, book-keeping, preparation of accounts or tax compliance assignments are unlikely to take place in privileged circumstances.

Discussion with the MLRO

6.2.27 Given the complexity of these matters – as well as the need for a considered and consistent approach to all decisions, supported by adequate documentation – it is recommended that they are always discussed with the *MLRO*.

6.2.28 Where the purpose of these discussions is to obtain advice on making a disclosure under Section 330 of *POCA* they do not affect the applicability of the privilege reporting exemption.

6.2.29 Anyone making an internal *SAR* is entitled to seek advice from an appropriate specialist (either a person within the *business* who falls within requirements of Section 330 (7B) of *POCA* or an external adviser who is similarly entitled to apply the privilege reporting exemption) without affecting the applicability of the privilege reporting exemption.

The crime/fraud exception

6.2.30 Communications that would otherwise qualify for the privilege reporting exemption are excluded from it when they are intended to facilitate or guide someone in committing or advancing some crime or fraud. This is usually the *client* but could be a third party. An example of such a situation could be where a person seeks tax advice ostensibly to regularise their tax affairs but in reality to help them evade tax by improving their understanding of the issues.

6.2.31 Someone worried that they may be guilty of tax evasion can still seek legal advice from a *tax adviser* without fear of the exception being invoked. This remains true even when, having received the advice, the person declines a *business relationship* and the *business* never knows if the irregularities were rectified. However, if that person's behaviour leads the *business* to suspect the advice has been used to further evasion, then a *SAR* could be required.

6.2.32 Whether privileged circumstances apply in a given situation is a difficult question with a fundamentally legal answer. *Businesses* are strongly recommended to seek the advice of a professional legal adviser experienced in these matters.

6.3 What is consent and why is it important?

6.3.1 When preparing to make a *SAR* the *MLRO* must consider carefully whether the *business* would commit a money laundering offence if it continued to act as it intends (usually as instructed by the client). In such cases the *NCA* may, in certain circumstances, provide a defence against money laundering in the form of a *consent* for the activity in question to go ahead.

Matters requiring consent

6.3.2 Before applying for a *consent* it is important to consider whether the *NCA* is in fact able to grant one for the activity in question. The *NCA's* powers in this regard are strictly

limited to activities that would otherwise be offences under Sections 327, 328 or 329 of *POCA* (see APPENDIX A). *Consent* cannot be given for other *POCA* offences, such as tipping off (Section 333A of *POCA*) or *prejudicing an investigation* (Section 342 of *POCA*), or for any offence under any other law.

6.3.3 When in doubt *MLROs* should seek advice from the helpline provided by their supervisory body, or else seek legal advice. The *NCA* will say if something falls outside its powers, but it is not in a position to provide advice about whether or not *consent* is required in any given situation.

6.3.4 Common situations in which *consent* may be required include:

- acting as an insolvency officeholder when there is knowledge or a suspicion that either:
  - all or some assets in the insolvency are criminal property; or
  - the insolvent entity may enter into, or become concerned in, an arrangement under Section 328 of *POCA*;
- designing and implementing trust or company structures (including acting as trustee or company officer) when a suspicion arises that the *client* is, or will be, using them to launder money;
- acting on behalf of a *client* in the negotiation or implementation of a transaction (such as a corporate acquisition) in which there is an element of criminal property being bought or sold by the *client*;
- handling through *client* accounts money that is suspected of being criminal in origin;
- providing outsourced business processing services to *client*s when the money is suspected of having criminal origins.

Applying for and receiving consent

6.3.5 *Consent* may only be sought on the basis of a *SAR* made under the provisions of Section 338 of *POCA* (authorised disclosures). The 'consent required' option should be selected to alert the *NCA* and enable it to prioritise the request.

6.3.6 The request should clearly state the reasons underlying the knowledge or suspicion that has given rise to the *SAR*, as well as the activity in question and the nature of the *consent* required. Great care is needed to make sure the *consent* will cover the nature and extent of the intended activity. It should make clear to the *NCA* exactly what is being requested. Too narrow a *consent* request could mean repeated subsequent requests are needed, adding cost, creating inefficiency and possibly harming service quality. Too broad or poorly-defined a *consent* request, on the other hand, could result in the request being refused by the *NCA* or deemed invalid for not showing clearly which activities would otherwise be offences under Section 327-329 of *POCA*.

6.3.7 If no refusal has been received within the seven working days following the day of submission (this is the notice period) *consent* is deemed to have been given and the activity in question can proceed.

6.3.8 For the best chance of a quick response, any critical timings should be explained clearly, and a complex report should always begin with a summary covering the key facts and the nature of the request.

When consent is refused

6.3.9 If *consent* is refused during the notice period, a further 31 days must pass (starting with the day of refusal) before the activity can continue. This is called the moratorium period. This period can be extended by court order in 31 day increments up to a maximum of 186 days.

6.3.10 It is possible that during either the notice or moratorium periods some law enforcement action (e.g. confiscation) will be taken.

6.3.11 If law enforcement takes no restraining action during the moratorium period, the activity can proceed as originally planned at the end of the moratorium period, however *businesses* may wish to seek legal advice.

Continuation of work while awaiting a consent decision

6.3.12 Once a *consent* request has been made, the activity in question must cease unless and until:

- *consent* has been received; or
- the notice period has expired; or
- *consent* having been refused during the notice period, the moratorium period has now expired.

To do otherwise is to risk prosecution for a money laundering offence.

6.3.13 If no deliverables are provided until after *consent* has been obtained it may be acceptable to continue working. Care is needed to make sure the work does not constitute a money laundering offence, particularly involvement in an arrangement under Section 328 of *POCA* or some other breach of legal or ethical requirements.

6.3.14 In some situations it can be extremely difficult to explain why activity has had to be halted unexpectedly. There is nothing in the *UK AML regime* that requires a *business* to lie to its *clients*, but conversations with the *client* should be kept to a minimum. When informing *clients* or anyone else about such delays the business must consider the risk of *tipping off* or *prejudicing an investigation* and may wish to seek legal advice.

6.4 What should happen after an external SAR has been made?

Client relationships

6.4.1 After a *SAR* has been submitted the business need not stop working unless *consent* has been requested (see 1.3.12 of this *guidance*). The activity in question must not go ahead when *consent* has been sought but refused.

6.4.2 Even when *consent* is not required, if a *SAR* involves a *client* or their close associate the *business* may wish to consider whether the suspicion is such that for professional or commercial reasons it no longer wishes to act for them.

6.4.3 Particular challenges may arise out of the requirement for *auditor*s to file resignation statements at Companies House. Consider these carefully to make sure that statutory and professional duties are met without including information that could constitute *tipping off*. There is no legal mechanism for obtaining *NCA* clearance for these statements or any other documents that might relate to a resignation. In complex cases a *business* may want to discuss the matter with the *NCA* or other law enforcement agency (to understand the law enforcement perspective). Document the discussions carefully. At times, *MLROs* may also need this kind of advice to help them formulate instructions for the wider *business*.

Data protection - including subject access requests

6.4.4 Under the Data Protection Act 1998 *businesses* need not comply with data subject access requests that are likely to prejudice the prevention or detection of crime, or the capture or conviction of offenders. Similarly, personal data that relates to knowledge or suspicion of *MLTF* (i.e., data that has been processed to help prevent or detect crime) need not be disclosed under a subject access request if to do so could constitute *tipping off*. Both of these exceptions apply to the personal data likely to be contained in records relating to internal *MLTF* reports and SARs.

6.4.5 Data exempt from one subject access request may no longer be exempt at the time of a subsequent request (perhaps because the original suspicion has by then been proved false). When a *business* receives a data subject access request covering personal data in its possession, it should always consider whether the exception applies to that specific request regardless of any history of previous requests relating to the same data. These deliberations will usually involve the *MLRO* and the data protection officer. It is recommended that the thinking behind any decision to grant or refuse access is documented.

Production orders, further information orders and other requests for information

6.4.6 The *NCA* or other law enforcement authority may seek further information about a *SAR* (usually via the *MLRO*). *Businesses* should have in place systems to enable a full and rapid response to such enquiries, and any enquiries from law enforcement regarding a *business relationship*. It is recommended that the enquirer's identity is formally verified before a response is provided. This can most easily be done by noting the caller's name and agency/force and then calling them back through their main switchboard. The *NCA* have a contact centre for such purposes.

6.4.7 To the extent that the request is simply to clarify the contents of a *SAR*, a response can be given without further formalities.

6.4.8 If a request is received from NCA other than in relation to a SAR, or from a source other than the NCA, then it is recommended that, any further disclosure should normally be made only in response to the exercise of a statutory power to obtain information (as contained in the relevant legislation) or in line with professional guidance on confidentiality and disclosures in the public interest. This approach is not intended to be uncooperative or obstructive. However, insisting on compulsion will protect the business against accusations of breach of confidentiality. When the *business* is compelled in this way, *client* or other third-party consent is not required, but nor should it be sought because of the risk of *tipping off.*

6.4.9 Before responding to an order to produce information, *businesses* should make sure that they understand:

- the authority under which the request is being made;
- the extent of the information requested;
- the timetable and mechanism for providing the information; and
- what parts of the information should be excluded (i.e., because they are subject to legal privilege).

6.4.10 If in any doubt seek legal advice and keep records of how the issues were judged.

Requests arising from a change of professional advisor (professional enquiries)

Requests regarding CDD information

6.4.11 In this situation the disclosure request can be made under regulation 39 of the *2017 Regulations* (which covers reliance), or else the new adviser may simply want copies of identification evidence to help in its own identification procedures.

6.4.12 *Businesses* should not release confidential information without the *client's* consent. If reliance is being placed on another *business* (see 5.3.25 of this *guidance*) then Section seven of this *guidance* (on record keeping) should be consulted.

Requests for information regarding suspicious activity

6.4.13 It is recommended that these requests are declined. The risk of *tipping off* greatly restricts the ability to make disclosures of this type.

6.4.14 Accountants who are *relevant professional advisers* are reminded that they do not commit a *tipping off* offence if they share information with another accountant of similar standing provided the information satisfies all of the following:

- it relates to the same *client* or former *client* of both advisers;
- it covers a transaction or provision of services that involved both of them;
- it was disclosed only for the purpose of preventing a money laundering offence;
- it was disclosed to a person in an EU member state or another state which imposes equivalent anti-money laundering requirements.

Reporting to other bodies

6.4.15 *Businesses* should have regard to their other obligations, such as their reporting responsibilities under the International Auditing Standards, statutory regulatory returns, or the reporting of misconduct by fellow members of a professional body. In all these cases the risk of tipping off must be considered and the offence avoided. Accountants may wish to contact their professional body for advice, or else seek legal advice.

6.4.16 A *tipping off* offence is not committed under Section 333A of *POCA*, if the *relevant employee* did not know or suspect that they were likely to prejudice any subsequent investigation. Situations in which this defence can apply include:

- reporting to your own professional body if it is an *anti-money laundering supervisory authority* (Section 333D of *POCA*);
- reporting a matter of material significance to the UK charity regulators: Charities Commission for England and Wales, Office of the Scottish Charity Regulator and Charity Commission for Northern Ireland.

7 RECORD KEEPING

- Why may existing document retention policies need to be changed?
- What should be considered regarding retention policies?
- What considerations apply to *SARs* and consent requests?
- What considerations apply to training records?
- Where should reporting records be located?
- What do businesses need to do regarding third-party arrangements?
- What are the requirements regarding the deletion of personal data?

7.1 Why may existing document retention policies need to be changed?

7.1.1 Records relating to *CDD*, the *business relationship* and *occasional transactions* must be kept for five years from the end of the *client* relationship.

7.1.2 All records related to an *occasional transaction* must be retained for five years after the date of the transaction.

7.1.3 The *2017 Regulations* do not specify the medium in which records should be kept, but they must be readily retrievable.

7.2 What should be considered regarding retention policies?

7.2.1 *Businesses* must be aware of the interaction between of *MLTF* laws and regulations with the requirements of the Data Protection Regime. The Data Protection Regime requires that personal information be subject to appropriate security measures and retained for no longer than necessary for the purpose for which it was originally acquired.

7.3 What considerations apply to SARs and consent requests?

7.3.1 No retention period is officially specified for records relating to:

- internal reports;
- the *MLRO's* consideration of internal reports;
- any subsequent reporting decisions;
- issues connected to *consent*, production of documents and similar matters;
- suspicious activity reports and consent requests sent to the *NCA*, or its responses.

7.3.2 Since these records can form the basis of a defence against accusations of MLTF and related offences, *businesses* may decide that five years is a suitable retention period for them.

7.4 What considerations apply to training records?

7.4.1 *Businesses* must demonstrate their compliance with regulations that place a legal obligation on them to make sure that certain of their *relevant employees* are, (a) aware of the law relating to *MLTF*, and (b) trained regularly in how to recognise and deal with transactions and other events which may be related to *MLTF*.

7.4.2 These records should show the training that was given, the dates on which it was given, which individuals received the training and the results from any assessments.

7.5 Where should reporting records be located?

7.5.1 Records related to internal and external *SARs* of suspicious activity are not part of the working papers relating to *client* assignments. They should be stored separately and securely as a safeguard against *tipping off* and inadvertent disclosure to someone making routine use of *client* working papers.

7.6 What do businesses need to do regarding third-party arrangements?

7.6.1 A *business* may arrange for another organisation to perform some of its AML related activities – *CDD* or training, for example. In which case, it must also ensure that the other party's record keeping procedures are good enough to demonstrate compliance with the *MLTF* obligations, or else it must obtain and store copies of the records for itself. It must also consider how it would obtain its records from the other party should they be needed, as well as what would happen to them if the other party ceased trading.

7.7 What are the requirements regarding the deletion of personal data?

7.7.1 Regulation 39(4) of the 2017 Regulations require that once the periods specified in 7.1 of this *guidance* have expired, the *business* deletes any personal data unless:

- The *business* is required to retain it under statutory obligation, or
- the *business* is required to retain it for legal proceedings, or
- the data subject has consented to the retention.

7.7.2 The *business* is not required to keep any records for more than 10 years after the end of the *business relationship*.

8 TRAINING AND AWARENESS

- Who should be trained and who is responsible for it?
- What should be included in the training?
- When should training be completed?

8.1 Who should be trained and who is responsible for it?

8.1.1 The regulations require that all '*relevant employees*' (including partners) are made aware of *MLTF* law and are trained regularly to recognise and deal with transactions which may be related to *MLTF*, as well as to identify and report anything that gives grounds for suspicion (see Section six of this *guidance*).

8.1.2 Thought should also be given to who else might need AML training.

8.1.3 A designated person should be made responsible for the detail of AML training. This could be the *MLRO* or a member of *senior management*. There should be a mechanism to ensure that *relevant employees* complete their AML training promptly.

8.1.4 Someone accused of a failure-to-disclose offence has a defence if:

- they did not know or suspect that someone was engaged in money laundering even though they should have; but
- their employer had failed to provide them with the appropriate training.

8.1.5 This defence – that the *relevant employee* did not receive the required AML training – is likely to put the *business* at risk of prosecution for a regulatory breach.

8.2 What should be included in the training?

8.2.1 Training can be delivered in several different ways: face-to-face, self-study, e-learning, video presentations, or a combination of all of them.

8.2.2 The programme itself should include:

- an explanation of the law within the context of the *business's* own commercial activities;
- so-called 'red flags' of which *relevant employees* should be aware when conducting business, which would cover all aspects of the MLTF procedures, including CDD (for example those that might prompt doubts over the veracity of evidence provided) and SARs (for example what might prompt suspicion); and
- how to deal with transactions that might be related to *MLTF* (including how to use internal reporting systems), the *business's* expectations of confidentiality, and how to avoid *tipping off* (see Section six of this *guidance*);
- The relevant data protection requirements

8.2.3 Training programmes should be tailored to each business area and cover the *business'* procedures so that *relevant employees* understand the *MLTF* risks posed by the specific services they provide and types of *client* they deal with, and so are able to appreciate, on a case-by-case basis, the approach they should be taking. Furthermore, *businesses* should aim to create an AML culture in which relevant employees are always alert to the risks of *MLTF* and habitually adopt a risk based approach to *CDD*.

8.2.4 Records should be kept showing who has received training, the training received and when training took place (see 7.4 of this *guidance*). These records should be used so as to inform when additional training is needed – e.g. when the *MLTF* risk of a specific business area changes, or when the role of a *relevant employee* changes.

8.2.5 A system of tests, or some other way of confirming the effectiveness of the training, should be considered.

8.2.6 The overall objective of training is not for *relevant employees* to develop a specialist knowledge of criminal law. However, they should be able to apply a level of legal and business knowledge that would reasonably be expected of someone in their role and with their experience, particularly when deciding whether to make an internal *SAR* to the *MLRO*.

8.3 When should training be completed?

8.3.1 *Businesses* need to make sure that new *relevant employees* are trained promptly.

8.3.2 The frequency of training events can be influenced by changes in legislation, regulation, professional guidance, case law and judicial findings (both domestic and international), the *business'* risk profile, procedures, and service lines.

8.3.3 It may not be necessary to repeat a complete training programme regularly, but it may be appropriate to provide *relevant employees* with concise updates to help refresh and expand their knowledge and to remind them how important effective anti-money laundering work is.

8.3.4 In addition to training, *businesses* are encouraged to mount periodic *MLTF* awareness campaigns to keep *relevant employees* alert to individual and firm-wide responsibilities.

GLOSSARY

2017 Regulations The Money Laundering Regulations, Terrorist Financing and Transfer of Funds Regulations 2017, SI 2017/692

Accountancy services For the purpose of this guidance this includes any service provided under a contract for services (i.e., not under a contract of employment) which requires the recording, review, analysis, calculation or reporting of financial information.

Anti-money laundering supervisory authority A body identified by Regulation 7 of the *2017 Regulations* as being empowered to supervise the compliance of businesses with the *2017 Regulations*. The professional bodies designated as anti-money laundering supervisory authorities are listed in Schedule 1 of the *2017 Regulations*.

Arrangement Any activity that facilitates money laundering, including planning and preparation.

Auditor Any business or individual who is — a statutory auditor within the meaning of Part 42 of the Companies Act 2006(a) (statutory auditors), when carrying out statutory audit work within the meaning of Section 1210 of that Act (meaning of statutory auditor), or (ii) a local auditor within the meaning of Section 4(1) of the Local Audit and Accountability Act 2014 (general requirements for audit) (b), when carrying out an audit required by that Act.

Business / Businesses A company, partnership, individual or other organisation which undertakes defined services. This includes accountancy practices, whether structured as partnerships, sole practitioners or corporates.

Business relationship a business, professional or commercial relationship between a relevant person and a customer, which—

(a) arises out of the business of the relevant person, and

(b) is expected by the relevant person, at the time when contact is established, to have an element of duration.

CCAB The Consultative Committee of Accountancy Bodies represents the Institute of Chartered Accountants in England and Wales, the Institute of Chartered Accountants of Scotland, the Institute of Chartered Accountants in Ireland, the Association of Chartered Certified Accountants and the Chartered Institute of Public and Finance and Accountancy.

Client Someone in a business relationship, or carrying out an occasional transaction, with a business.

Consent Permission to carry out any activity which would constitute a money laundering offence without that permission. Generally granted by the NCA. The definition of, and governing legislation for, consents can be found in s335 of POCA, which also deals with the passing of consent from the MLRO to the individual concerned s336 of POCA.

Criminal property The benefit of criminal conduct where the alleged offender knows or suspects that the property in question represents such a benefit (s340 of POCA).

Customer Due Diligence (CDD) The process by which the identity of a client is established and verified, for both new and existing clients.

Defined services Activities performed in the course of business by organisations or individuals as *auditor*s, external accountants, insolvency practitioners or tax advisers (Regulation 8(c), *2017 Regulations*), or as trust and company services providers (Regulation 8(e), *2017 Regulations*). It also includes services under the designated professional body provisions of part XX, Section 326 of *FSMA*

2000 or otherwise providing financial services under the oversight of the appropriate professional body.

De minimis

EEA European Economic Area. Countries which form the combined membership of the European Union (EU) and the European Free Trade Association (EFTA).

Engagement agreement concerning the delivery of a specific service within a business relationship.

EU directive Refers in this document to the Fourth Money Laundering Directive.

External accountant A firm or sole practitioner who by way of business provides accountancy services to other persons when providing such services (Regulation 11(C), *2017 Regulations*).

Family member of a politically exposed person includes spouse or civil partner; children of that person and their spouses and partners; and parents of that person.

FATF Financial Action Task Force. Created by G7 nations to fight money laundering.

FSMA 2000 Financial Services and Markets Act 2000.

Guidance Advice which is: (a) issued by a supervisory authority or any other appropriate body; (b) approved by HM Treasury; and (c) published in a manner approved by HM Treasury as suitable for bringing it to the attention of persons likely to be affected by it. In this document the term also includes guidance for which Treasury approval has been sought and is expected to be granted. Any use of the term 'guidance' which falls outside of this definition will not have been italicised in this document. *POCA* and the *2017 Regulations* both set out the circumstances in which the courts (and others) are required to take account of *guidance* when determining whether an offence has been committed.

Independent legal professional Provider of legal or notarial services as defined in Regulation 12(1), *2017 Regulations*.

Internal report A report made to the *MLRO* of a *business*.

Insolvency practitioner Any business who acts as an insolvency practitioner within the meaning of s388, Insolvency Act 1986, or art 3, Insolvency (Northern Ireland) Order 1989 (Regulation 11(2), *2017 Regulations*).

JMLSG The Joint Money Laundering Steering Group is the body representing UK trade associations in the financial services industry which aims to promote good practice in anti-money laundering and to provide relevant practical guidance.

Known close associate of a politically exposed person means an individual known to have joint beneficial ownership of a legal entity/arrangement or any other close business relations with a politically exposed person; or an individual who has sole beneficial ownership of a legal entity or a legal arrangement which is known to have been set up for the benefit of a politically exposed person (Regulation 35(12) the *2017 Regulations*).

MLTF (money laundering and terrorist financing) Defined for the purposes of this document to include those offences relating to terrorist finance which are required to be reported under *TA 2000* as well as the money laundering offences defined by *POCA*.

Moratorium period The 31 days following refusal of a consent request during which time the activity for which consent was sought must cease. Law enforcement may take action during this period.

MLRO Money laundering reporting officer.

Money laundering reporting officer See *MLRO*, above.

Nominated officer the person who is nominated to receive disclosures under Part 7 POCA or Part 3 TA 2000.

NCA National Crime Agency or equivalent successor body (UKFIU).

Notice period The seven working days following a consent request within which the NCA must respond and during which the activity for which *consent* is sought must cease until granted.

Occasional transaction A transaction which occurs outside of a business relationship and has a value of more than €15,000.

PEPs Politically exposed persons. As defined in Regulation 35(12), *2017 Regulations*. An individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official. Prominent public functions include head of state, head of government, minister and deputy or assistant ministers; members of parliament or of similar legislative bodies; members of the governing bodies of political parties;, members of supreme courts, members of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances; members of courts of auditors or of boards of central banks; ambassadors, charges d'affaires and high ranking officers in the armed forces; members of the administrative, management or supervisory bodies of state-owned enterprises; directors, deputy directors and members of the board or equivalent function of an international organisation.

POCA Proceeds of Crime Act 2002

Prejudicing an investigation An offence related to money laundering, defined under s342, *POCA*. In summary, it captures the following: disclosure of information likely to prejudice an investigation; falsifying, concealing or destroying documents relevant to a money laundering investigation; or being complicit in behaviour of that sort.

Regulated investment market Within the *EEA* this has the meaning given by point 14, art 4(1), Markets in Financial Instruments Directive 2004/39/EC (or MiFID). Outside the EEA it means a regulated financial market in which the listed companies are subject to the disclosure obligations contained in international standards equivalent to the specified disclosure obligations.

Regulated sector As defined in Schedule 9, part 1, *POCA* (includes those who provide *defined services*).

Relevant employee An employee (including partner) whose work is relevant to compliance with the Regulations, or is otherwise capable of contributing to the identification and mitigation of the risks of money laundering and terrorist financing to which the business is subject, or to the prevention or detection of money laundering and terrorist financing in relation to the business.

Relevant professional adviser An accountant, *auditor* or tax adviser who is a member of a professional body which: (a) tests competence as a condition of admission to membership; and (b) imposes and maintains professional and ethical standards for its members, with sanctions for non-compliance.

Required disclosures The identity of a suspect (if known); the information or other material on which the knowledge or suspicion of money laundering (or reasonable grounds for it) is based; and the whereabouts of the laundered property (if known).

SAR Suspicious activity report.

SAR glossary of terms Glossary of key terms used by the NCA to give theme to individual SARs and so increase the effectiveness of data mining by the NCA and law enforcement. The general use of these terms is not mandatory.

Senior management means an officer or employee with sufficient knowledge of the firm's *MLTF* risk exposure, and of sufficient authority to take decisions regarding its risk exposure (for example, having a role in determining whether high risk clients are taken on).

SOCPA Serious Organised Crime and Police Act 2005

Source of funds The origin of the funds that are the subject of the business relationship.

Source of wealth The origin of the subject's total assets.

Suspicious activity report Otherwise known as a *SAR* (see above).

TA 2000 The Terrorism Act 2000 (as amended by the Anti-Terrorism, Crime and Security Act 2001 and the *Terrorism Act 2006*).

TA 2006 The Terrorism Act 2006.

Tax adviser A firm or sole practitioner who by way of business provides advice about the tax affairs of others, when providing such services (Regulation 11(4) of the *2017 Regulations*). Tax compliance services – e.g., assisting in the completion and submission of tax returns – is for the purpose of this document included within the term 'advice about the tax affairs of others'.

Terrorist financing offences These offences relate to:

- fundraising (s15 TA 2000 (inviting others to provide money or other property with the intention that it will be used for the purposes of terrorism, or with the reasonable suspicion that it will));
- using or possessing terrorist funds (s16 TA 2000 (receiving or possessing money or other property with the intention, or the reasonable suspicion, that it will be used for the purposes of terrorism));
- entering into funding arrangements (s17 TA 2000 (making arrangements as a result of which money or other property is, or may be, made available for the purposes of terrorism – this includes where there is reasonable cause for suspicion));
- money laundering (s18 TA 2000);
- disclosing information related to the commission of an offence (s19 TA 2000); and
- failing to make a disclosure in the regulated sector (ss19 and 21A TA 2000 (as amended)).

Tipping off A money laundering-related offence for the regulated sector, defined under s333A-D, POCA.

UK AML Regime UK anti-money laundering and terrorist financing regime

APPENDIX A: LEGISLATIVE SUMMARIES – PROCEEDS OF CRIME ACT 2002

s327

A person commits an offence if he **conceals, disguises, converts, transfers or removes criminal property** from England and Wales or from Scotland or from Northern Ireland.

s328

A person commits an offence if he **enters into or becomes concerned in an arrangement which he knows or suspects facilitates** (by whatever means) the **acquisition, retention, use or control of criminal property** by or on behalf of another person.A person **does not commit** the offences above if:

a) He makes an authorised disclosure under Section 338 and (if the disclosure is made before he does the act mentioned in sub Section (1)) he has the appropriate consent;

b) He intended to make such a disclosure but had a reasonable excuse for not doing so;

c) The act he does is done in carrying out a function he has relating to law enforcement.

s329

A person commits an offence if he **acquires, uses, or has possession of criminal property**. In addition to the s327/328 defences there is also available the defence of having acquired possession of the property for adequate consideration.

s330 Failure to disclose: Regulated sector

A person commits an offence if, during the course of business he develops knowledge or suspicion (or has reasonable grounds for doing so) that another person is engaged in money laundering, and he does not make the required disclosure as soon as is practicable.

The required disclosure is a disclosure of the information or other matter to the MLRO or the NCA.

A person does not commit an offence under this Section if:

a) He has a reasonable excuse for not disclosing the information or other matter;

b) He is a professional legal adviser and the information or other matter came to him in privileged circumstances;

c) He has no actual knowledge or suspicion and has not received AML training.

s333 Tipping off: Regulated sector

A person commits an offence if he knows or suspects that a disclosure has been made, and he makes a disclosure which is likely to prejudice any investigation which might be conducted following the disclosure.

s342 Prejudicing an investigation

A person commits an offence if he knows or suspects that an appropriate officer is conducting or about to conduct a confiscation investigation, a civil recovery investigation, a detained cash investigation or a money laundering investigation and either makes a disclosure which is likely to prejudice it or falsifies, conceals, destroys or otherwise disposes of relevant document or causes another to do so.

APPENDIX B: OUTSOURCING, SUBCONTRACTING AND SECONDMENTS

B.1 Outsourcing and subcontracting arrangements

B.1.1 Where a *business* chooses to outsource or subcontract work to a third party it is still obliged to maintain appropriate risk management procedures to prevent *MLTF*. This also requires the *business* to consider whether the outsourcing or subcontracting increases the risk that it will be involved in, or used for, *MLTF*, in which case appropriate controls to address that risk should be put in place.

B.1.2 Where a *business* contracts with a *client*, it remains responsible for ensuring that it undertakes *CDD* to UK standards, including maintaining the appropriate records even if execution of all or part of the *client* work is outsourced or sub-contracted out. Some aspects of *CDD* such as collecting documentary evidence can also be delegated to an outsourcer or sub-contractor, but the business remains responsible for compliance with UK legislation.

B.1.3 Regardless of any outsourcing or subcontracting arrangement, a *business* remains responsible for reporting any knowledge or suspicion of *MLTF* that comes to it in the course of its own *business*. However a *business* is not responsible for reporting knowledge or suspicion that comes to the attention of the outsourcer or sub-contractor, where such knowledge or suspicion has not been passed on to the *business*. Although there is no legal obligation for an outsourcer or subcontractor to report knowledge or suspicion of *MLTF* to a *business*, if such a *SAR* is made, then the *business* should consider their own reporting obligations. When a sub-contractor is integrated into a UK business it may be appropriate for its *relevant employees* to be trained in the *MLTF* procedures adopted by that *business* so that common standards can be observed.

B.2 Secondees and those temporarily working outside the UK

B.2.1 A secondee is an individual employed by one organisation (the seconder) but acting as an employee of another (the receiver). The formal terms of all secondments should make clear to all concerned how the obligations imposed by the *UK AML regime* will be applied.

B.2.2 The position of a secondee working temporarily outside the UK or on foreign secondments, or working permanently outside the UK but still within a UK *business* is difficult. For example the duty to report may be influenced by the terms of the secondment. Issues to consider include:

- If the work outside the UK is part of a UK defined service then in some circumstances it will be reportable.
- If an individual works permanently outside the UK for a UK *business*, it may be appropriate to consider whether they are working at a separate *business* or at a branch office of a UK *business*.
- An individual should be particularly cautious about any decision not to make a SAR on their return to the UK if the information relates to work that they are undertaking in the UK.

B.2.3 Arrangements must be considered on their own facts to determine which policies and procedures the secondee should follow. *Businesses* may wish to take legal advice in relation to the need for their relevant employees to comply with the UK's money laundering reporting regime as well as any local legal requirements, and in relation to the drafting of appropriate secondment agreements.

B.3 Reporting requirements for subcontractors and secondees

B.3.1 Where all or part of a piece of work is contracted-out there is no legal requirement for the subcontractor to report suspicious activity to the referring *business' MLRO*. However, where the subcontractor notifies the referring *business* of information which gives rise to a MLTF suspicion, the referring *business* must consider its own reporting obligations.

APPENDIX C: CLIENT VERIFICATION

Documentation purporting to offer evidence of identity may emanate from a number of sources. These documents differ in their integrity, reliability and independence. Some are issued after due diligence on an individual's identity has been undertaken; others are issued on request, without any such checks being carried out. There is a broad hierarchy of documents:

- certain documents issued by government departments and agencies, or by a court; then
- certain documents issued by other public sector bodies or local authorities; then
- certain documents issued by regulated firms in the financial services sector; then
- those issued by other firms subject to the Regulations, or to equivalent legislation; then
- those issued by other organisations.

C.1 Individuals

Client identification:

The full name, date of birth and residential address should be obtained.

Client Verification:

A document issued by an official (e.g., government) body is deemed to be independent and reliable source even if provided by the *client*. Documents should be valid and recent. Documents sourced online should not be accepted if there is any suspicion regarding the provenance of the documents. The following is a suggested non-exhaustive list of sources of evidence.

Risk Profile	Verification
Individual deemed normal risk	The original, or an acceptably certified copy, of one of the following documents or similar should be seen and a copy retained: • valid passport • valid photo card driving licence • national Identity card (non UK nationals) • identity card issued by the Electoral Office for Northern Ireland
Individual deemed high risk	The original of one of the following documents or similar should be seen and a copy retained: • valid passport • valid photo card driving licence • national identity card (non UK nationals) • identity card issued by the Electoral Office for Northern Ireland
	In addition The original of a second document should be seen and a copy retained. This should be one of the following: • A valid UK driving licence. • Recent evidence of entitlement to a state- or local authority-funded benefit (including housing benefit, council tax benefit, tax credits, state pension, educational or other grant). • Instrument of a court appointment (such as a grant of probate).

	• Current council tax demand letter or statement. • HMRC-issued tax notification (NB: employer-issued documents such as P60s are not acceptable). • End of year tax deduction certificates. • Current bank statements or credit/debit card statements. • Current utility bills.

Source of wealth and source of funds

C.1.2 Where appropriate, evidence can be obtained from searching public information sources like the internet, company registers and land registers.

C.1.3 If the *client*'s funds/wealth have been derived from, say, employment, property sales, investment sales, inheritance or divorce settlements, then it may be appropriate to obtain documentary proof.

C.2 Private companies/LLPs

Client identification

C.2.1 The following information must be obtained and verified:

- full name of company
- registered number
- registered office address and, if different, principal place of business
- any shareholders/members who ultimately own or control more than 25% of the shares or voting rights (directly or indirectly including bearer shares), or any individual who otherwise exercises control over management must be identified (and verified on a risk sensitive basis).
- The identity of any agent or intermediary purporting to act on behalf of the entity and their authorisation to act e.g., where a lawyer engages on behalf of an underlying *client*.

Unless the entity is listed on a regulated market, reasonable steps should be taken to determine and verify:

- the law to which it is subject
- its constitution (for example via governing documents)
- the full names of all directors (or equivalent) and senior persons responsible for the operations of the company.

Company registers of beneficial ownership may be used but not solely relied upon.

C.3 Listed or regulated entity

Client identification

C.3.1 The following information should be gathered:

- full name
- membership or registration number
- address

Client verification

Risk Profile	Recommended verification
Normal/ high risk	One of the following documents should be seen and a copy retained: • a printout from the web-site of the relevant regulator or exchange (which should be annotated); • written confirmation of the entity's regulatory or listing status from the regulator or exchange.

C4. Government or similar bodies

Client identification

C.4.1 The following information should be gathered:

- full name of the body
- main place of operation
- government or supra-national agency which controls it

Client verification

Risk Profile	Recommended verification
Normal/ high risk	One of the following documents should be seen and a copy retained: • a printout from the web-site of the relevant body (which should be annotated). Additionally for housing associations: • the printout must contain its registered number, registered company number (where appropriate) and registered address.

APPENDIX D

Should I report to the MLRO?

- Do I have knowledge or suspicion of criminal activity resulting in someone benefitting?
- Am I aware of an activity so unusual or lacking in normal commercial rationale that it causes a suspicion of money laundering?
- Do I know or suspect a person or persons of being involved in crime, or does another person who I can name have information that might assist in identifying them?
- Do I know who might have received the benefit of the criminal activity, or where the criminal property might be located, or have I got any information which might allow the property to be located?
- Do I think that the person(s) involved in the activity knew or suspected that the activity was criminal?
- Can I explain my suspicions coherently?

As the MLRO, should I report externally?

- Do I know, suspect or have reasonable grounds to know or suspect that another person is engaged in money laundering; **and**
- did the information or other matter giving rise to the knowledge or suspicion come to me in a disclosure made under s 330, POCA; **and**
- do I know the name of the other person or the whereabouts of any laundered property from the s 330 disclosure; or
- can I identify the other person or the whereabouts of any laundered property from information or other matter contained in the s 330 disclosure; or
- do I believe, or is it reasonable for me to believe, that the information or other matter contained in the s 330 disclosure will or may assist in identifying the other person or the whereabouts of any laundered property.
- Does the privileged circumstances exemption apply?
- Is consent required?

CHECKLIST: Essential elements of a SAR

- Name of reporter.
- Date of report.
- Who is suspected or information that may assist in ascertaining the identity of the suspect (which may simply be details of the victim and the fact that the victim knows the identity but this is not information to which the business is privy in the ordinary course of its work). The reporter should provide as many details as possible to allow NCA to identify the main subject.
- Who is otherwise involved in or associated with the matter and in what way.
- The facts.
- What is suspected and why
- Information regarding the whereabouts of any criminal property or information that may assist in ascertaining it (which may simply be the details of the victim who has further information but this is not information to which the business is privy in the ordinary course of its work).
- What involvement does the business have with the issue in order that requirements for consent.
- Reports should generally be jargon free and written in plain English.

APPENDIX E: RISK FACTORS

High risk factors

Customer risk factors, including whether—

i. the business relationship is conducted in unusual circumstances;

ii. the customer is resident in a geographical area of high risk (see below);

iii. the customer is a legal person or legal arrangement that is a vehicle for holding personal assets;

iv. the customer is a company that has nominee shareholders or shares in bearer form;

v. the customer is a business that is cash intensive;

vi. the corporate structure of the customer is unusual or excessively complex given the nature of the company's business;

Product, service, transaction or delivery channel risk factors, including whether—

i. the product involves private banking;

ii. the product or transaction is one which might favour anonymity;

iii. the situation involves non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;

iv. payments will be received from unknown or unassociated third parties;

v. new products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products;

vi. the service involves the provision of nominee directors, nominee shareholders or shadow directors, or the formation of companies in a third country;

Geographical risk factors, including—

i. countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering or terrorist financing;

ii. countries identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism (within the meaning of Section 1 of the Terrorism Act 2000(a)), money laundering, and the production and supply of illicit drugs;

iii. countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;

iv. countries providing funding or support for terrorism;

v. countries that have organisations operating within their territory which have been designated—

(aa) by the government of the United Kingdom as proscribed organisations under Schedule 2 to the Terrorism Act 2000(a), or

(bb) by other countries, international organisations or the European Union as terrorist organisations;

vi. countries identified by credible sources, such as evaluations, detailed assessment reports or published follow-up reports published by the Financial Action Task Force, the International Monetary Fund, the World Bank, the Organisation for Economic Co-operation and Development or other international bodies or non-governmental organisations as not implementing requirements to counter money laundering and terrorist financing that are consistent with the recommendations published by the Financial Action Task Force in February 2012 and updated in October 2016.

Low risk factors

Customer risk factors, including whether the customer—

i. is a public administration, or a publicly owned enterprise;

ii. is an individual resident in a geographical area of lower risk (see sub-paragraph (c));

iii. is a credit institution or a financial institution which is—

(aa) subject to the requirements in national legislation implementing the fourth money laundering directive as an obliged entity (within the meaning of that directive), and

(bb) supervised for compliance with those requirements in accordance with Section 2 of Chapter VI of the fourth money laundering directive;

iv. is a company whose securities are listed on a regulated market, and the location of the regulated market;

Product, service, transaction or delivery channel risk factors, including whether the product or service is—

i. a life insurance policy for which the premium is low;

ii. an insurance policy for a pension scheme which does not provide for an early surrender option, and cannot be used as collateral;

iii. a pension, superannuation or similar scheme which satisfies the following conditions—

(aa) the scheme provides retirement benefits to employees;

(bb) contributions to the scheme are made by way of deductions from wages; and

(cc) the scheme rules do not permit the assignment of a member's interest under the scheme;

iv. a financial product or service that provides appropriately defined and limited services to certain types of customers to increase access for financial inclusion purposes in an EEA state;

v. a product where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership;

vi. a child trust fund within the meaning given by Section 1(2) of the Child Trust Funds Act 2004(a);

vii. a junior ISA within the meaning given by regulation 2B of the Individual Savings Account Regulations 1998(**b**);

Geographical risk factors, including whether the country where the customer is resident, established or registered or in which it operates is—

i. an EEA state;

ii. a third country which has effective systems to counter money laundering and terrorist financing;

iii. a third country identified by credible sources as having a low level of corruption or other criminal activity, such as terrorism (within the meaning of Section 1 of the Terrorism Act 2000(c)), money laundering, and the production and supply of illicit drugs;

iv. a third country which, on the basis of credible sources, such as evaluations, detailed assessment reports or published follow-up reports published by the Financial Action Task Force, the International Monetary Fund, the World Bank, the Organisation for Economic Co-operation and Development or other international bodies or nongovernmental organisations—

(aa) has requirements to counter money laundering and terrorist financing that are consistent with the revised Recommendations published by the Financial Action Task Force in February 2012 and updated in October 2016; and

(bb) effectively implements those Recommendations.