

# Anti-Money Laundering Guidance for the Legal Sector

Legal Sector Affinity Group

April 2025

Professional Bookshop  
[www.pbookshop.com](http://www.pbookshop.com)



The Law  
Society

All rights reserved. No part of this publication may be reproduced in any material form, whether by photocopying, scanning, downloading onto computer or otherwise without the written permission of the Law Society except in accordance with the provisions of the Copyright, Designs and Patents Act 1988. Applications should be addressed in the first instance, in writing, to Law Society Publishing. Any unauthorised or restricted act in relation to this publication may result in civil proceedings and/or criminal prosecution.

Whilst all reasonable care has been taken in the preparation of this publication, neither the publisher nor the authors can accept any responsibility for any loss occasioned to any person acting or refraining from action as a result of relying upon its contents.

The views expressed in this publication should be taken as those of the authors only unless it is specifically indicated that the Law Society has given its endorsement.

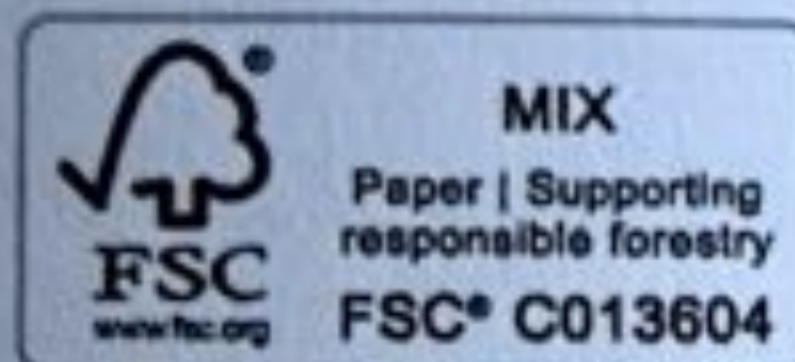
© The Law Society 2025

Crown copyright material is reproduced with the permission of the Controller of His Majesty's Stationery Office

ISBN-13: 978-1-78446-288-8

Published in 2025 by the Law Society  
113 Chancery Lane, London WC2A 1PL

Typeset by Data Standards Ltd, Frome, Somerset  
Printed by CPI Group (UK) Ltd, Croydon CR0 4YY



The paper used for the text pages of this book is FSC® certified. FSC (the Forest Stewardship Council®) is an international network to promote responsible management of the world's forests.

## Contents

<b>1</b>	<b>The Status of this Guidance and Terminology Used</b>	<b>1</b>
1.1	Status	1
1.2	Terminology	1
<b>2</b>	<b>Background</b>	<b>3</b>
<b>3</b>	<b>High-Level Compliance Principles</b>	<b>4</b>
3.1	Introduction and context	4
3.2	Compliance Principles	4
<b>4</b>	<b>AML Governance and Policies, Controls and Procedures</b>	<b>8</b>
4.1	Overview	8
4.2	Approvals, Roles and Positions	9
4.3	Money Laundering Reporting Officer (otherwise known as Nominated Officer)	11
4.4	Money Laundering Compliance Officer (MLCO)	13
4.5	Practices with both a MLRO and a MLCO	14
4.6	Senior Management Responsibilities	14
4.7	Informing your Supervisor of MLRO and MLCO Appointments and registering for the Economic Crime Levy	15
4.8	Policies, Controls and Procedures (PCPs)	15
<b>5</b>	<b>AML Risk Assessments</b>	<b>18</b>
5.1	Risk Assessments and the Risk Based Approach	18
5.2	Assessing Risk	20
5.3	Practice Wide Risk Assessment (PWRA) – Introduction	20
5.4	Assessing your practice's risk profile	24
5.5	Reviewing the PWRA	27
5.6	Risk Factors for consideration at all levels of Risk Assessment	27
5.7	Conclusions of a Risk Assessment	36
5.8	Application of Risk Assessments	37
5.9	Client and Matter Risk Assessments	37
5.10	Client Risk Assessments	38
5.11	Matter-Level Risk Assessments	39
5.12	Undertaking Client/Matter Risk Assessments	40
5.13	Risk Weightings	41
5.14	Recording and Documenting Risk Assessments	42
5.15	Application of Risk Assessments	43
5.16	Risk Mitigation	43

<b>6</b>	<b>Client Due Diligence</b>	
6.1	General Comments	46
6.2	Long-standing/Personal Relationships	47
6.3	Application of CDD	47
6.4	Definition of Business Relationship	48
6.5	Definition of an occasional transaction	48
6.6	Intermediaries, agents or representatives	48
6.7	Referrals to another legal practice (or referrals between other entities in scope of the regulations)	49
6.8	Timing of CDD	50
6.9	What happens when you cannot complete CDD?	50
6.10	Exceptions to the timing requirement	51
6.11	Undertaking CDD on Clients	51
6.12	Identification and verification	52
6.13	A risk-based approach	53
6.14	Methods of verification	53
6.15	Beneficial ownership requirements	53
6.16	CDD on a beneficial owner	72
6.17	Source of Funds and Source of Wealth	74
6.18	Enhanced Due Diligence	77
6.19	When to apply EDD	80
6.20	Simplified Due Diligence	83
6.21	Ongoing Monitoring	90
6.22	Records	91
6.23	Reliance and outsourcing	92
6.24	Transferring clients between jurisdictions ('passporting')	93
6.25	Using CDD Information in relation to sanctions measures	95
6.26	Communicating with your clients about CDD	96
6.27	Acquisition/Merger of Practice Units	97
<b>7</b>	<b>Technology</b>	
7.1	Overview	98
7.2	Choice of Solution	99
7.3	Electronic Verification	100
7.4	Understanding the system used	101
7.5	Tiered Services	102
7.6	Digital ID Certifications	102
7.7	Training Considerations	103
7.8	Record Keeping and Data Protection considerations	103
7.9	Use of Technology to Conduct Employee Screening and Verification	104
7.10	Company Registry Checkers & Verification of Beneficial Ownership of non-natural persons	104
7.11	Initial and Ongoing Sanctions/PEP/Adverse Media Screening	104
7.12	Specific Screening System Considerations	106
7.13	New Technologies relevant to AML Control in Legal Practices	107

<b>8</b>	<b>Training</b>	<b>108</b>
8.1	General Introduction	108
8.2	Who should be trained?	109
8.3	What should be included in training?	110
8.4	What might be considered as training?	111
8.5	Timing of Training	112
8.6	Training Records	112
<b>9</b>	<b>Internal Controls</b>	<b>113</b>
9.1	General Overview	113
9.2	Appointing an individual as the officer responsible for the practice's compliance with the Regulations	114
9.3	Establishing an independent audit function	114
9.4	Screening relevant employees prior to, and during their employment	115
<b>10</b>	<b>Record Keeping &amp; Data Protection</b>	<b>117</b>
10.1	General Comments	117
10.2	Record keeping policy	118
10.3	CDD Records	118
10.4	Retention period for CDD records (R40)	119
10.5	Sharing CDD information with other parts of a group	120
10.6	Reliance	120
10.7	Other records that you must keep	121
10.8	Other Considerations	122
10.9	Security	122
10.10	Data protection	122
<b>11</b>	<b>Suspicious Activity Reporting</b>	<b>124</b>
11.1	General Comments	124
11.2	Application	124
11.3	What is a SAR?	125
11.4	Internal processes for identifying and reporting suspicious activity	125
11.5	When to submit a SAR	125
11.6	Other notifications	125
11.7	If you decide not to submit a SAR	125
11.8	How to submit a SAR	126
11.9	Information to include	126
11.10	Seeking consent (Defence Against Money Laundering)	127
11.11	Tipping off	129
11.12	Extensions of the moratorium period	129
11.13	Contacting the NCA/UKFIU	131
11.14	Confidentiality of SARs	131

CONTENTS

11.15	Sharing of information within the regulated sector and joint disclosure reports	132
<b>12</b>	<b>Other Duties</b>	<b>133</b>
12.1	General Comments	133
12.2	Money Laundering Regulations Part 5 Requirements – Overview	133
12.3	Obligations on UK body corporates	133
12.4	Obligations of trustees of trusts with a UK Tax Consequence	134
12.5	Obligations of trustees of trusts without a UK Tax Consequence	139
12.6	Reporting of Discrepancies on Registers	140
<b>13</b>	<b>Legal Professional Privilege</b>	<b>143</b>
13.1	Introduction & Application	143
13.2	What is Legal Professional Privilege?	145
13.3	Definition of LPP	147
13.4	Crime/fraud or iniquity exception	150
13.5	Definition of Privileged circumstances – s330 POCA	152
13.6	Differences between privileged circumstances and LPP	153
13.7	The Tension between LPP and Disclosure Obligations under POCA	154
13.8	When do I disclose? – Documenting the decision-making process	156
<b>14</b>	<b>Civil Liability</b>	<b>162</b>
14.1	Introduction	162
14.2	Constructive Trusteeship	162
14.3	Knowing Receipt	162
14.4	Knowing Assistance	163
14.5	Civil Liability and Disclosures to the National Crime Agency (NCA)	164
14.6	Civil liability & SARs	165
<b>15</b>	<b>Supervision</b>	<b>166</b>
15.1	General Comments	166
15.2	Legal Sector Supervisors	166
15.3	Other supervisors	167
15.4	Supervision under the Regulations	167
15.5	Additional Requirements for Supervisors	168
15.6	Enforcement powers under the Regulations	169
15.7	Disciplinary action against legal professionals	169
15.8	Regulations – relevant offences and penalties	169
15.9	Joint liability	172
15.10	Prosecution authorities	172

CONTENTS

<b>16</b>	<b>Money Laundering Offences</b>	<b>173</b>
16.1	General Overview	173
16.2	Application	173
16.3	Principal money laundering offences	173
16.4	Defences to principal money laundering offences	176
16.5	Failure to disclose offences – money laundering	180
16.6	Defences to failure to disclose offences	181
16.7	POCA Offences – other features	182
16.8	Tipping off Offences	185
16.9	Prejudicing an investigation	186
16.10	Defences	186
16.11	Section 342(4) – professional legal adviser exemption	187
16.12	Making enquiries of a client	187
<b>17</b>	<b>Terrorist Property Offences</b>	<b>188</b>
17.1	General Comments	188
17.2	Application	188
17.3	Section 14 – Definition of Terrorist Property	188
17.4	Principal terrorist property offences	189
17.5	Defences to principal terrorist property offences	189
17.6	Failure to disclose offences	190
17.7	Defences to failure to disclose	190
17.8	Section 21D tipping off offences: regulated sector	191
17.9	Defences to tipping off	191
17.10	Making enquiries of a client	192
17.11	The offences	192
17.12	Other terrorist property offences (No Deal Brexit; post-implementation period)	193
17.13	The offences	193
<b>18</b>	<b>Red Flags and Warning Signs</b>	<b>195</b>
18.1	General Overview	195
18.2	Examples of Red Flags	195
18.3	The Nature of the Transaction	200
18.4	Trusts and Administration of Estates	202
18.5	Property work	202
18.6	Company and Commercial Work	203
18.7	Trust and Company Service Providers (TCSPs)	204
18.8	Litigation (generally out of scope but still may be relevant for POCA or TACT)	206
18.9	Choice of Lawyer	206
18.10	Proliferation Financing	206
<b>19</b>	<b>Glossary</b>	<b>208</b>

Annex I

Annexes II and III

Acknowledgements

Schedule of amendments

210

211

215

216

## [1] The Status of this Guidance and Terminology Used

---

### 1.1 Status

This guidance replaces previous guidance and good practice information on complying with AML/CTF obligations.

This guidance is issued by the Legal Sector Affinity Group, which comprises the AML Supervisors for the legal sector.

The authors will aim to keep this guidance up to date with new legislation as it comes into force, but this guidance cannot be regarded as a definitive statement of the law or of the effect of the law, and does not comprise, and should not be relied on as giving, legal advice. It has been prepared in good faith, but neither the Legal Sector Supervisors nor any of the individuals responsible for or involved in its preparation accept any legal responsibility or liability for anything done in reliance on it.

Practice Units are not required to follow this guidance, however legal sector supervisors will consider whether a legal professional has complied with this guidance when undertaking its role as regulator of professional conduct, and as a supervisory authority for the purposes of the Regulations. You may be asked by your regulatory body to justify a decision to deviate from this guidance.

Some independent legal professionals are authorised and regulated by the FCA because they are involved in mainstream regulated activities, e.g., advising clients directly on investments such as stocks and shares. Those professionals should also consider the Joint Money Laundering Steering Group's guidance [<https://jmlsg.org.uk>].

In accordance with sections 330(8) and 331(7) of the Proceeds of Crime Act 2002, section 21A(6) of the Terrorism Act 2000, and Regulation 86(2)(b) of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, the court is required to consider compliance with this guidance in assessing whether a person committed an offence or took all reasonable steps and exercised all due diligence to avoid committing the offence.

### 1.2 Terminology

This guidance uses 'must', 'should' and 'may' throughout to contextualise how to understand the various directions.

The terms have the below meanings:

**Must** – a requirement in legislation or a requirement of a regulation or other mandatory provision. You must comply, unless there are specific exemptions or defences provided for in relevant legislation or regulations.

[1]

Should – good practice for most situations. These may not be the only means of complying with the requirements and there may be situations where the suggested route is not the best option.

If you do not follow the suggested route, you should be able to justify to supervisors why your alternative approach is appropriate, either for your practice, or in the particular instance.

May – an option for meeting your obligations or running your practice. Other options may be available and which option you choose is determined by the nature of the individual practice, client or matter. You may be required to justify why this was an appropriate option to your supervisor.

## [2] Background

This guidance has been written both as a result of the changes made to The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 by The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 that came into force on 10 January 2020 and an extensive review of the previous guidance by the Legal Sector Affinity Group.

These iterative pieces of legislation will be referred to collectively as ‘the Regulations’ throughout this guidance.

The guidance has two over-arching goals:

- First, it intends to provide practical information for legal practices in scope of the Regulations to aid their compliance and to effectively protect against Money Laundering and Terrorist Financing risks; and
- Second, it aims to communicate supervisors’ expectations for those they supervise.

It is not the intention of this document to cover every eventuality. In reviewing it, we have aimed to strike a balance between specificity where helpful and providing the tools that legal practices need in order to deal with any given scenario. The risk-based approach (RBA), which is a long-established principle within Anti-Money Laundering (AML), acknowledges that every situation is different and that the legal practitioners and practices themselves are best placed to understand the risks and deal with them proportionately.

The guidance is separated into two parts:

- Part 1 includes the guidance, generally applicable for legal practices; and
- Part 2 includes guidance for particular sectors (including barristers).

The guidance for barristers in Part 2 has been written recognising the specific nature of the Bars and the risks to which they are exposed. In particular, it recognises that most barristers are self-employed, do not engage directly with the lay client and are limited by their regulation in the scope of practice, which means that they do not hold client money or manage their clients’ affairs. Barristers should read Part 2 in the first instance, drawing on Part 1 for further detail where relevant.

Likewise, the Part 2 guidance makes clear that most work undertaken by notaries (or in Scotland and Northern Ireland, solicitors acting solely in a notarial capacity) in their core role as public certifying officers will fall outside the scope of the Regulations.

## [3] High-Level Compliance Principles

### 3.1 Introduction and context

The Regulations set out requirements which must be adhered to. These, in addition to the compliance principles below, should be viewed as the 'building blocks' for creating robust AML policies, controls and procedures.

The guidance in Part 1 and Part 2 provides additional information and support to help in adhering to these principles.

All legal practices must consider whether their business brings them into scope of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended) ('the Regulations'), through any of the qualifying activities but particularly those stated in R12.

If a legal practice deems itself to be in scope, it is a 'relevant person' for the purposes of the Regulations. We will generally refer to a relevant person as a 'practice' throughout the guidance.

All Relevant Persons must demonstrate to their supervisor that they have adopted a risk-based approach to the management of Money Laundering (ML) and Terrorist Financing (TF) risk within their businesses.

This guidance is intended to address issues faced by relevant persons that are drawn into scope of the Regulations.

### 3.2 Compliance Principles

The following compliance principles are the key areas to address when trying to ensure a practice is compliant with the Regulations.

#### AML Governance

1. All current beneficial owners, officers and managers must be approved by their supervisory authority in accordance with R26.
2. Practices must appoint a MLRO (Money Laundering Reporting Officer) who is responsible for receiving disclosures from staff of suspected money laundering and determining whether they warrant the submission of a suspicious activity report (SAR) to the National Crime Agency (NCA). This individual is responsible for the submission of SARs to the NCA where appropriate. The practice must notify its supervisory authority of this appointment within 14 days of the date of the appointment.
3. Where appropriate to the size and nature of the practice a member of the board (or equivalent) or of senior management must be appointed to be responsible for compliance of the practice with the Regulations. This position is referred to as the Money Laundering Compliance Officer (MLCO). The practice must notify

its supervisory authority of this appointment within 14 days of the date of the appointment.

4. The Board Level Person may delegate the operational day to day AML compliance work of the practice to the MLRO though cannot delegate responsibility/accountability. This delegation must be documented.
5. The AML duties/responsibilities of all partners and employees of the practice should be adequately documented.
6. The AML policies, controls and procedures (PCPs) of the practice must be approved by the practice's senior management (and/or board). This approval must be documented.
7. The Board (or equivalent) must monitor and manage compliance with AML PCPs. Board discussions and decisions regarding AML compliance must be documented.
8. All practices must allocate adequate and competent resource to the management of AML/TF risks.
9. Procedures (including robust, easily accessible record keeping) must be in place to ensure comprehensive and timely reporting and submissions to relevant supervisory authorities.

#### Practice-Wide Risk Assessment

10. Practices must have a written, up-to-date practice-level risk assessment in place, in line with R18 requirements.
11. Practices must use this to directly inform their AML PCPs.

#### Client/Matter Level Risk Assessment

Practices must have:

12. Client and matter level ML/TF risk assessment procedures that include a requirement to undertake a written risk assessment on each new client and matter/retainer particularly where the matter is non-repetitive.
13. A documented procedure for the application of client/matter level risk assessment outcomes to the due diligence undertaken on any particular client/matter.

#### AML Policies, Controls and Procedures

The practice must have clearly documented PCPs based on their practice-wide risk assessment which include:

14. The AML governance arrangements of the practice.

#### Client Due Diligence

The practice must have clearly documented PCPs based on their practice-wide risk assessment which include:

- [3]
15. Client Due Diligence procedures (including procedures to identify the ownership and control structures of non-natural persons).
  16. Identification and verification (ID&V) procedures relating to natural persons (this includes ID&V procedures in relation to the ultimate beneficial owners of non-natural clients, and those purporting to act on behalf of a client).
  17. Procedures to facilitate a clear understanding of the client's source of wealth and funds in relation to a transaction, and the level of evidence required, in line with the risk profile of the client/matter.
  18. Procedures to facilitate reporting of discrepancies between Beneficial Ownership information obtained through due diligence checks and what is held on the Companies House register.
  19. Enhanced Due Diligence procedures – including the provision of adequate controls to manage higher risk clients/transactions, and measures to establish Source of Funds/Source of Wealth where appropriate.
  20. The practice's position on the use and application of Simplified Due Diligence.
  21. The timing of any due diligence procedures.
  22. The practice's position on the use of R39 Reliance and any related procedures.
  23. The ongoing monitoring of clients and their matters.
  24. The identification of instances where it is required or appropriate to re-apply or renew CDD or EDD on a client.
  25. Dealing with the return of un-solicited or apparently accidentally deposited funds.
  26. Identification and scrutiny of any complex or unusually large transactions, or an unusual pattern of transactions, or those which serve no apparent economic or legal purpose.
  27. Any additional measures to prevent products/transactions that support anonymity being used for ML/TF.
  28. Identification of Politically Exposed Persons (PEPs), their relatives or close associates and the control of any associated risks.

#### *Suspicious Activity Reporting*

29. The practice must have procedures setting out how, and in what circumstances an internal disclosure should be submitted to the Nominated Officer (MLRO).

#### *Technology*

The practice must have clearly documented PCPs based on their practice-wide risk assessment which include:

30. Measures taken when new technology is adopted to protect against ML or TF risks.

31. Where practices use electronic identification and verification (EID&V) tools they should document the role of the tool, the data sources it uses, and in what circumstances (clients/matters) it is appropriate to use the solution.

#### *Training*

The practice must have clearly documented PCPs based on their practice-wide risk assessment which include:

32. Measures deployed to ensure AML relevant training of partners, staff and agents, including the maintenance of records relating to such training. This training must include awareness of MLR, Proceeds of Crime Act Part 7 and Terrorism Act Part 3 reporting requirements, legal professional privilege and data protection requirements. Training should also cover recognition of red flags/risk indicators as relevant to their duties and responsibilities, along with other relevant laws.
33. Procedures for the communication of PCPs to partners and staff.

#### *Internal Controls*

Where appropriate to the size and nature of the practice:

34. The practice must conduct an independent audit of the adequacy and effectiveness of its AML policies, controls and procedures.
35. The practice must undertake screening of relevant employees – both at pre-employment stage and on an ongoing basis.

#### *Record Keeping*

36. The practice must have procedures relating to records keeping and related data protection matters.

## [4] AML Governance and Policies, Controls and Procedures

### 4.1 Overview

This section outlines the Anti-Money Laundering (AML) roles, responsibilities, and appointment of senior individuals in a practice including the Money Laundering Reporting Officer (MLRO), Money Laundering Compliance Officer (MLCO), and beneficial owners, officers, and managers (BOOMs), as well as some of the structures that practices must or should put in place (e.g., training and independent audit).

Note that sole practitioners will fulfil the responsibilities of all role holders mentioned in this section, but rather than having any duty to report matters internally within their practice, they must instead record such information in writing (e.g., records of SARs).

#### Relevant Compliance Principles

1. All current beneficial owners, officers and managers must be approved by their supervisory authority in accordance with R26.
2. Relevant Persons must appoint a MLRO (Money Laundering Reporting Officer) who is responsible for receiving disclosures from staff of suspected money laundering and determining whether they warrant the submission of a suspicious activity report (SAR) to the National Crime Agency (NCA). This individual is responsible for the submission of SARs to the NCA where appropriate. The practice must notify its supervisory authority of this appointment within 14 days of the date of the appointment.
3. Where appropriate to the size and nature of the practice a member of the board (or equivalent) or of senior management must be appointed to be responsible for compliance of the practice with the Regulations. This position is referred to as the 'Board Level Person' or Money Laundering Compliance Officer (MLCO). The practice must notify its supervisory authority of this appointment within 14 days of the date of the appointment.
4. The Board Level Person may delegate the operational day to day AML compliance work of the practice to the MLRO though cannot delegate responsibility/accountability. This delegation must be documented.
5. The AML duties/responsibilities of all partners and employees of the practice should be adequately documented.
6. The AML policies, controls and procedures (PCPs) of the practice must be approved by the Relevant Person's senior management (and/or board). This approval must be documented.
7. The Board (or equivalent) must monitor and manage compliance with AML Policies, Controls & Procedures (PCPs). Board discussions and decisions regarding AML compliance must be documented.

8. All Relevant Persons must allocate adequate and competent resource to the management of AML/TF risks.
9. Procedures (including robust, easily accessible record keeping) must be in place to ensure comprehensive and timely reporting and submissions to relevant supervisory authorities.

### 4.2 Approvals, Roles and Positions

The Regulations specify the roles and responsibilities of certain individuals in a practice. These are the:

- Beneficial Owners.
- Officers.
- Managers.
- MLRO; and
- MLCO or 'Board Level Person'.

#### 4.2.1 Beneficial Owners, Officers and Managers

Under R26, you must gain approval from your supervisor for all BOOMs at your practice before the practice can undertake any of the activities that fall under the Regulations.

Those acting as BOOMs without approval, could be subject to summary conviction and a prison term of up to three months or a conviction on indictment and a prison term of up to two years.

#### Definition of a BOOM

##### Beneficial Owner (R5)

- (1) In these Regulations, 'beneficial owner', in relation to a body corporate which is not a company whose securities are listed on a regulated market, means:
  - (a) any individual who exercises ultimate control over the management of the body corporate;
  - (b) (any individual who ultimately owns or controls (in each case whether directly or indirectly), including through bearer share holdings or by other means, more than 25% of the shares or voting rights in the body corporate; or
  - (c) any individual who controls the body corporate.
- (2) For the purposes of paragraph (1)(c), an individual controls a body corporate if:
  - (a) the body corporate is a company or a limited liability partnership and that individual satisfies one or more of the conditions set out in Part 1 of Schedule 1A to the Companies Act 2006 (people with significant control over a company); or
  - (b) the body corporate would be a subsidiary undertaking of the individual (if the individual were an undertaking) under section 1162 (parent and

- [4] subsidiary undertakings) of the Companies Act 2006 read with Schedule 7 to that Act.
- (3) In these Regulations, 'beneficial owner', in relation to a partnership (other than a limited liability partnership), means any individual who:
- (a) ultimately is entitled to or controls (in each case whether directly or indirectly) more than 25% share of the capital or profits of the partnership or more than 25% of the voting rights in the partnership;
  - (b) satisfies one or more the conditions set out in Part 1 of Schedule 1 to the Scottish Partnerships (Register of People with Significant Control) Regulations 2017 (references to people with significant control over an eligible Scottish partnership); or
  - (c) otherwise exercises ultimate control over the management of the partnership.
- (4) In this regulation 'limited liability partnership' has the meaning given by the Limited Liability Partnerships Act 2000.

**'Officer' (R3)**

- (a) in relation to a body corporate (including LLPs), means:
- (i) a director, secretary, chief executive, member of the committee of management, or a person purporting to act in such a capacity, or
  - (ii) an individual who is a controller of the body, or a person purporting to act as a controller.
- (b) in relation to an unincorporated association, means any officer of the association or any member of its governing body, or a person purporting to act in such a capacity.
- (c) in relation to a partnership, means a partner, and any manager, secretary or similar officer of the partnership, or a person purporting to act in such a capacity.

**'Manager' (R3)**

in relation to a practice, means a person who has control, authority or responsibility for managing the business of that practice, and includes a nominated officer (MLRO)

**4.2.2 Who might be a BOOM?**

Without contravening or limiting the definitions in the Regulations, the individuals you should particularly consider seeking approval for as BOOMs include:

- Beneficial Owners: partners who exercise significant control, owners (of a share of more than 25%), those with significant control of the entity (through ownership, voting rights or otherwise).
- Officers: partners who exercise significant control, Executives (e.g., CEO, CFO, CTO), Managing Directors, Board members or equivalent; and
- Managers: will often include roles sitting below the Officers, including senior leadership team, heads of departments or practice areas.

**4.2.3 Approval of BOOMs**

The test that must be applied by supervisors is whether an applicant has been convicted of any of the offences in Schedule 3 of the Regulations. If the applicant has no such conviction, the supervisor must approve the application, and can apply their own processes to assess the application.

The updated regulations require applications to include 'sufficient' information for the supervisor to determine whether the test is met. You must follow the directions of your supervisor and provide them with the information they require to establish that the applicant does not have any relevant convictions (this will often take the form of a criminal record check).

Approval must be granted prior to any activity that would bring the practice or the individual into scope of the Regulations. This is equally relevant to established practices as new ones. Established practices must seek approval for new BOOMs before they take up their role.

Individuals may not be able to port their approval from one practice to another and should clarify the processes and specifics of this with their own supervisor.

If an approved BOOM is convicted of a relevant offence under Schedule 3 their approval will cease to be valid and:

- the individual must cease all activities in scope of the Regulations and notify their supervisor within 30 days starting from the date of the conviction; and
- the practice must report the conviction within 30 days, starting from the date they became aware of it.

When someone ceases to act as a BOOM, you should notify your supervisor within 14 days.

**4.3 Money Laundering Reporting Officer (otherwise known as Nominated Officer)**

R21(3) requires all practices to have a nominated officer (MLRO) to receive disclosures for possible submission to the National Crime Agency (NCA) under Part 7 of POCA and TACT.

R21(6) provides that there is no requirement to appoint a MLRO if you are an individual who provides regulated services, but do not employ or act in association with anyone else. In this case the duties of the MLRO will fall with you.

**4.3.1 Who should be MLRO?**

Your MLRO should be:

- of sufficient seniority to make decisions on reporting which can impact your practice's business relations with your clients and your exposure to criminal, civil, regulatory and disciplinary sanctions.
- in a position of sufficient responsibility to have access to all client files and business information. This will allow them to make decisions on the basis of all information held by the practice; and

[4]

- supported and empowered in the carrying out of their duties by Senior Management.

The MLRO may be a member of the Board of Directors (or equivalent Senior Management body) or able to attend their meetings and should be able to directly report to the board on how the practice is fulfilling its obligations and compliance work in this area.

You should consider whether the person you are appointing has access to sufficient resources in order to be able to effectively fulfil the role, especially if the MLRO is also undertaking other duties.

Practices authorised by the Financial Conduct Authority (FCA) must obtain the FCA's approval for the appointment of the MLRO as this is a controlled function under section 59 of the Financial Services and Markets Act 2000.

#### 4.3.2 Role of the MLRO

Your MLRO is responsible for ensuring that information leading to knowledge or suspicion, or reasonable grounds for knowledge or suspicion of money laundering is properly disclosed to the NCA. The decision to report, or not to report, must not be subject to the consent of anyone else. Your MLRO may liaise with the NCA or law enforcement on whether to proceed with a given transaction or what information may be disclosed to clients or third parties.

The MLRO has a personal responsibility to ensure they fulfil their duties and may be subject to conviction under s331 of the Proceeds of Crime Act, 2002, for a failure to disclose information to the NCA.

A range of factors, including the type of practice, its size and structure, may lead to the MLRO delegating certain duties regarding the practice's AML/CTF obligations.

All practices must consider arrangements for temporary cover when the MLRO is absent. You may appoint one or more deputy MLROs where appropriate in order to ensure the work is sufficiently resourced and continuously covered. The MLRO and any deputies must have unrestricted and direct access to the NCA SARs online system and the internal records of SARs at the practice.

An MLRO may also be empowered with further duties under delegation from senior management or the Board of the practice, however the delegating party will retain accountability. For example, an MLRO may be appointed responsible by the Board or MLCO for the creation, management and review of the practice's Policies, Controls and Procedures (PCPs) under R19.

An MLRO should consider whether and in what form the content of their disclosures to the NCA should be reported to senior management or their Board.

The identity of the MLRO and deputies should be known to all relevant staff and should be noted in the PCPs.

[4]

#### 4.3.3 MLRO Reporting (to the Senior Management Body)

The MLRO should submit an annual report (more frequent reporting may be determined appropriate by the Board or equivalent Senior Management Body) setting out:

- changes to the AML/CTF risks of the practice.
- advised improvements to be made in the coming year.
- progress on any past improvements.
- the results of any internal auditing.
- resourcing concerns/considerations.
- any interactions with their supervisor.
- AML staff training undertaken.
- key information, for example regulatory changes or notable publications/guidance from AML authorities; and
- other information, for example, trends, deficiencies, lessons relating to SARs made by the practice.

The MLRO may also be the appropriate person to record the AML compliance responsibilities of individuals at the practice.

#### 4.3.4 Responding to enquiries from law enforcement agencies

In accordance with R21(8), a practice must establish and maintain systems which enable it to respond fully and rapidly to enquiries from law enforcement agencies as to:

- whether it maintains, or has maintained during the previous five years, a business relationship with any person; and
- the nature of that relationship.

In responding to enquiries, practices must consider the privileged nature of any information they hold before sharing it.

Record keeping that meets the requirements of the Regulations will help a practice to comply with these requirements. A practice may appoint the MLRO as the lead person to act as liaison with law enforcement.

#### 4.4 Money Laundering Compliance Officer (MLCO)

R21(1)(a) requires that where appropriate to the size and nature of the business, a practice must appoint a member of the Board (or equivalent management body) or member of the senior management team (the 'Board-Level Person') as being responsible for the practice's compliance with the Regulations. This role is commonly known as the Money Laundering Compliance Officer, or MLCO.

The general focus of this role is being a lead within the senior management of the practice, supporting the work of the MLRO and ensuring that the AML efforts of the practice have appropriate oversight and engagement at the highest level.

The MLCO should have:

- an understanding of the business, its service lines and clients;

[4]

- sufficient seniority to direct the activities of all members of staff (including senior individuals) and to influence resourcing levels and AML controls;
- the authority to ensure the business' compliance with the regime; and
- the time, capacity, and resources to fulfil the role.

#### 4.5 Practices with both a MLRO and a MLCO

You may appoint the same individual to fulfil both the MLRO and MLCO roles.

However, the larger, the more complex and the higher the risk exposure of the practice, the greater the rationale is for appointing separate people to the roles, in order to better resource the compliance efforts. This should be balanced against the possible advantages and synergies of having one person fulfil both.

The MLCO may delegate some of the operational aspects (though never responsibility/accountability) of the day-to-day AML compliance of the practice to the MLRO or other individuals. These delegations must be documented, and roles/responsibilities clearly defined.

When appointing people to the MLRO/MLCO roles, Senior Management should have regard to the risk of any possible conflicts of interest they may face (particularly with any fee-earning duties the MLRO/MLCO may retain) and address this in the policies of the practice. This may be adequately addressed by the general conflicts of interest policy in the practice.

Senior management should also have regard to the amount of resource they have dedicated for the purpose of allowing their MLRO and MLCO to adequately fulfil their duties (e.g., time and access to support staff).

In considering the issue of resource, it is worth highlighting that although it may not be common practice, there is nothing to prevent MLRO/MLCO roles rotating among a group of individuals, as long as they all meet the requirements. This can be particularly advantageous when rotating the lead role (e.g., MLRO) among a group of deputies, as it spreads resource demand while also ensuring deputies are experienced at taking over the lead when required.

#### 4.6 Senior Management Responsibilities

Senior management refers to any officer or employee of the practice with sufficient knowledge of the practice's money laundering and terrorist financing risk exposure, and of sufficient authority, to take decisions affecting its risk exposure.

Senior management should ensure the MLRO/MLCO has:

- active support.
- adequate and competent resources (staff, time, budget, technology, training see Section 8 for further information).
- independence of action.
- access to the relevant information.
- the ability to fulfil their duties.

[4]

Senior Management must mitigate and effectively manage their ML/TF risks via the implementation and approval of PCPs (R19(2)(b)). Reporting by MLROs may assist Senior Management in their efforts to assess and address the practice's efforts to this end.

Any decisions made by Senior Management on issues of AML compliance should be documented and tracked over time. The Practice Wide Risk Assessment should be signed off by Senior Management along with all revisions of this document.

It is important that the Senior Management of a practice is informed and engaged with their responsibilities under the Regulations. They should consider any information their MLRO/MLCO shares with them about ML/TF risk.

Senior Management are also responsible under the Regulations for providing approval for the practice to be able to establish or continue a business relationship with a PEP or a close family member or known associate of a PEP or to enter into business relationships with clients established in high risk third countries.

#### 4.7 Informing your Supervisor of MLRO and MLCO Appointments and registering for the Economic Crime Levy

You must inform your supervisor of the identity of your MLRO (this must be a specific individual) and where relevant your MLCO within 14 days of appointment (R21(4)(b)).

You must also inform your supervisor of any subsequent appointments to either of those positions within 14 days. If you are operating a rotating model of MLROs among more than one person, the above requirement to inform your supervisor must be met whenever a new person takes over the lead position.

Note that an MLRO will automatically be a manager and must therefore be approved as a BOOM (R26) prior to their appointment. If you are using a rotating model, you should consider all the individuals among whom the role is rotating as BOOMs and get them approved as such.

You must also register to pay the Economic Crime (Anti-Money Laundering) Levy (ECL) if your annual turnover exceeds £10.2 million pounds.

The ECL is payable to HMRC and falls due each year your turnover exceeds the threshold amount. You must register and pay online.

If you are dual-regulated by the FCA and a professional body supervisor, you must register using your FCA credentials.

Further guidance, and a link to register, can be found here [[www.gov.uk/government/publications/prepare-for-the-economic-crime-levy/get-ready-for-the-economic-crime-levy](http://www.gov.uk/government/publications/prepare-for-the-economic-crime-levy/get-ready-for-the-economic-crime-levy)].

#### 4.8 Policies, Controls and Procedures (PCPs)

##### 4.8.1 What must be included in PCPs?

R19 requires that practices establish and maintain written policies, controls and procedures (PCPs) for identifying, managing and mitigating the risks identified in the