Guidance on anti-money laundering legislation

October 2008

The Association of Accounting Technicians
Registered charity No. 1050724
Guidance on anti-money laundering legislation

Disclaimer........................................................................................................................................... 3
About this guidance............................................................................................................................. 3
Abbreviations used in this guidance.................................................................................................... 4
Introduction........................................................................................................................................ 4
What is money laundering?.................................................................................................................. 4
The statutory definition of money laundering.................................................................................... 5
Criminal property................................................................................................................................. 5
Criminal conduct................................................................................................................................. 6
Where can I find the rules about money laundering?......................................................................... 7
What is the difference between the different pieces of legislation?..................................................... 7
Do the rules apply to me?................................................................................................................... 8
How do the rules apply to me?........................................................................................................... 9

The Money Laundering Regulations 2007......................................................................................... 11
Policies and procedures...................................................................................................................... 11
Risk sensitive approach...................................................................................................................... 12
What are the risks?............................................................................................................................. 13
The source of risk.............................................................................................................................. 13
The need for a risk assessment.......................................................................................................... 15
How to conduct a risk assessment.................................................................................................... 15
Risk assessment of individual clients............................................................................................... 18

Customer Due Diligence (CDD)........................................................................................................ 19
The three elements of CDD................................................................................................................ 19
Different verification requirements in relation to clients and beneficial owners............................... 22
CDD illustrations............................................................................................................................... 23
Simplified CDD................................................................................................................................ 25
Enhanced CDD................................................................................................................................. 26
Reliance upon CDD carried out by others........................................................................................ 30
When you must carry out CDD......................................................................................................... 31
Timing of verification......................................................................................................................... 33
If you are unable to satisfactorily apply CCD measures................................................................... 34
Ongoing monitoring........................................................................................................................... 34
Enhanced ongoing monitoring.......................................................................................................... 35
Record keeping.................................................................................................................................. 35
Internal reporting procedures........................................................................................................... 37
The Money Laundering Reporting Officer (MLRO)........................................................................... 37
MLRO offences................................................................................................................................. 38
Internal control................................................................................................................................. 39
Risk assessment and management..................................................................................................... 40
Internal communication of policies and procedures......................................................................... 40
Monitoring and management of compliance.................................................................................... 40
Training............................................................................................................................................ 41
Client account.................................................................................................................................... 41
Suspect territory................................................................................................................................. 42
Dealing with SOCA........................................................................................................................... 42
Supervision........................................................................................................................................ 43

Proceeds of Crime Act 2002............................................................................................................. 46
Part 7 POCA..................................................................................................................................... 46
Knowledge and suspicion................................................................................................................... 47
How to treat your client’s explanation............................................................................................... 48
Reasonable grounds to know or suspect........................................................................................... 49
POCA money laundering offences..................................................................................................... 49
Defences to allegations of money laundering (section 327-329 POCA).............................................. 50
This edition

This edition, issued in October 2008, replaces all previous editions. It is important that you check that any guidance you consult is the latest version available and up to date.

Disclaimer

This guidance is no substitute for familiarity with the anti-money laundering legislation (AMLL). Although all reasonable efforts have been made to ensure that this guidance accurately reflects our members’ legal obligations under the AMLL at the date of issue, it is emphasised that each situation to which the law on money laundering applies must be considered in its individual circumstances. Therefore, this guidance does not constitute legal advice but is intended to bring issues to your attention and to set the rules in context. The AAT accepts no liability for loss caused to any person as a result of following this guidance.

About this guidance

This guidance is specifically intended to help AAT members comply with their obligations under the AMLL. It applies equally to students, affiliate, full and fellow member and outlines the main rules that we anticipate will apply to them. For the sake of clarity, we have been selective in the rules mentioned, and in some cases we have paraphrased or abridged those rules. We have also avoided detailed reference to professional activities, which, although covered by the law on money laundering, are less likely to be pursued by our members.

The format of this guidance is, where appropriate to; present a summary of an obligation, set out the rule, followed by a commentary. This guidance has been drafted in discrete sections, on the assumption that members will consult only those sections that answer their immediate concerns. Therefore, it is necessarily repetitive. However, you are advised to read this guidance in its entirety. To minimise awkward sentence construction, the convention of using masculine expressions to include the feminine has been adopted.

In deciding whether a person has committed a “failure to disclose” offence under the Proceeds of Crime Act 2002 or any breach of the Money Laundering Regulation 2007, the court must consider whether he followed relevant guidance by a ‘supervisory authority’ or any other ‘appropriate body’ if such guidance has been approved and published in a manner approved by the Treasury. The AAT is a supervisory body but has not sought Treasury approval for this guidance. However, the courts are likely to take it into account. The AAT may seek Treasury approval in the future.

The CCAB have issued comprehensive Treasury-approved guidance, which is available on the CCAB website, www.ccab.org.uk While this guidance has been drafted to reflect AAT members’ niche position, it has been drafted, as far as possible, to be consistent with the CCAB guidance.
Introduction
This guidance has been updated to take account of amendments to the Proceeds of Crime Act 2002 (POCA) and Terrorism Act 2000 (TA) and the changes introduced by the Money Laundering Regulations 2007 (the Regulations), which came into force on 15 December 2007.

The regulations should seem familiar because they preserve many of the principles contained in the Money Laundering Regulations 2003, which they replace. The changes that have been introduces are intended to encourage you to move away from a tick-box approach and to take proportionate measures to manage the risks of your practice being exploited to facilitate money laundering and terrorist financing.

The main changes are that: you must apply the Regulations on a proportionate risk-sensitive basis; the old identification procedures are now part of a wider duty to conduct customer due diligence (CDD); you must now conduct on-going monitoring of existing clients; and you will be supervised and monitored in your compliance with the Regulations by your Supervisory Authority. This all may sound daunting but the reality for most is that not much will change at practice level.

POCA and TA have been amended slightly to restrict the duty to report money laundering to when the money launderer or the whereabouts of the proceeds of crime can be identified. Another change to the regulatory landscape is that the National Criminal Intelligence Service (NCIS) has been replaced by the Serious Organised Crime Agency (SOCA). However, to all practical purposes, this is merely a change of name.

What is money laundering?
“Money laundering is the process by which criminally obtained money or other assets (criminal property) are exchanged for ‘clean’ money or other assets with no obvious link to their criminal origins. It also covers money, however come by, which is used to fund terrorism.” HMRC guidance MLR8.

This is not the statutory definition of money laundering but is a useful working definition. The HMRC Guidance goes on to explain that “money laundering takes many forms including:

- handling the proceeds of crimes such as theft, fraud and tax evasion
- handling stolen goods
- being knowingly involved in any way with criminal or terrorist property
- entering into arrangements to facilitate laundering criminal or terrorist property
• investing the proceeds of crime into other financial products
• investing the proceeds of crime into the acquisition of property/assets.

The statutory definition of ‘money laundering’ is consistent with the HMRC definition but is more complex. It isolates the various constituent elements of the offence, including the degree of knowledge of the different parties concerned, and expands the circumstances in which money laundering is deemed to have taken place.

An AAT member will be guilty of a primary money laundering offence if he provides accountancy services while turning a ‘blind eye’ to a client’s suspect dealings (this is a contextual interpretation of the fourth bullet point above).

**The statutory definition of money laundering**

The statutory definition of money laundering is an act which constitutes an offence under sections 327, 328 or 329 of POCA. This includes the inchoate offences of attempting, helping or encouraging another to commit such an offence.

Note: the inchoate offences relate to the dealing in the proceeds of crime (the proceeds must already exist and the crime producing them must already have been committed. To attempt or encourage acquisitive crime is an offence in its own right but is not money laundering.

The sections 327, 328 and 329 offences (referred to in more detail later) are respectively:

327 - Concealing, disguising, converting, transferring or removing criminal property.
328 - Taking part in an arrangement to facilitate the acquisition, use or control of criminal property.
329 - Acquiring, using or possessing criminal property.

The statutory definition is all encompassing, criminalising those who possess, deal or attempt to deal in criminal property - except in particular circumstances specified in POCA (referred to later). As the statutory definitions is dependent upon the existence of criminal property, the starting point to understanding the money laundering legislation is to understand the concept of criminal property.

**Criminal property**

Criminal property is property which was obtained as a result of criminal conduct and the person knows or suspects that it was obtained from such conduct. The property can be in any conceivable legal form, whether money, rights, real estate or any benefit. It may have changed from one form to another or been through several hands but it could still be criminal property if the original property was obtained from criminal conduct.

Because the definition of criminal property (an essential element of money laundering) requires actual knowledge or suspicion, it is not possible to money launder inadvertently. Unless committed deliberately, strict liability offences (such as non-payment of VAT), although offences in their own right, do not give rise to criminal property or, therefore, money laundering.

A peculiarity of the definition of criminal property is that the proceeds of criminal conduct can be both criminal and non-criminal property at the same time, depending upon individual perception. Perception, therefore, determines the individual’s criminality and obligations.

**Illustration:** your client, John, has been gifted company shares by his uncle, who purchased them with money retained through the criminal conduct of tax evasion.
Despite the actual circumstances of their purchase, the shares will only be criminal property as far as John is concerned if he knows or suspects that they had been acquired as a result of criminal conduct. He will then commit a money laundering offence if he deals in them. They will not be criminal property and he will not commit an offence by dealing in them if he neither knows nor suspects that they represent a benefit from criminal conduct.

Likewise, the shares will not be criminal property as far as you are concerned if you neither know nor suspect that they represent the benefit from criminal conduct. However, if you know or suspect that the shares were purchased from the proceeds of crime (perhaps you were also the uncle’s accountant), the shares will be criminal property as far as you are concerned, even if John is completely innocent. You will commit a money laundering offence if you provide your services to facilitate John’s dealing in them, unless you had applied for and received consent to do so from your MLRO or SOCA, as appropriate. Your client’s state of mind does not determine your own obligations and criminality.

**Criminal conduct**

Criminal conduct is conduct which would result in conviction for a criminal offence if proved before a UK court. You are expected to assess whether activity is criminal conduct by its nature. There does not have to be a police investigation, a trial or a conviction in relation to conduct for it to be criminal conduct. For example, drug dealing is criminal conduct even if undetected. In assessing whether conduct is criminal conduct, you may have regard to the following:

- the legal presumption that persons are law-abiding. This presumption will not apply if circumstances suggest otherwise
- if it is a moot point whether the conduct is criminal, you should not decide that it is. For example, a client might have legal arguments as to why VAT is not payable. You should not determine the outcome of unsettled law or dispute
- if it is capable of reasonable explanation, you should afford your client the opportunity to provide an explanation, unless you have cause to fear recriminations from your client
- you are not expected to be expert in criminal law but you are expected to have the knowledge of a reasonable accountant working in your particular field.

For the purposes of the legislation, criminal conduct can relate to any crime known to UK law, regardless of how serious or trivial.

This lack of a *de minimus* is controversial but the value of criminal property is not necessarily the most helpful indicator of potential harm to society. An argument often advanced to justify the lack of a *de minimus* is that investigation of low value criminal property can lead to discovery of serious crime. No doubt, this has happened but, as stated, this argument is undiscriminating and lacks refinement. While it is reasonable to suggest that serious criminals may become involved in low-value criminal conduct, and that investigation of a large number of low value criminal transactions, therefore, will lead to some serious criminals, it would be preposterous to suggest that all low-value criminal conduct is indicative of more serious underlying crime.

However, some low value criminal property is inevitably the tip of an organised crime ‘iceberg’. For example, the investigation into the profits from low-value drug dealing could reasonable be expected to lead to a chain of supply, to drug smuggling, violence and exploitation, and sometimes crimes such as people trafficking and terrorism. Likewise, investigation into small profits from burglary could reasonable be expected to reveal dealers in stolen goods and other criminal networks. It is therefore, more apt to
consider the origin of criminal property than its value, and to distinguish between the profits from isolated 'accountancy irregularities' and crimes which are inevitably part of a chain of criminal conduct, when designing a proportionate response to the risk of your practice being exploited to facilitate money laundering.

Conduct carried out abroad counts as a criminal conduct for the purposes of the UK legislation if it would be criminal if committed in the UK, even if not regarded as such in the host country. This rule has been subject to amendments, firstly to provide exceptions, then subsequently to restrict the exceptions to such a degree as to render them virtually meaningless (except in relation to cultural differences such as the dealing in the profits from Spanish bullfighting).

**Note:** There is an important distinction between criminal conduct and money laundering. While the conduct may be criminal, it is only the **possessing or dealing** with property arising from criminal conduct that amounts to money laundering. If, for example, a client submits a false tax return to understate the tax owed, he may be attempting to commit a fraud, but until he gains the benefit of his fraud - that is, he knowingly and deliberately retains the tax after it has become due and owing - he is not engaged in money laundering because there is no criminal property prior to this point.

Although accountants must be aware of the full definition of money laundering in order to recognise potential money laundering by their clients and third parties, an accountant will usually only commit a money laundering offence if he facilitates his client's dealing in criminal property by providing accountancy services when he knows or suspects that the client is dealing in criminal property. If an accountant does inadvertently facilitate money laundering after having applied the legislation reasonably and proportionately, he will not commit a money laundering offence.

**Where can I find the rules about money laundering?**
The legislative rules relating to money laundering are contained in:

- **The Proceeds of Crime Act 2002 (POCA) (as amended):** This sets out the principal money laundering offences and the requirements to report suspicious transactions.

- **The Terrorism Act 2000 (TA) (as amended):** This sets out the principal terrorist financing offences and reporting obligations in similar terms to POCA.

- **The Money Laundering Regulations 2007 (the Regulations):** These require sole traders and firms to establish a risk-sensitive procedural framework intended to detect and prevent activities relating to money laundering and terrorist financing. They revoke and replace the Money Laundering Regulations 2003.

**What is the difference between the different pieces of legislation?**
- **POCA** sets out offences for knowingly or carelessly possessing or dealing in the profits from crime or assisting others to do so, and imposes upon professionals an obligation to report suspected money.
- **TA** sets out offences for knowingly or carelessly engaging or assisting in the raising, possessing or dealing with property intended for terrorist purposes. TA obligations are similar to those imposed by POCA.
- **The Regulations** require practices to establish and maintain specified risk-sensitive policies and procedures to increase the likelihood of suspicious transactions being recognised and reported;
and ensure that an audit trail is available to the authorities in the event of an investigation. Failure to comply with the Regulations is itself a criminal offence.

POCA and TA use different terminology to the Regulations to describe persons to whom they apply. POCA and TA refer to the **regulated sector**, while the Regulations refer to **relevant persons**. The distinction is relevant:

**Regulated sector** is a term used in POCA and TA to describe a number of types of businesses and professional services. Individuals within those businesses or providing such services, such as accountancy, are personally liable for breaching POCA and TA.

**Relevant person** is a term used in the Regulations to describe particular entities (sole traders and firms) within the regulated sector responsible for implementing and complying with the Regulations. The Regulations apply to entities and not employees because the prescribed procedures must be operated at practice level. The sole trader or firm will be liable for any breach of the Regulations, even if brought about by an employee.

**Do the rules apply to me?**
The rules will apply to you to a greater or lesser extent, depending upon whether you are:
- in practice as a sole trader
- in practice within a firm within the regulated sector
- an employee of a firm in the non-regulated sector.

If you are a Member in Practice, employed by an accountancy firm, or employed by a non-accountancy organisation within the regulated sector, you must comply with the rules in the POCA and TA to their fullest extent. Your employer will, no doubt, require you to comply with internal procedures prescribed by the Regulations.

If you are employed by an organisation that is not within the regulated sector you must comply with some of the rules in POCA and TA (in particular, sections 327 - 329 POCA and sections 15 to 18 TA – the primary money laundering and terrorist financing offences). Your employer will be exempt from the Regulations unless it applies them on a voluntary basis.

The regulated sector, as defined by POCA and TA, consists of:
- external accountants, tax advisers, auditors and insolvency practitioners
- trust or company service providers
- credit institutions
- financial institutions
- independent legal professionals
- estate agents
- high value dealers – businesses accepting cash payments of 15,000 Euro or more
- casinos.

The various relevant persons are defined in regulation 3 and 4 of the Regulations. If you wish to access the Regulations you can do so by clicking [here](#) but for your convenience, abridged definitions of external accountant and trust or company service provider are set out below, on the assumption that they are the most pertinent to our members’ practices:
An **external accountant** is a sole trader or firm providing accountancy services to clients by way of business.

For the sake of clarification
- A sole trader is an individual trading on his own identity; a firm is an individual trading through a limited company, or two or more individuals trading through a limited company, partnership, limited liability partnership, or group practice however constituted.
- Individuals who provide accountancy services but not ‘by way of business’ are exempt from the rules that apply to the regulated sector. This narrow exemption exists so as not to inhibit charitable works or informal arrangements between family and friend. It applies only to those who provide their services in return for no more than genuine reasonable expenses.
- ‘Accountancy services’ are not defined but are interpreted widely to include bookkeeping and payroll etc.

A **trust or company service provider** is a sole trader or firm, who by way of business provides to other persons the services of:
- forming companies or other legal persons
- acting as or arranging for another person to act as a director or secretary of a company, as a partner of a partnership, or in a similar position for another legal person
- providing a registered office or address or related services for a company, partnership or other legal person or arrangement
- acting or arranging for another person to act as a trustee of an express trust or similar legal arrangement, or a nominee shareholder for a person other than a company whose securities are listed on a regulated market.

**How do the rules apply to me?**
The extent to which the legislation affects you will depend on whether you are:
- a manager or partner of a firm
- a money laundering reporting officer (MLRO) of a firm
- a sole practitioner
- an employee of a firm within the regulated sector
- an employee of a firm operating outside the regulated sector.

The rules apply in their entirety to all those within the regulated sector but not uniformly:
- If you manage a firm, you must establish and maintain appropriate and risk-sensitive policies, as required by the Regulations, ensuring the nomination of an individual to act as MLRO to accept and administer Internally Reports and suspicious activity reports (SARs) to SOCA.
- If a firm in the regulated sector employs you, you must know and follow your firm’s internal procedures and report suspicious activities to your MLRO in accordance with those procedures, and refrain from tipping-off the client that you or anyone else has done so.
- If you are a sole practitioner, you must abide by the rules as they apply to your situation. You do not have to implement the complete list of policies and procedures referred to in the Regulations, and you must submit SARs directly to SOCA.

Whether you are within or outside the regulated sector, you must not provide services to a client (or otherwise enter any arrangement) which you know or suspect facilitates or conceals money laundering or
the raising or dealing in terrorist financing, unless you have consent to do so from SOCA (or your MLRO, if you have one).

If you are within the regulated sector you have the additional duty to report any person you know or suspect or in relation to whom you have reasonable grounds to know or suspect is engaged in money laundering, whether or not you intend to act for that person.

If you are a MLRO within or outside the regulated sector, you must decide when an Internal Report should be referred to SOCA by way of SAR, and whether it should be accompanied by a request for consent to undertake a client’s instruction. If consent is necessary, you must ensure that your firm refrains from acting in relation to the suspicious transaction until you receive consent from SOCA to proceed, whether actual or deemed consent.
The Money Laundering Regulations 2007

The Regulations came into force on 15 December 2007, replacing the Money Laundering Regulations 2003. The Regulations impose high level obligations on relevant persons - sole traders and firms within the regulated sector. For the majority of AAT members, this means sole traders and firms who provide accountancy services, tax advice, and trust and company services to clients.

The Regulations do not impose obligations upon employees, although employees will be indirectly affected by having to comply with the policies and procedures established by their employers in compliance with the Regulations. Any failure by an employee to abide by such policies and procedures will be the employer's breach of the Regulations, for which it will be liable. However, the employee may, as a result, be subject to his employer's internal disciplinary process. This is in contrast to POCA and TA, which impose individual responsibility on professionals within the regulated sector, whether employer or employee.

Failure to apply the Regulations is a criminal offence. It is also a disciplinary offence enforceable by your supervisory authority. However, if you apply the Regulations reasonably then you have fulfilled your obligation and have nothing to fear from the authorities, even if you inadvertently facilitate a client to launder money. Realistically, the only likely danger of falling foul of the authorities is by disregarding the legislation or acting in bad faith in relation to it.

Policies and procedures

Rule (r.20)
The Regulations require relevant persons (sole traders and firms) to establish and maintain appropriate and risk sensitive policies and procedures to prevent activities relating to money laundering and terrorist financing (r.20 (1)). Those policies and procedures must relate to:

- CDD
- on going monitoring of existing clients
- internal reporting to a firm's MLRO
- record keeping
- internal control
- risk assessment and management
- internal communication of such policies and procedures
- monitoring and management of compliance with such policies and procedures
- training (This is not listed in the Regulations as a policy and procedure but it is convenient to include it as such).

Comment

Much has been retained from the 2003 regulations and should be familiar. Nevertheless, this list may be daunting when viewed without the context of accountancy and your own individual practice. However, with understanding and a common-sense approach, the list is easily satisfied. It must be emphasised that your obligation is to apply the Regulations appropriately and proportionately, as would a reasonable accountant in your practice circumstances.
The Regulations are not very prescriptive about form and content of the policies and procedures. They leave you to devise policies and procedures that are suitable in the context of your own practice, but they do require that your policies and procedures provide:

**Rule (r.20 (2))**

(a) For identifying and scrutinising:
- complex or unusually large transactions
- unusual patterns of transactions which have no apparent economic or visible lawful purpose
- activities which you regard as particularly likely by their nature to relate to money laundering or terrorist financing.

(b) For specifying the taking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products and transactions which might favour anonymity.

(c) For determining whether a person is a politically exposed person.

(d) For firms to nominate a MLRO and to ensure that persons in the firm abide by the reporting obligations in the POCA and TA. A MLRO is a person within a firm who will receive all Internal Reports and assess them before deciding whether they justify a SAR to SOCA.

**Comment**

As stated elsewhere in this document, it is clear that the regulations were drafted predominantly with banks in mind. In particular, the requirement to scrutinise transactions, in (a) above, may be a necessary prescription for banks, which have customarily transferred fund upon the bare instruction and without concern for the purpose of the transfer. The simple cheque transaction, repeated millions of times every day, is an example of this. By contract, accountants have a relatively close relationship with clients, and require relatively detailed instructions in order to provide their professional services. Accountants will usually, therefore, satisfy (a) as a matter of course. Although, some inquiry might be necessary to fill gaps in information provided by clients.

**Risk sensitive approach**

Perhaps the biggest change to the Regulations is more a change in approach than in hard and fast rules. This is the encoding into the Regulations of the risk-sensitive approach, intended to provoke a proportionate response to any potential money laundering risk, in preference to the 'tick-box' approach. But this is not a sudden change. The authorities have been talking for some time about a proportionate approach in combination with the need to know your customer or KYC.

The Regulations require the establishment of procedures that are appropriate and risk-sensitive:

*Appropriate* means that your policies and procedures should be reasonable, confining any actions within the bounds of normal professional practice and ethics. You should not embark upon an investigation of your client or ask for information that an accountant would not normally ask for.

*Risk sensitive* means a proportionate response to the risks that you can realistically predict to encounter. Put simply, while you should not be superficial in devising or implementing your policies and procedures, you should not be over-zealous. You should do more when circumstances suggest a higher risk, and less when they suggest a lower risk, but no more and no less than justified by the level of risk that you have assessed. Considering the broader picture, there are two distinct advantages to the risk-sensitive approach, particularly to AAT members, who are generally viewed as posing only a low risk. It allows you to:

- dedicate less time, effort and expense in applying the Regulations in respect of the majority of your clients. (More resources are required in respect of higher risks - the minority of clients)
• more fairly balance competing interests:
  • society’s – not to suffer crime and terrorism
  • your clients’ – not to have their privacy violated unnecessarily
  • yours – to protect the accountant/client relationship and to follow your calling unencumbered by
    unwieldy and oppressive bureaucracy.

The context in which you apply the legislation - your own practice - is immensely important. Risks, and therefore policies and procedures, are expected to vary from practice to practice, from the simple and low key for small practices with a long-established, stable client base, increasing in detail and complexity as practices grow in size and clients are involved in transactions that are more complicated.

The government has accepted that a natural consequence of the risk sensitive approach is that it will not detect or deter all money launderers and that a zero tolerance approach would be over-burdensome for businesses. If you apply the Regulations reasonably in the context of your own practice, you will have nothing to fear from the law enforcement agencies or your supervisory authority, even if you inadvertently act for money launderers or terrorist financiers.

What are the risks?
When we talk about risk, we are describing a combination of three things:
1. Opportunity: - opportunity for a client to exploit your services for money laundering or terrorist financing related activity. Opportunity exists irrespective of the honesty of the particular client. High cash businesses, complex transactions and corporate structures provide heightened opportunity.
2. Likelihood: - of the opportunity being exploited. Your assessment of the opportunity and your client is relevant. A client you know is less likely to exploit the opportunity than a client you do not know; a transaction that does not appear to have an economic purpose represents a heightened likelihood of being a money laundering or terrorist financing transaction.
3. Impact: - the likely negative impact upon society should the opportunity be exploited. It is suggested that the dealing in proceeds from non-accountancy-related crime would tend to have greater negative impact upon society than accountancy ‘irregularities’, as it is likely to be linked to other criminal activity and contribute to the profitability of organised crime.

The source of risk
The risks to your practice may come from a variety of sources, such as:
• the services you provide;
• your client base
• individual clients
• geographic location
• your existing management policies and procedures (or lack of them).

There is overlap between these bullet points but they are useful to separate for analysis. Your policies and procedures will naturally compensate for a mix of influences.

Your services
Some accountancy services lend themselves more readily to exploitation for money laundering and terrorist financing purposes than others. For example, some services can be used to obscure ownership or the source of property, such as:
• services in relation to complex transactions, particularly involving layering
• setting up trusts to distribute funds
• setting up corporate structures, particularly where ownership is opaque

Other services may be used to aid the movement of illicit funds, such as those involving:
• payments to or from third parties
• payments made in cash or by electronic transfer
• cross-border dimensions.

Your client base
The make up of your client base will indicate the general risk that your practice faces in terms of opportunity and likelihood of exploitation, and should determine the general rigour of your policies and procedures. For example:
• Stable, long-term, clients will present a lower risk than new clients. This is not because long-term clients have less opportunity to launder money but because you have had more time to ‘know your client’. This is more about the likelihood of money laundering than opportunity. There is always the risk that a new client is looking for a new practice to exploit or engage in short-term business activity to ‘clean’ criminal property.
• Individual clients are generally perceived to present a lower risk than legal entities. This is because the structures of legal entities (companies, trusts, etc) lend themselves to obscuring the real source, ownership and control of property.
• Some trusts are particularly susceptible to use for obscuring the source and control of property;
• Politically exposed persons (PEPs) are always seen as presenting a heightened risk.
• Clients who you do not meet face to face for identification purposes are also always seen as presenting a heightened risk.
• Clients with an affiliation to countries with high levels of corruption or from which terrorist organisations are known to operate are always seen as presenting a heightened risk.

Individual clients
While a review of your client base can inform you about general risk level faced by your practice, individual clients can present specific risks, to which you must respond. As stated above, PEPs, non-face-to-face clients and clients from certain countries are always high risk but clients outside these categories can also present a high risk, such as those who:
• engage in transactions with no apparent economic rationale
• operating through complex and opaque structures
• deal with third parties who are not readily identifiable or accountable for their participation.

The converse of this is that some individual clients are always seen as low risk (see Simplified CDD, page 25).

Geographic location
Geographic location is generally accepted as a contributing factor to the level of risk. For example:
• Clients with overseas connections, whether they are concerned in an entity’s ownership or are involved in a transaction, may present an increased risk of money laundering or terrorist financing.
• Clients from an area renowned for high levels of crime or certain types of crime, may present an increased likelihood that their transactions are connected with such crime, particularly if they are not local to your practice.
• Clients from a distant location may raise questions of why they have come to you. They could be going from accountant to accountant until they find one they can exploit or until they perfect their CDD responses.

**Your existing management policies and procedures (or lack of them)**
Your own management policies (or lack of them) could present opportunities for unscrupulous clients to exploit your services to deal in the proceeds of crime or direct funds to terrorist causes. The need for appropriate management of the accountant/client relationship is expressed in the regulations as ‘internal control’ (see Internal control, page 39).

**The need for a risk assessment**
To apply the regulations on a risk-sensitive basis, as required, you must:
• have a reasonable estimate of the risks to which your practice is exposed
• establish and maintain appropriate and proportionate policies and procedures to manage those risks. There no need to eliminate risk, merely to reduce them to a tolerable level. What is ‘tolerable’ is a matter of balance between opportunity, likelihood and impact.

**How to conduct a risk assessment**
You may have your own methods of assessing risk. The following is merely a suggestion.

The management of risk is engrained in today’s business culture, and most large organisations, including the AAT, carry out regular risk assessments with the aid of a risk register. This practice may be alien to many AAT members but it is a simple one. All practices, from the smallest to the largest, can easily develop a risk register to reflect their own particular risk profiles. It is important not to follow the example in this guidance slavishly, but strive to reflect your own practice’s risks. The size and detail of risk registers will, no doubt, differ between practices to reflect their different risks.

The advantage of the risk registers is that policies and procedures emerge from it organically. It is also a physical record that you have taken a rational and considered approach to your legal obligations. Record keeping is more important than ever, now that your practice will be supervised and monitored for compliance with the Regulations.

To carry out an effective assessment of your risks, you should assess your practice in context. You should be careful to assess the three elements of risk (opportunity, likelihood and impact) even in relation to clients that you know and trust. There is no magic formula for devising a risk register - it is more art than science. It is simply a matter of:
• listing the realistic risks that you can think of
• categorising the various elements of the risk as H (high), M (medium) or L (low), taking account of any current management policies (if any)
• finding the aggregate of the various elements
• using your imagination to devise a way of managing that risk (if necessary)
• assessing the level of risk (H, M, L) after the management strategy has been implemented.

To set your level of risk, you should apply your experience and common sense – your best guess. One person’s assessment may well be different from another’s but there is nothing wrong with that. It is important to review your risk register periodically, so that you can re-evaluate the risks and the effectiveness of your management policies. A simple risk register is provided below for you to adapt to your own circumstance:
**Risk register:** to consider risks of money laundering/terrorist financing and to formulate policies to manage such risks. Risks arise from, for example: obscure ownership, source and destination of property and nature of transactions; third parties acting through clients; transactions dealing with the proceeds of crime and to supply funds for terrorist activity.

<table>
<thead>
<tr>
<th>Opportunity</th>
<th>Characteristics</th>
<th>How Likely (a)</th>
<th>Impact (b)</th>
<th>Aggregate risk (a) + (b) ÷ 2</th>
<th>Management policy</th>
<th>Resultant risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services/licensed areas</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complex transactions - new client</td>
<td>Layering; obscure ownership of property, source, destination of funds; no commercial purpose</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>Identify all parties and source and destination of funds (enhanced CDD)</td>
<td>M</td>
</tr>
<tr>
<td>Complex transactions - long-standing client</td>
<td>Ditto</td>
<td>L</td>
<td>H</td>
<td>M</td>
<td>M level ongoing monitoring</td>
<td>L</td>
</tr>
<tr>
<td>High-cash business – long-standing client</td>
<td>Current client - satisfactory KYC information – moderate sums</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L level ongoing monitoring</td>
<td>L</td>
</tr>
<tr>
<td>High-Cash business – new client</td>
<td>New client – overseas connection</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>Enhanced CDD and ongoing monitoring</td>
<td></td>
</tr>
<tr>
<td>Payroll: - ghost employees; non-payment of tax and NI</td>
<td>Usually perpetrated by employee – difficult to detect</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>Ongoing monitoring/be aware of possible exploitation</td>
<td>L</td>
</tr>
<tr>
<td>Tax services – tax evasion</td>
<td>Figures do not reconcile and false invoices.</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>Persuade to regularise</td>
<td>L</td>
</tr>
<tr>
<td>Clients</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-face-to-face</td>
<td>Medical reason</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>Enhanced CDD - obtain medical evidence as extra</td>
<td>L</td>
</tr>
<tr>
<td>Non-face-to-face</td>
<td>Business trips</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>Enhanced CDD – obtain info. about business interests</td>
<td>M</td>
</tr>
<tr>
<td>Involvement of 3rd party</td>
<td>non-commercial transaction; unusual transaction;</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>Enhanced CDD and enhanced ongoing monitoring</td>
<td>M</td>
</tr>
<tr>
<td>Area of high crime – cash business</td>
<td>Area’s reputation</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>Be aware that source of funds may not be legitimate –</td>
<td>L</td>
</tr>
</tbody>
</table>
### Involvement of person(s) in high risk foreign country

|       | New client - overseas trade | H | H | H | Enhanced CDD enhanced ongoing monitoring | M |

### Management policies

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>M</th>
<th>H</th>
<th>H</th>
<th></th>
<th>L</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acting for acquaintances</td>
<td>Poss. compromise of objectivity</td>
<td></td>
<td></td>
<td></td>
<td>Training to focus on maintaining objectivity</td>
<td></td>
</tr>
<tr>
<td>CDD undertaken by junior member of firm</td>
<td>Inexperience – may not recognise suspicious circumstances</td>
<td></td>
<td></td>
<td></td>
<td>Improve lines of communication with managers</td>
<td></td>
</tr>
<tr>
<td>Junior acts in relation to complex transactions</td>
<td>Inexperience – may not recognise suspicious circumstances</td>
<td></td>
<td></td>
<td>M</td>
<td>Improve lines of communication with managers</td>
<td>L</td>
</tr>
</tbody>
</table>

The above is an example of a simple risk register. The above format is Portrait on A4 but Landscape on A3 is a better.

Assignment of the above risk values (H/M/L) is for illustrative purposes only, having been made without the context of real circumstances. Your assessment will be based on the individual circumstances of your practice and your particular client base. The risks identified by you and the values and solutions you attach to them are, therefore, likely to differ to those illustrated.

Areas of risk do not necessarily fall into neat categories but overlap and any particular risk should be seen as an accumulation of all elements together. There are no absolutely rights or wrongs when identifying risks, rating them as H/M/L or in the formulation of a proportionate response. All you can do is to make estimates based upon your experience and common sense. This lack of absolute certainty may cause discomfort to some but this is the nature of professional judgment. As long as your estimates are honest and within the wide band of reasonableness, your judgment will be valid, even if your estimates differ from those of others.

### Risk register columns explained

**Opportunity:** The purpose of this column is to identify the various opportunity risks that exist in relation to your particular practice. It is important to be realistic, and not include fanciful risks.

**Characteristics:** the purpose of this column is to record details of the opportunity to enable you to maintain consistency of decision-making by identifying consistencies or distinguishing between the risk register examples and any case in hand.

**How likely:** This is your estimate of how likely it is that a particular risk will materialise. If you have identified a risk, there is always a possibility that it will materialise. How likely that is depends upon how well you know the particular client.
**Impact:** This is the estimate of the negative impact to society if the risk were to materialise. This is, perhaps, the most difficult assessment, as it may relate to the crime underlying the money laundering, as well as the value of the property. Some transaction lend themselves more readily to organised crime and terrorism than others, including those involving overseas dealings, particularly with countries where corruption is rife and terrorism sponsored or tolerated, or from areas of high instances of drug dealing; complex transactions and corporate structures, which could obscure ownership; and high value transactions. It is suggested that the negative impact on society corresponds to the potential negative impact upon your practice. Clearly, the more serious the negative impact, the more likely you are to become involved in a money laundering investigation.

**Aggregate risk:** An aggregate of the values in the ‘how likely’ and ‘impact’ columns will provide you with a workable value for determining the rigour of your (proportionate) response to the particular risk.

**Management policy:** This records the proportionate response to the identified risks – the policies and procedures for forestalling and detecting money laundering, as required by the Regulations. Whether you implement or change a policy will depend upon your assessment of the magnitude of the aggregate risk.

**Resultant risk:** This is your assessment of the risk should the Management policy be implemented. It is a useful marker for future review of your risk assessment, in light of experience of its implementation.

**Risk assessment of individual clients**
Although your risk register will reflect your practice’s general risk profile, you can assess individual clients by comparing their characteristics and transactions with those listed in it. This will promote consistency of treatment of clients. You will need to assess individual clients and record such assessment but this does not have to be very detailed or difficult. The adaptation of a single row from the risk register is likely to be adequate. For example (see also page 36):

**John Smith:**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>High cash but long establish business</td>
<td>New client – moderate sums –no beneficial owner</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>Standard (medium) CDD measures and on-going monitoring</td>
<td>L</td>
</tr>
</tbody>
</table>


Customer Due Diligence (CDD)

If you have been compliant with the Money Laundering Regulations 2003, you will be used to identifying new clients and taking photocopies of their identification documents. The Regulations have expanded the identification procedures and renamed them CDD but they have also sought to simplify compliance, by allowing flexibility in the way you gather and record relevant information.

Under the 2003 regulations, the term 'identification' included both concepts of:
- finding out who the client claims to be
- obtaining evidence in support of that claim.

Under the current regulations, ‘identification’ means merely to ascertain who the client says he is (this does not have to be a tortuous process – just ask your client); obtaining the supporting evidence is now called ‘verification’. It was necessary to separate these concepts, to accommodate the risk-sensitive approach. Now, although identification is required in all circumstances, verification should be conducted on a risk-sensitive basis. Put simply, although you should always ascertain a client’s (and any beneficial owner’s) name, address, and possibly date of birth, the amount and quality of evidence you gather to test the truth of their claims should vary according to the level of risk of money laundering or terrorist financing that they present.

The three elements of CDD

Summary
CDD is not just about checking that the client is who he says he is. It is also about checking whether any individual has real influence over the client, and if so, whether his relationship with the client is transparent; and checking whether transactions conducted are open and above board. The three elements of CDD, as paraphrased, are to:

a) identify the client and verify (on a risk sensitive basis) his identity
b) identify any individual (beneficial owner) who has influence over the client and verify (on a risk sensitive basis) his identity, so that you are satisfied that you know who he is

c) obtain information (on a risk sensitive basis) about the purpose of transactions.

Although documents, such as utility bills, driving licences and passports, are likely to remain the preferred evidence of verification, the Regulations now permit reliance upon a wider source of evidence, including data and information. And you do not have to keep hard copies of verification evidence. It is sufficient to record key references, so that the original evidence can be traced, if necessary. For example, you would record the number, client’s details, and the expiry date of a passport. This will save on storage space and the inconvenience that photocopying entails.

Rule (r.5)
CDD measures means:

(a) identifying the client and verifying the client’s identity on the basis of documents, data or information obtained from a reliable and independent source
(b) identifying a beneficial owner (who is not the client) and taking adequate measures (on a risk sensitive basis) to verify his identity so that you are satisfied that you know who the beneficial owner is – including, in the case of a legal person, trust or similar arrangement, measures to understand the ownership and control structure
(c) obtaining information on the purpose and intended nature of the business relationship.

Commentary
Taking each element in turn and expanding upon the italicised terms:

(a) "identifying the client and verifying the client's identity on the basis of documents, data or information obtained from a reliable and independent source;"

Identifying means to ascertain who a person claims to be; verifying means to obtain evidence that tends to show that the person is who he says he is.

An individual’s identity consists of a totality of his name, current address, previous addresses, date of birth, place of birth, physical appearance, employment history, financial history and family circumstances. However, the AAT encourages a proportionate, practical, common-sense approach to the interpretation and application of legislation, and considers that name and address are adequate in the vast majority of cases, although there may be some cases when it may be appropriate to look more deeply into a person’s identity. Sufficient identity information about the client may be apparent from the client’s instructions but if not, ask the client for the identity information that you need. You may also need to ask the client to identify any beneficial owners.

You can take a flexible approach to verification. The Regulations allow you to refer to documents, data or information obtained from a reliable independent source.

Documents: The emphasis of guidance on the 2003 regulations was upon obtaining copies of documents, such as new style driving licences and passports, as evidence of identity. Such documents are still extremely valid, and in all likelihood will remain the evidence of choice for most, but the Regulations make it clear that other forms of evidence are equally valid.

Data: This is an acknowledgment that we now operate in an age when so much data is so freely available electronically and by other means. Some commentators have understood this provision to require professionals to obtain electronic data checks on clients by specialist agencies but this is to misunderstand the Regulations. While it is open to you to obtain a data check from an agency, this is just one option open to you, and is certainly not a requirement. Data is also available from internet search engines, such as Google or Yahoo, and from official sources, such as Companies House, local authorities and regulatory bodies, etc. All are valid sources of data.

Information: Information may be in any form, documents, data, word of mouth, personal experience etc. For example, someone you know and trust may confirm a client’s identity; some members have been to clients’ homes, in which case they have information as to home address; or a client might be in the public eye.

Independent source: An independent source is one over which the client or other person in question has no influence or control. For example, a passport is from an independent source because a government department produced it, even though your client may provide it to you.
(b) “identifying a beneficial owner (who is not the client) and taking adequate measures (on a risk sensitive basis) to verify his identity so that you are satisfied that you know who he is – including, in the case of a legal person, trust or similar arrangement, measures to understand the ownership and control structure;”

A beneficial owner (r. 6): is an individual who (either directly or indirectly) has a specified level ownership or control of, or interest in the property of a company (but not a listed company), a partnership (but not a limited partnership), a trust that administers and distributes funds, or any other legal entity or arrangement.

A beneficial owner is an individual, in relation to:

- a company or partnership (except a listed company or limited partnership):
  - with more than 25% of shares, voting rights or profit
  - otherwise exercised control over the management of the company or partnership.

- a trust that administers and distributes funds:
  - is an individual entitled to a specified interest in 25% or more of the capital of the trust property
  - where there is no such individual, the class of persons vest with the main interest
  - any individual who has control over the trust. Control in this context means a power (exercisable alone, jointly or with the consent of another) under the trust instrument or by law to: deal in trust property, vary the trust, add or remove beneficiaries, appoint or remove trustees, veto the exercise of such powers.

- any other legal entity or arrangement that administers and distributes funds:
  - individuals who benefit from 25% or more of the property
  - where such individual are not determined, the class of individuals vested with the main interest
  - any individual who controls 25% or more of the property.

Individual: Only a natural person (as opposed to a legal person) can be a beneficial owner. Where a legal entity has the requisite ownership or control over the management of the client, it is the individual who has ultimate ownership or control of the legal entity who is the beneficial owner (r.6).

The principle that a beneficial owner can only be an individual seems to be contradicted by the wording ‘including, in the case of a legal person, trust or similar arrangement, measures to understand the ownership and control structure’ (r.5). But legislative drafting is extremely difficult and draftsmen do not always manage to achieve perfect consistency. That is why there are rule for statutory interpretation. Read in the context of the Regulations as a whole, it is clear that the legislative intention is the discovery of the individual(s) who act(s) through the legal entity.

Where a legal entity stands in the place of a beneficial owner, you must take measures to understand the ownership and control structure of the legal entity. This is to discover the ultimate individual beneficial owner(s), and to gauge whether the legal entity is operated on normal commercial lines. If the measures to understand the ownership and control of the legal entity revealed a layered structure or opaque ownership, this would tend to increase the risk classification of the client.

Sufficiency of evidence – general principles: The amount and quality of evidence that you require to comply with your duty to verify the identities of your clients and beneficial owners is of central concern to most professionals. The more pieces of information from different sources that support a person’s
identify, the more likely he is who he says he is. The cumulative effect of evidence is exponential – that is, two pieces of evidence from independent sources are worth more than twice the value of a single piece. But you are not required to prove a person’s identity, merely to obtain the appropriate amount of evidence, taking account of the risks in the context of the individual circumstances. The extent of the evidence that you require will have implications: for your client’s legal right to privacy and confidentiality, convenience, expense and irritation levels; for your legal obligations, convenience, expense, reputation as a client-friendly service provider; and for the accountant-client relationship, generally. Therefore, you should obtain just sufficient evidence (no more or less) that you consider, in your professional judgment, to be necessary.

The Regulations (r.6) provides that it is for you to determine the extent of CDD measures on a risk-sensitive basis, depending on the type of client, business relationship, product and transaction. This applies to both clients and beneficial owners, even though the definition of CDD measures (in r. 7, above) explicitly mentions the risk-sensitive approach only in relation to beneficial owners. This extra reference to the risk-sensitive approach is, presumably, to balance the more rigorous requirement to be ‘satisfied’ in relation to beneficial owners and to discourage overly in-depth investigation.

**Different verification requirements in relation to clients and beneficial owners**

The CDD measures for verifying the identities of clients and beneficial owners are drafted differently. This difference is deliberate and very important, as explained below:

- **a client:** you must verify your client’s identity (on a risk-sensitive basis) on the basis documents, data or information.

Your obligation is to obtain evidence on a risk sensitive basis. There is no requirement to satisfy yourself that you know who your client is. The verification requirement for clients, therefore, lends itself, in part, to a standardised approach. You can place your clients into categories, such as ‘low’, ‘medium’ or ‘higher’ risk, and require appropriate standardised evidence in relation to ‘low’ and ‘medium’. For example, for an individual client:

- low risk verification could consist of a single piece of evidence, such as a recent utility bill bearing the name and address of the client
- medium risk verification could consist of two pieces of evidence from different sources, such as a recent utility bill and a government generated document bearing a signature and photograph, such as a new style driving licence or passport.

It is possible to standardise verification only for low and medium risk clients because the values ‘low’ and ‘medium’ have upper limits. Standardised verification is not possible for ‘higher’ risk clients because the ‘higher risk’ category is without upper limit – a higher risk can lie anywhere on a spectrum between ‘only just above’ and ‘far above’ medium risk. Therefore, higher risks must be dealt with on an individual basis, if a proportionate approach is to be maintained. Such approach to higher risks is termed ‘enhanced CDD’ and is subject to separate rules (r.14).

There is no mystery to ‘enhanced CDD’. It is simply a case to considering the extra risk in its individual circumstances and taking appropriate and proportionate measures to compensate for it. The measures could consist of obtaining one more piece of evidence or it could be much more, depending upon the level of extra risk (see ‘Enhanced Due Diligence, page 26).
Some professionals prefer to operate a two category system, ‘standard’ and ‘enhanced’, which some might find more convenient, but as AAT members are generally considered to represent low risk clients, a three category system, specifically catering for low-risk clients has been illustrated above.

- **a beneficial owner (who is not the client):** you must taking adequate measures, on a risk sensitive basis, to verify his identity so that you are satisfied that you know who he is....

There is nothing inherently sinister about beneficial owners. The vast majority will be legitimate, for example, investors in non-listed companies. However, beneficial owners can be shadowy background figures who exercise influence over a client and/or the client’s property, and therefore have a heightened opportunity to engage in money laundering or terrorist financing, using the client as a shield to remain anonymous and unaccountable.

The European directive that gave rise to the Regulations clearly indicates that beneficial or ultimate owners, as a class, are of particular concern. The concern seems to be one of transparency of activity. The requirement, to satisfy yourself that you know who the beneficial owner is, means that you must look at each beneficial owner on an individual basis.

The dual requirements, to apply the risk-sensitive approach and to be 'satisfied' that you know who the beneficial owner is, seem to be in conflict. But this apparent conflict can be reconciled by regarding ‘satisfaction’ as a variable quality, so that the higher your assessment of the risk, the more difficult it is to attain satisfactions; and the lower, the easier.

(c) **“obtaining information on the purpose and intended nature of the business relationship.”**

This requirement, more than most, demonstrates that the Regulations were aimed primarily at banks, and similar institutions, which have traditionally processed transaction with little or no scrutiny of them. The standard cheque transaction is an example – a bank would transfer funds on the simple instructions exhibited on a cheque, without any inquiry about the purpose and nature of the transfer.

By contrast, accountants need relatively detailed instructions from clients in order to provide accountancy services, and will naturally be more aware of the nature and purpose of client’s dealings. One would expect that in the majority of cases, AAT members will obtain sufficient information on the purpose and intended nature of the business relationship simply by taking and executing the client’s instructions. Of course, there will be instances when the level of perceived risk suggests that you should require further explanation or evidence from the client, such as when a transaction or structure lacks transparency, or you do not understand the economic justification for a transaction, or you do not understand a third party’s involvement.

**CDD illustrations**

1. Inda Black, an accountant, is approached to prepare annual accounts by Elliot’s Ergonomic Chairs Ltd, whose business is the wholesale purchase/retail sale/on-site adjustment of ergonomically designed office chairs. The company’s shares are distributed within a family: 51% to Elliot, the sole director; 23% to Ruth, Elliot’s wife and company secretary; and 26% to Rachel, Elliot’s mother, who has provided Elliot with a start-up loan. The client is Elliot’s Ergonomic Chairs Ltd but many accountants would treat Elliot as the client. Inda treated Elliot and Rachel as beneficial owners, each owning more that 25% of the company’s shares.
Although the company is a new client, its structure is typical for a small business and does not present significant money laundering or terrorist financing opportunities (of course, any business could be used for such activity but ongoing monitoring would be more likely than CDD conducted at the beginning of the business relationship to detect it). Elliot attended Inda’s office and did not give any cause for concern. Inga, therefore rated the client as ‘low risk’.

Inda understood the purpose and structure of the company and the nature of her business relationship with it from merely asking for the information she needed to carry out her instructions. To complete her CDD, she noted the company’s name, company registration number and registered address, and asked Elliot to provide two recent utility bills, one relating to him, and one to Rachel. She decided to apply low level ongoing monitoring.

Inda applied her professional judgment in complying with the CDD requirements but could have done more or less and still have stayed within the bounds of reasonableness.

2. Inda Black, accountant, is approached by Stephanie Morgan, a young clothing designer, trading through her limited company, Sans Elegance Ltd, whose business is to design and produce women’s clothing for high street retailers. As part of CDD in relation to the company, Inda obtained the company’s certificate of incorporation, a list of directors, a list of shareholders and the registered address. Inda noticed that Stephanie is sole director of the company and holds 26% of its shares, the other 74% being owned by Slick Mode Ltd; and that the registered address is with another accountant.

Inda asked about Slick Mode Ltd, and Stephanie explained that it is a holding company owned by her investor, Mr Silvester Archimedes, who part owns several businesses. Mr Archimedes has his own clothing manufacturing business and provides premises and support to young talent in return for shares in their companies. He arranged for all the businesses’ clothing to be made at his factory in Cyprus. Apart from that, Stephanie did not know a great deal about Mr Archimedes, except that he is very charming and has a finger in lots of pies.

Asked why she had not instructed the accountant at her company’s registered address, Stephanie explained that that accountant used to act for her company as well as Slick Mode Ltd but the accountant had told her that there had been a VAT mix-up and HMRC wanted more independence between the two companies. Stephanie was concerned because she had been called in for interview by HMRC in relation to the company’s VAT registration but as soon as she mentioned Mr Archimedes, they terminated the meeting, commenting, ‘we know all about Mr Archimedes.’

Inda conducted a company search on Slick Mode Ltd, which revealed that Mr Archimedes was sole shareholder and that Slick Mode Ltd owned shares in several other UK clothing companies, and a lease on a fashion studio in Oxford Street, London. A Google search revealed a biography of Mr Archimedes, confirming that he was a Cypriot businessperson with homes in London and Cyprus.

Inda had obtained the following information:
- 74% of shares in Sans Elegance Ltd are owned by Slick Ltd, which in turn was owned by an individual, Mr Silvester Archimedes, who was the beneficial owner.
- Mr Archimedes had exercised influence over the management of Sans Elegance Ltd, in terms of manufacture, the choice of previous accountant, and very possibly in VAT matters.
- Mr Archimedes is known to HMRC.
Inda was satisfied that she knew who the beneficial owner was. Although she was concerned that Mr Archimedes might be taking advantage of Stephanie’s naivety, she had seen nothing to raise a suspicion of money laundering or terrorist financing. However, she made a note to subject Sans Elegance Ltd to a medium level ongoing monitoring in case Mr Archimedes should seek to manipulate the accounts. She was content to verify Stephanie’s identity by a driving licence displaying a photograph.

Simplified CDD

Summary

The Regulations acknowledge that certain entities, transactions and products are already subject to much scrutiny and control or are by their nature very unlikely to be involved in money laundering or terrorist financing. Simplified CDD really means that you do not have to carry out CDD in relation to a client, transaction or product within a prescribed list, unless you have a suspicion that they are involved in money laundering or terrorism financing.

Rule (r.13)

A relevant person is not required to apply CDD measures where he has grounds for believing that the client, transaction or product falls within one of the following categories:

- A credit or financial institution in the UK licensed by the FSA
  - a credit or financial institution in an EEA state which is subject to the requirements of the money laundering directive
  - a non-EEA state which imposes equivalent requirements to those in the money laundering directive and is supervised for compliance with those requirements.
  - **Note:** The money laundering directive referred to is ‘Directive 2005/60/EC – on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing’, which sets out a supervisory regime equivalent to that in the UK.

- A company listed on a regulated market (the London Stock Exchange, in the UK). The AIM is not regulated but may be considered as equivalent under the risk-sensitive approach.

- Where the client is a UK solicitor and the product is a pooled account (most likely a client account) and the identities of the persons on whose behalf monies are held is available on request to the deposit holding bank (or other institution)
  - an independent legal professional and pooled account in an EEA state - on equivalent terms
  - a pooled account held in a non-EEA state will conform only if the state imposes an anti-money laundering and terrorism financing regime which is consistent with international standards and the independent legal professional is supervised in that state for compliance with those requirements.

- A public authority in the UK
  - a public authority acting pursuant to a European treaty or secondary legislation and fulfils all the conditions in paragraph two of Schedule 2 of the Regulations.

- A life assurance contract where the annual premium is no more than 1,000 Euro or a single premium is no more than 2,500 Euro.

- An insurance contract for the purposes of a pension scheme where the contract contains no surrender clause and cannot be used as collateral.

- An employee pension, superannuation or similar scheme, which does not permit the assignment of a member’s interest under the scheme, other than as permitted by section 44 of the Welfare Reform and Pensions Act 1999 (disapplication of restrictions on alienation) or section 91(5)(a) of the Pensions Act 1995 (inalienability of occupational pension).
- Electronic money stored on a device, subject to strict specified limits on storage and usage (see Regulation 13(7) (d)).
- A product and any transaction related to such product that fulfils all the conditions in paragraph 3 of Schedule 2 of the Regulations.
- A child trust fund within the meaning of section 1(2) of the Child Trust Funds Act 2004.

Comment
The above rule is complete but not faithfully reproduced. For the sake of clarity and emphasis on matters of likely concern to AAT members, it has been paraphrased, abridged and rearranged.

Although you do not have to carry out CDD in relation to the above entities and products unless you suspect money laundering or terrorist financing, you should still check that the individuals who instruct you are authorised to do so. Many organisations have website which are useful in confirming projects and personnel.

Although the listed items are exempt from CDD, you should still perform ongoing monitoring, as appropriate, on a risk sensitive basis.

Enhanced CDD

Summary
It would be inconsistent to accept that some clients, transactions and products are, by their nature, low-risk, without accepting that others are, by their nature, high risk. The Regulations sets out four circumstances in which enhanced CDD is required - just three of which are relevant to AAT members (indicated by the first three bullet points below). The first is a general requirement to apply enhanced CDD measures in any situation which presents a higher risk and the second and third are specific.

Rule (r.14)
The Regulations require that you apply, on a risk sensitive basis, enhanced CDD measures and enhanced on-going monitoring:
- in any situation which by its nature can present a higher risk of money laundering or terrorism financing
- where a client has not been physically present for identification purposes (see below)
- where you propose to have a business relationship or carry out an occasional transaction with a politically exposed person (see below)
- a credit institution which has or proposes to have a correspondent banking relationship with a respondent institution from a non-EEA state (this provision imposes obligations on credit institutions, and is outside the scope of this guidance).

Comment
There is no mystery in how to conduct ‘enhanced’ CDD. It is merely a question of taking CDD measures that are appropriate and proportionate to compensate for the extra risks in each individual case. Enhanced CDD is conducted on a risk-sensitive basis, as is all CDD but is carried out on an individual basis, which takes it outside a standardised approach. As a higher risk can lie anywhere between just above and far above medium risk, the compensatory measures can vary between doing a little more than required for medium CDD, to much more.

In general higher risk situations, the measures you take are left entirely to your professional judgment. But the Regulations make suggestions or mandatory requirements in relation to the specific circumstance (see below).
As with other CDD requirements, enhanced CDD only has to be conducted when you enter a business relationship or carry out an occasional transaction (that is a single transaction or linked transactions involving 15,000 Euro or more).

**Rule (r.14 (2))**

Where a client has not been physically present for identification purposes, you must take specific and adequate measures to compensate for the higher risk, for example, by applying one or more of the following measures:

(a) ensuring that the client’s identity is established by additional documents, data or information

(b) supplementary measures to verify or certify documents supplied, or requiring confirmatory certification by a credit agency or financial institution which is subject to the money laundering directive

(c) ensuring that the first payment is carried out through an account opened in the client’s name with a credit institution.

**Comment**

The Regulations do not make the actions in (a) to (c), above, mandatory but merely cites them as examples of what would be regarded as ‘adequate measures’. There is, therefore, scope to take further or different measures that you consider, in your professional judgment, to be adequate.

With regard to (a), each additional document or piece of data or information from an independent source that supports the client’s identity greatly increases the likelihood that the client is who he says he is. If your client would otherwise be a low-risk client, from whom you would otherwise have required nothing more than a recent utility bill, you could comply with the enhanced due diligence obligation by requiring a second piece of information, such as a certified copy of his passport. If the reason for absence were illness or disability, it would make sense to require evidence of the illness or disability. Depending upon where the client is on the scale of higher risk, you may well need further evidence to confirm identity, and/or may need to resort to (b) and/or (c).

With regard to (b), the risk-sensitive approach would allow you to rely upon certification by another professional who is subject to the AMLL. The reference to a credit agency is a mere suggestion but may be useful if you doubt the veracity of a document. The reference to ‘a credit agency or financial institution which is subject to the money laundering directive’ indicates that you may use such a regulated entity within the EEA, not just the UK. The ‘money laundering directive’ imposes a UK-style anti-money laundering regulatory regime.

With regard to (c), it is clear from the originating European directive that ‘the first payment’ refers to a payment which is part of a transaction which is the subject of your engagement by the client. The fact that the client has a ‘bank account’ would mean that he has already been subject to CDD, and the payment would be subject to the bank’s ongoing monitoring.

It should be emphasised that just one extra measure may be adequate, although more may be appropriate, depending upon the individual circumstances. The extent of your additional measures should be proportionate to your assessment of the risk, taking into account:

- the client’s reason for non-attendance
- the nature of the client
- the nature of any beneficial owners
- the nature of the business relationship (the nature of the client’s business, transactions, third party dealings etc).

**Rule (r.14 (4))**
Where you propose to act for a politically exposed person, whether in a business relationship or in relation to an occasional transaction, you must:
(a) have approval from senior management
(b) take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or occasional transaction
(c) where the relationship is entered into, conduct enhanced on-going monitoring of the relationship.

**Comment**
The above three measures are mandatory, and self-explanatory. Of course, if you are a sole practitioner, you are senior management.

**Rule (r.14 (5))**
A politically exposed person is:
(a) an individual who is, or has at any time in the preceding year, been entrusted with a prominent public function by:
- a state other than the UK
- a Community institution
- an international body.

Persons entrusted with a prominent public function include:
- heads of state, heads of government, ministers and deputy or assistant ministers
- members of parliament
- members of supreme courts, of constitutional courts or other high level judicial bodies whose decisions are not generally subject to further appeal other than in exceptional circumstances
- members of courts of auditors or of boards of central banks
- ambassadors, chargés d’affaires and high-ranking officers in the armed forces
- members of the administrative, management, or supervisory bodies of state-owned enterprises.

Note: The above list does not include middle ranking or more junior officials.

(b) an immediate family member of such a person, including:
- a spouse
- a partner
- children and their spouses or partners
- parents

A partner means a person who is considered by his national law as equivalent to a spouse.

(c) a known close associate of a person referred to in (a) above, including:
- any individual who is known to have beneficial ownership of a legal entity or legal arrangement, or any other close business relationship with a person referred to in (a) above
- any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a person referred to in (a) above.
Comment
The definition of PEP focuses on officials sponsored by non-UK governments, and provides a list of examples of such individuals. This list is not necessarily exhaustive but it indicates very clearly that the definition is based upon high-ranking officials.

Also included in the definition are individuals who have been entrusted with a prominent public function by an international institution. Reference to such institutions in the definition can be considered as the catchall for such bodies that are not readily identified as an arm of government but carry out a public function.

Corruption is confined to third world dictatorships, although such regimes are typically regarded as high-risk. High-ranking officials of European Institutions have been specifically included in the definition of PEPs, which would appear to be an acknowledgement that European governance is not immune to corruption. For many years the Mafia has been reputed to be involved in EU subsidy frauds, and more recently *The Times* (26 February 2008) reported that an official audit had revealed “embezzlement and fraud on a massive scale” in relation to MEPs’ expenses.

The rationale for regarding high-ranking public officials as presenting a high risk of money laundering or terrorist financing is that they often have large budgets derived from public funds at their disposal. Their authority could mean that they are not accountable or subject to rigorous scrutiny, especially when they operate away from their home country. The opportunity for them to divert public funds to their own use or purpose is, therefore, high.

Typically, fraudsters attempt to mask their association with fraudulent conduct by acting through others. For this reason, persons most likely to be used as a ‘front’ for the official are included in the definition of PEP, namely, immediate family and ‘known’ close associates. This makes sense in theory but in practice it creates a major difficulty in determining whether a client is a PEP for all but the banks and the largest firms.

The provisions relating to PEPs originated as a FATF recommendation, the EU approved them, and the UK government encoded them into domestic law, yet the above institutions have declined to produce a list of PEPs, despite being best placed to do so. Some private enterprises, such as World Check and Factiva, produce PEP lists but the cost of a single-user licence is prohibitive for all but the largest financial institutions and firms.

However, it is questionable whether it was necessary for PEPs to be singled out as a special category, at least as far as accountants are concerned, given their relatively close professional relationship with clients. PEPs are likely to attract enhanced CDD measures in any event, given their strong overseas connection, especially if there is anything unusual about the source of their funds and/or their transactions. Therefore, although you should be aware of the category and nature of PEPs, there is no need for you to agonise about detecting them. You will probably know one when you see one. There may well be tell-tail signs, including one or more of the following:

- possession of a foreign passport
- living in a central city location – near to their embassy (from HMRC guidance)
- official letterheads (from HMRC guidance)
- general conversation
- dealing in funds sourced from an official governmental-type account or organisation
- dealing in funds from overseas
• a lack of an underlying commercial justification for the funds
• dealing in funds of obscure origin
• dealing through a non-UK bank account.

Logically, since the ‘known’ close associate of the official (as opposed to their close family members PEPs) has to be publicly known, it follows that the official will also be publicly known. Therefore, an internet search may provide some information in cases of doubt. Of course, close family may be more difficult to spot, but are likely to draw your attention, according to the above indicators.

If the client has a UK bank account, you will be able to treat him (on a risk-sensitive basis) as not presenting a heightened risk, as banks have the resources to identify PEPs and tend to apply rigorous CDD. You could also consider whether you could rely upon the bank’s CDD (see below).

Also, the Treasury maintains a list of regimes, organisations and individuals with whom you should not deal. Your client may be a PEP and not be included in the Treasury list but it might help to check on http://www.hm-treasury.gov.uk/financialsanctions

Reliance upon CDD carried out by others

Summary
The Regulations make provision for you to rely upon the CDD conducted by others if they are included in a particular class of professionals listed in the Regulations. On the face of it, this is an attractive proposition. However, there are conditions attached to this provision which render it less attractive to you and to the person being relied upon.

Rule (r.17)
You may rely upon CDD performed by persons or organisation specified in the Regulations on condition that:
• they consent to you relying upon them
• you remain liable for failure to apply CDD measures.

The persons and organisation specified in the regulations are:
• an auditor, insolvency practitioner, external accountant, tax adviser, or independent legal professional supervised by one of the bodies listed in Part 1 of Schedule 3 of the Regulations. This list will change from time to time but currently consists of:
  - Association of Chartered Certified Accountants
  - Institute of Chartered Accountants in England and Wales
  - Institute of Chartered Accountants in Ireland
  - Institute of Chartered Accountants of Scotland
  - Council for Licensed Conveyancers
  - Faculty of Advocates
  - General Council of the Bar
  - General Council of the Bar of Northern Ireland
  - Law Society of England and Wales
  - Law Society of Scotland
  - Law Society of Northern Ireland
Note: The AAT is not currently in the list but is hopeful of future inclusion.

• A credit or financial institution (excluding a money service business) which is authorised by the FSA.
• A person who carries on business in another EEA state who is:
  - a credit or financial institution, auditor, insolvency practitioner, external accountant, tax adviser or independent legal professional
  - subject to mandatory professional registration recognised by law
  - supervised for compliance with the requirements laid down in the money laundering directive in accordance with section 2 of Chapter V of that directive.

• A person who carries on business in a non-EEA state who is:
  - a credit or financial institution (or equivalent), auditor, insolvency practitioner, external accountant, tax adviser or independent legal professional
  - subject to mandatory professional registration recognised by law
  - subject to requirements equivalent to those laid down in the money laundering directive
  - supervised for compliance with those requirements in a manner equivalent to section 2 of Chapter V of the money laundering directive.

Comment
The directive referred to above is ‘Directive 2005/60/EC – on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing’. Section 2 of Chapter V sets out the requirement for a supervisory regime, as operated in the UK.

The advantage of relying upon another person’s CDD is that you relieve the client of having to submit to your CDD, which may cause delay and inconvenience, expense and irritation, particularly in relation to matters that connects you and the person on whom you rely. However, you will still bear the responsibility for any inadequate CDD. In relation to instructions that provide little opportunity of money laundering or terrorism financing, you do not need to worry, as CDD would be proportionately light touch. In high risk situations, you should ensure that you can be reasonably confident of the integrity of the person on whom you rely. Also, in high risk situations, it is advisable to deal with the other person in writing and obtain a copy of their CDD verification evidence.

As stated above, the provision permitting reliance is rendered less attractive that it otherwise would be by the attachment of conditions: for you, because you remain liable for inadequate CDD; for the person relied upon, because he must keep copies of the CDD evidence for five years starting with the date on which he is relied upon, and within the five years, make the records available to you if you request them (which may involve retrieving them from archive). So, do not be surprised if your reliance request is met with a frosty response.

When you must carry out CDD

Summary
One of the primary objects of CDD is to prevent money launderers and terrorist financiers from gaining access to professional services. So, to fulfil this purpose, CDD measures must be applied at the start of an encounter with a client.

Rule (r. 7)
Sole traders and firms must apply CDD measures on a risk-sensitive basis when they:
• establish a business relationship
• carry out an occasional transaction
• suspect money laundering or terrorist financing
• doubt the veracity or adequacy of documents, data or information previously obtained for the purposes of identification and verification
Commentary
To appreciate these rules fully it is necessary to understand the definitions of the highlighted terms.

A business relationship is a professional relationship between a professional and a client which the professional expects (when contact is established) to have an element of duration.

As far as the majority of AAT members in practice are concerned, a business relationship would merely be an ongoing arrangement to provide accountancy and related services on a rolling basis, or perhaps, to deal with a firm’s accountancy issues as and when they arise.

An occasional transaction is a transaction (carried out other than as part of a business relationship) amounting to 15,000 Euro or more, whether the transactions carried out in a single operation or several operations which appear to be linked.

This definition is in similar terms to the definition of the 'one-off transaction' in the 2003 regulations, but more accurately reflects the fact that a client can undertake more than one such transaction. CDD is unnecessary in relation to a client undertaking a transaction outside of a business relationship involving less than 15,000 Euro, unless there is a suspicion that the transactions is connected with money laundering or terrorist financing.

An occasional transaction is one which has its own identity and defined limits. The same client may repeatedly instruct an accountant in occasional transactions, as long as each instruction has its own identity and definite limits. It is for you and not your client to decide (when first engaged by the client) whether the relationship has an element of duration, and is, therefore, a business relationship, or whether it is a discrete transaction above or below the threshold of an occasional transaction. You must exercise your professional judgment in this matter. Of course, professional judgment is fallible and you may get it wrong occasionally, or circumstances may arise that cause you to reassess your decision. A misclassification between business relationship and occasional transaction is of no significant consequence. However, if it is necessary to reclassify upwards from a transaction outside of a business relationship involving less than 15,000 Euro to an occasional transaction or a business relationship, you should then apply the appropriate CDD measures.

This will happen when seemingly separate transactions later appear to be linked, taking the combined value of property involved above the occasional transaction threshold. As money launderers and terrorist financiers may deliberately enter numerous transactions below the 15,000 Euro threshold to avoid CDD, you should consider whether, in all the circumstances, this causes you to suspect or forms reasonable grounds to suspect money laundering. However, legitimate commercial activity takes many forms and is subject to change, so do not assume that a linked transaction is necessarily untoward. The mere existence of a link, although a possible cause for concern, is unlikely, by itself, to be a sufficient basis for suspicion or reasonable ground for suspicion. Further evidence of money laundering will usually be necessary.
Timing of verification

Summary
The general rule that CDD measures must be applied at the beginning of an engagement could seriously disrupt commercial activity if executed inflexibly, possibly preventing a business from fulfilling its contractual/statutory obligations or capitalising upon commercial opportunities. It could also restrict a business’ commercial freedom to change professional advisors mid-transaction or until there is a lull in commercial activity. R.9 introduces tolerance, to reduce the harsh effects of strict application of CDD, but only in low-risk situations.

Rule (r. 9)
You must always, without exception, identify your client and any beneficial owners (find out who they say they are – at least name and address) before you carry out an occasional transaction or establish a business relationship.

You must also verify their identities (obtain corroborative evidence) prior to acting upon instructions, except:

• where to do so would interrupt the normal conduct of business
• there is little risk of money laundering or terrorist financing occurring.

If you rely upon this exception, you must complete the verification as soon as practicable.

Comment
This regulation does not specifically require application of the third element of CDD – obtaining information about the purpose and nature of the transaction or business relationship. However, this is an implicit requirement to a certain degree, if you are to make an assessment of risk. But, as stated elsewhere in this document, unlike banks and some other professions, accountants obtain such information as a matter of course in order to provide their services.

The interruption of normal conduct of business can only be a matter of timing – not having enough time to complete the CDD before the particular transaction reaches a critical moment. You should make a careful file note of the circumstances justifying reliance upon this exception.

Illustration
Inda Black, accountant, was approached by an employer, who was concerned that his payroll would not be completed in time for his staff to receive their salary payment by the usual payday. The employer had recently terminated his business relationship with an accountant and had been too busy to engage another. Although it would have been possible for Inda and the employer to complete appropriate CDD, it would have been disruptive to other business activities. Inda agreed to defer verification of the identities of the employer and his beneficial owners until after completing the current payroll.
If you are unable to satisfactorily apply CCD measures

Summary
You are not obliged to complete CDD when acting in privileged circumstances, and so can continue to act in privileged circumstance without having completed CDD. However, in privileged circumstances, you will not be providing services with direct commercial benefit to the client.

In other circumstances, you must disengage yourself from the client if he fails to satisfy the CCD measures that you have applied as a result of your risk assessment of him. If the client fails to satisfy the CDD you must consider the reason for such failure, and whether you should make a Report.

Rule (r.11)
Where you are unable to apply CDD measures as required by the Regulations, you must:
• not establish a business relationship or carry out an occasional transaction with the particular client
• terminate any existing business relationship with the client
• consider whether you are required to make a disclosure under POCA or TA.

Comment
As you will have determined the rigour of the CDD measures according to your perception of risk, you will not be justified in continuing an engagement if those CDD measures are not satisfied. If you know or suspect or if there are reasonable grounds for you to know or suspect that the failure to satisfy the CCD measures was due to your client, any beneficial owner, or any other connected person engaging in money laundering or terrorist financing, you must make a Report.

However, be aware that your client may have a legitimate reason for any failure on his part to satisfy the CDD. Reasons may vary widely and can be idiosyncratic, so keep an open mind. Some people may simply object to providing information that they believe to be unnecessary. This attitude can be reduced by you explaining the legal requirement for you to obtain CDD evidence, and by not asking for more than would be proportionate in the circumstances.

If you decide not to make a Report, you may wish to make a file not to show that you have considered making one, and recording the circumstances and reasons supporting your decision not to.

Ongoing monitoring

Summary
A person who is intent upon acquiring your professional services to facilitate money laundering or terrorist financing may present himself as a legitimate client or act through an existing client (whether by deceit, coercion or persuasian). He may engage you in relation to a corrupt transaction well into the business relationship, after having won your trust by satisfying your CDD measures and by a course of dealing. In this scenario, CDD alone would not prevent abuse of your professional standing. Ongoing monitoring is, therefore, a logical inclusion in the anti-money laundering principles.

Rule (r.8)
You must conduct ongoing monitoring of a business relationship. This means:
• scrutiny of transactions throughout the relationship to ensure that they are consistent with your knowledge of the client, his business and risk profile
• keeping the CDD documents, data or information up to date.

Ongoing monitoring should be conducted on a risk-sensitive basis.

Comment
The Regulations describe what ongoing monitoring is but they are not prescriptive about how or when to go about it. It could have been called ongoing CDD (r.7 (2) requires you to apply CDD measures at appropriate times to existing customers). As with CDD, ongoing monitoring should be conducted on a risk-sensitive basis, and the measures adopted should be proportionate to your assessment of the risks.

Some supervisory authorities may specify measures and frequency of ongoing monitoring but that is consistent with their view of what is suitable for their members. The AAT advocates members determining such matters according to their own professional judgment.

The requirement to conduct ongoing monitoring at appropriate times is not necessarily an onerous obligation. Accountants, by the nature of their services, have a relatively detailed knowledge of their client’s transactions, and will usually be aware of the nature of those transactions. For the majority of AAT members, it is expected that ongoing monitoring will take the form of:
• being aware any transactions that are out of character with the clients normal business or business methods
• taking measures to understand transactions that appear to be opaque or lack a commercial rationale
• keeping client’s CDD records up to date.

For example:
• If you have cause to doubt the veracity of verification or any other information obtained during CDD, you should take measures to obtain further evidence on your area of doubt.
• If you become aware that an existing client suddenly has an injection of cash, seems to be influence by a third person, embarks upon a transaction which is inconsistent with usual business or appears to be without commercial justification, etc you should take CDD measures appropriate to your assessment of the risk.
• If a client changes or acquires an additional partner or director, changes it business activities, or address, etc you should update your records.

Enhanced ongoing monitoring
As with enhanced CDD, the purpose of enhanced ongoing monitoring is to manage the extra perceived risk. Enhanced ongoing monitoring for AAT members is likely to be the maintaining of heightened alertness in relation to the particular business relationship and to take proportionate CDD measures when appropriate.

Record keeping
Summary
The keeping of records serves a dual purpose, to:
• create and maintain a paper trail in case the authorities decide to investigate your client
• enable you to demonstrate to your supervisory authority that you have complied with your obligations under the Regulations, or to law-enforcement authorities that you have complied with the AMLL.
The paper trail consists of two types of record:

- a copy of or references to the identification and verification evidence
- supporting records – which consist of the originals or copies of documents relating to a particular transaction that has been subject to CDD measures or ongoing monitoring.

Both types of records must be kept for a five year statutory retention period but the period for each has a different start date, as follows:

- a copy of or references to the identification and verification evidence must be kept for five years starting on the date that the occasional transaction is completed or the business relationship ends
- supporting records must be kept for five years starting on the date the transaction that has been subject to CDD measures or ongoing monitoring is completed.

Your supervisory authority will expect to see evidence of your practices:

- Practice level risk assessments, which are necessary as the basis for the formulation of proportionate policies and procedures, as required by the Regulations.
- Client-specific risk assessment, which are necessary as the basis for the determination of the appropriate level of CDD and/or ongoing monitoring.
- Policies and procedure, as required by the Regulations.

Rule (r.19)
The three paragraphs above are paraphrased extracts of the Regulations.

Comment
The Regulations allow you to keep references to the identification and verification evidence in preference to photocopies. However, supporting records must consist of hard copies, either original documents or copies. Supporting records are not records of all transactions, but only those which have been subject to CDD measures or ongoing monitoring. In this guidance, ongoing monitoring is described as ‘being aware’, this could include all transactions. It is suggested that, for the purposes of this rule, supporting records are those relating to transactions which have been subject to extra CDD measures or have led to an updating of CDD records.

The Regulations require supervising authorities’ to monitor their members’ compliance with the Regulations – not with POCA and TA. The AAT, therefore, is not concerned with Reports, but merely that you have performed the necessary risk assessments, and that you have established and maintained the required policies and procedures.

How much information and detail you record is a matter for your professional judgment but it is important that you can demonstrate to your supervisory authority that you have assessed your risks and established proportionate policies and procedures. A regularly updated risk-register may suffice for your general practice risks, policies and procedures. In addition, you will need to assess the level of CDD for each client, taking account of his individual circumstances. However, such records may be brief. For example, in addition to the identification record, you might note,

“New client - web designer – parent provided £5,000 loan and is beneficial owners with 26% share of company. Client / beneficial owners L risk – business activity M risk – medium (or standard) CDD and ongoing monitoring.” (See Risk assessment of individual clients, page 18).

You may need to record more detail for higher risks, complex transactions and clients.
Most commentators advise that records relating to money laundering be kept separate from client files, to avoid the inadvertent tipping off, in the event that the client or his agent should want a copy of accounting papers.

**Internal reporting procedures**

**Summary**
A sole practitioner who does not employ or act in association with anyone else does not have to establish and maintain an internal reporting procedure. A sole practitioner must comply with POCA and TA to the same extent as a firm but, whereas a practitioner within a firm must make an Internal Report to the firm’s MLRO if he knows or suspects or has reasonable grounds to know or suspect that another person is engaged in money laundering, a sole practitioner must make a SAR directly to SOCA.

The Regulations require firms to appoint a MLRO to act as the firm’s interface with SOCA. The MLRO will receive all Internal Reports of suspicious activity and decide in light of information available to him whether a SAR to SOCA is justified and whether the firm needs consent from SOCA to proceed with a client’s instructions.

The Regulations require firms to establish and maintain a policy and procedure for internal reporting of suspicion activity to the MLRO. This will relate the reporting obligations, set out in POCA and TA, to the firm’s analysis of its particular risk profile. It will also achieve consistency throughout the firm to the submission of Internal Reports.

A policy and procedure should ensure that all relevant personnel know how to make an Internal Report and who to report to. It should also set out the internal reporting method, level of formality, and the amount of detail to be reported, which may vary from firm to firm. For example, one firm may encourage its personnel to have a ‘quiet word’ with the MLRO, so that he can decide whether a suspicion is justified; another may devise its own standard reporting form.

**Rule (r.20 (2) (d)**
A firm must establish and maintain an appropriate and risk-sensitive policy and procedure relating to internal reporting which requires:

- the appointment of a MLRO
- anyone in the firm to whom information comes in the course of business as a result of which he knows or suspects or has reasonable grounds to know or suspect that a person is engaged in money laundering or terrorist financing, to report such to the MLRO
- the MLRO to consider such report in light of any other relevant information which is available to the firm and determine whether it gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion that a person is engaged in money laundering or terrorist financing.

**Commentary**
Information that comes to an accountant in privileged circumstances should not make a Report based on such information (see Privileged circumstances, pages 52 and 60).

**The Money Laundering Reporting Officer (MLRO)**
The duties of a MLRO are onerous, as he is personally liable to criminal prosecution if he breaches them. He is the focal point within his firm for receiving Internal Reports from the firm’s personnel and dealing with SOCA.
The MLRO must:

- receive Internal Reports from the firm’s personnel
- conduct internal investigations of any relevant information held by the firm
- decide, in the light of information available to the firm, whether the Internal Report gives rise to knowledge or suspicion or reasonable grounds to know or suspect a person of money laundering or terrorist financing
- if the information does not give rise to knowledge or suspicion, give consent for the firm to proceed with the client’s instructions
- if an internal report does give rise to:
  - knowledge or suspicion of money laundering or terrorist financing, the MLRO must refuse consent for the firm to execute the instructions which gave rise to the Internal Report until he receives consent from SOCA (actual or deemed), and he must submit a SAR to SOCA, requesting consent
  - reasonable grounds to know or suspect only, he must submit a SAR to SOCA. Consent to proceed is unnecessary.
- liaise with SOCA.

The MLRO should be of sufficient seniority to

- gain access to all of the firm’s files and business information, so that he may consider an Internal Report in light of other information held by the firm
- carry out his functions free from the influence of others. The MLRO must exercise his independent judgement at all times.

**MLRO offences**

**Rule**

Under section 331 POCA, a MLRO commits an offence if he fails to disclose to SOCA his knowledge or suspicion or any reasonable grounds to know or suspect that another person is engaged in money laundering as soon as he reasonable can after receipt of the Internal Report that gave rise to such knowledge or suspicion or reasonable grounds. The only defence available to him is that he has a reasonable excuse for not disclosing the information.

**Commentary**

A MLRO must perform his duties diligently. If he fails to do so, he may commit a criminal offence and his firm may be fined. This does not mean that he should be overzealous or act defensively. There is no imperative to decide in favour or submitting a SAR, and an MLRO within accountancy is likely to do so only rarely.

The exercise of judgment rarely meets with universal agreement. The MLRO may often have to make ‘on balance’ decisions but these cannot be regarded as wrong if the MLRO can provide a reasonable rationale for them. For this reason, he should keep adequate records of his decisions relating to his dealing with Reports. A MLRO should also keep a record of the policy and procedure on internal reporting (even if it is very simple) and ensure that all relevant personnel are aware of such policy and procedure. That way, he will be able to demonstrate that he had operated the internal reporting procedure appropriately.

The firm should consider appointing a deputy MLRO to act during the MLRO’s absence. The duty to make a SAR as soon as reasonably practicable does not abate because the MLRO is absent.
The defence of reasonable excuse has not been tested by the court and so is difficult to predict but might include:

- real danger of reprisal
- followed relevant guidance approved by the Treasury
- following a supervisory authority's guidance, even if not approved by the Treasury
- following direction by SOCA or other government sponsored authority.

**Internal control**

**Summary**

This requirement does not apply to sole practitioners who do not employ staff or work in association with others. However, an awareness of the issues should reduce the risk of committing a money laundering or terrorist financing offence.

The Regulations cannot set out policies and procedures to cover every eventuality. The term 'internal control' is used as a 'catch all' to encourage you to respond to risks, of which you become aware from your risk assessment, and which are not covered by the specific policy and procedure requirement.

**Rule (r.20 (d))**

A firm must establish and maintain appropriate and risk-sensitive policies and procedures relating to internal control in order to prevent activities relating to money laundering and terrorist financing.

**Commentary**

Risks that are not covered by the Regulation’s specific requirements are likely to emerge from your firm’s general risk assessment. Once identified, such risks can be addressed proportionately.

**Illustration 1**

A partner introduces a businessperson to his practice after a conversation at the golf club, a common source of business for many professionals. The partner does not know the businessperson well but they have been acquainted for some time and share a circle of friends. The partner decides to deal with the businessperson’s affairs himself but his familiarity and ‘club mentality’ risks undermining his objectiveness and professional scepticism in relation to his conduct of CDD.

This threat to objectivity from familiarity with clients is emphasised in the *AAT Guidance on Professional Ethics (GOPE)*. The GOPE advises that you may act for persons with whom you are familiar, so long as you maintain your objectivity. The risk to objectivity could be managed by various means, for example, by ensuring that practitioners are reminded of such threats periodically, perhaps as part of the duty to training relevant staff or by partners checking each other’s CDD in such circumstances.

**Illustration 2**

An inexperienced accountant conducts CDD on a client and prepares accounts in relation to a complex transaction. Although technically competent, he lacks the experience to know when the course of the transaction becomes unusual, and the confidence to challenge the client when he feels uneasy.

Inexperienced accountants may provide an opportunity risk if they are assigned to act in relation to high risk transactions or clients. Such opportunity risks could be reduced by implementing management policies that require experienced accountants to conduct such work, or at least, to maintain good lines of communication between inexperienced and experienced accountants.
There are alternative ways to manage the same risk. The details of your policies should be determined by the circumstances of your firm, its risk profile and resources (and your ingenuity).

**Risk assessment and management**

**Summary**
The issues relating to risk-assessment and risk-management have been extensively covered earlier in this guidance.

**Rule (r.20 (e))**
A firm must establish and maintain appropriate and risk-sensitive policies and procedures relating to risk-assessment and management in order to prevent activities relating to money laundering and terrorist financing.

**Comment**
Risk assessment and management is not a one-off process but must be repeated periodically. How often is a matter for your professional judgement? By reviewing your risk assessment, you will be able to gauge the effectiveness of your policies and procedures, and amend them as necessary. It is important to remember that risks do not have to be eliminated but merely reduced to a tolerable level.

**Internal communication of policies and procedures**

**Summary**
Once the requisite policies and procedures have been developed, you must ensure that all relevant personnel are familiar with them to the extent necessary, given their respective role within the practice.

**Rule (r.20 (f))**
A firm must establish and maintain appropriate and risk-sensitive policies and procedures relating to internal communication of its policies and procedures in order to prevent activities relating to money laundering and terrorist financing.

**Comment**
The method and frequency of informing relevant personnel of a firm’s policies and procedures is a matter for the individual firm. As a minimum, new personnel should be informed as part of their induction to the firm, and established personnel should be provided with timely updates. Clearly, this requirement cannot apply to sole practitioners.

**Monitoring and management of compliance**

**Summary**
Firms are obliged to take measures to ensure that its personnel implement its policies and procedures appropriately, on a risk sensitive basis.

**Rule (r.20 (f))**
A firm must establish and maintain appropriate and risk-sensitive policies and procedures relating to monitoring and management of compliance with its policies and procedures in order to prevent activities relating to money laundering and terrorist financing.

**Comment**
Monitoring and management of compliance is a matter for the individual firm in the context of its particular risk-profile. Monitoring of compliance could vary greatly in rigour - for example, from periodic
individual or group meetings, line management, or client file review. It is suggested that compliance is managed in two ways: by ensuring that sufficient information is communicated to all relevant employees and; by dealing with wilful non-compliance through the firm's disciplinary process on the basis that an employee's failure to comply can render the firm liable to a fine or other sanction.

Training

Summary
This requirement does not apply to sole practitioners who do not employ staff or work in association with others. However, sole practitioners must keep up to date with the AML.

A firm's relevant staff must know the applicable law, how to recognise suspicious transactions and circumstances, how and to whom to report their suspicions.

Rule (r.21)
A firm must take appropriate measures so that all relevant employees are:
(a) made aware of the law relating to money laundering and terrorist financing
(b) given regular training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.

Commentary
Again, who is trained and the level and frequency of training should be on a risk sensitive basis. The form of the measures taken to fulfil this obligation is a matter for each particular firm, taking account of its size, complexity and risk profile.

Not all employees need necessarily receive training but it is essential that those who deal with client matters do. The MLRO may be best placed to decide who should be trained and the training content.

All relevant staff should receive training in line with their responsibilities and activities. Firms should consider whether support staff should receive some training, particularly in relation to tipping off and confidentiality, so that they know not to repeat sensitive information outside work or at inappropriate times. If their roles bring them into contact with clients, client funds, client accounts or identification procedures, they may need to be able to recognise a suspicious transaction.

Employees' awareness of the law can be restricted to practical application of the money laundering and terrorist financing definitions, how to avoid tipping off, and the firms relevant policies and procedures. They are not expected to become experts in the law.

Ongoing training should be provided, as appropriate, to ensure that the relevant employees are kept up to date. Also, to avoid the risks arising from untrained staff, training should be part of new employees' induction to the firm. It is advisable to keep records of training, to counter possible allegations that it had failed to comply with its obligations under the Regulations.

Client account
Funds paid from your client account gain the appearance of legitimacy. Therefore, you should not merely receive funds into the account and pay them out again upon the instructions of another person. The client account should only be used for purposes connected with your provision of a service in which you are licensed to practise.
You should think carefully before disclosing your bank account details, as this may allow money to be deposited into it without your prior knowledge. If it is necessary to provide these details, ask the client where the funds will be coming from.

**Suspect territory**
The Treasury may direct any relevant person not to:
- enter into a business relationship
- carry out an occasional transaction
- proceed any further with a business relationship or occasional transaction

with a person situated or incorporated in a non-EEA state to which the Financial Action Taskforce (FATF) has decided to apply sanctions.

You can check to see if a person is a prohibited person or from a prohibited jurisdiction via the following link to the Treasury's webpage: [http://www.hm-treasury.gov.uk/financialsanctions](http://www.hm-treasury.gov.uk/financialsanctions)

**Dealing with SOCA**
**Making a SAR**
SARs must be made in writings, either by letter or on one of SOCA's pro formas. SOCA has two pro forms:
- the Standard SAR form
- the Limited Intelligence SAR form.

These forms, and guidance notes on how to complete them, are available at [Http://www.soca.gov.uk/financialLntel/suspectActivity.html](http://www.soca.gov.uk/financialLntel/suspectActivity.html)

Forms can be conveyed to SOCA by:
- post to The FIU, P.O.Box 8000, London SE11 5EN
- fax to 020 7238 8286
- online via the above web address.

The Limited Intelligence SAR Form was devised for reporting circumstances which were caught by the strict wording of the POCA and TA reporting obligations but the information to be reported was such that the money launderer or laundered property were unlikely to be discerned. The guidance on completing the Form cites circumstances such as, driving away from a petrol station and discrepancies in stock discovered by audit. POCA and TA have now been amended to exclude such circumstance from the reporting obligation, so it is questionable whether the Limited Intelligence SAR Form has any use today. Also, SOCA and most supervisory authorities discourage the reporting of trivial and technical offences.

However, the Limited Intelligence SAR Form still exists and is still held out by SOCA as legitimate. Therefore, you may consider using it when you feel obliged to submit a SAR in accordance with the amended POCA and TA provisions, but think that the information you have is of little use in the fight against money laundering or terrorist financing. Common sense should be your guide in this (see A practical approach to the duty to report, page 53).

If you intend to report non-trivial and non-technical offences, you are likely to use the Standard SAR Form. SOCA prefers to receive the Form via ‘SARs Online’. You will only receive an acknowledgement if you use this method. Before using SAR Online, you will have to register with SOCA.
Clearly, the form was drafted for use by banks, and is difficult for accountants to complete all of the mandatory fields. If you cannot complete a mandatory field type in ‘n/a’, if you can. Otherwise, leave it blank. If you want to keep a copy of the form, print a copy before pressing ‘send’.

Firms that anticipate making over 200 reports per annum may consider subscribing to Moneyweb but this is unlikely for AAT members. The appropriate electronic method for AAT members is SAR Online. There are plans to render SARs invalid unless they are typed and on a SOCA standard form, but until those plans are put into effect, you have the option to make a SAR by letter.

SOCA is interested to receive information about:
- The suspected person, such as, full name, address, telephone numbers, passport details, date of birth, account details. If you do not have sufficient details of the suspected money launderer, include details of the person affected.
- The information forming the basis of knowledge, suspicion or reasonable grounds for knowledge or suspicion and the type of underlying criminal activity, if known.
- Details of the person making the report. This will normally be the MLRO or sole practitioner.
- If you wish to act in relation to a transaction that would otherwise be a prohibited act and so requires consent, tick the box to indicate that you require consent.

**Supervision**

**Summary**

A major change introduced by the Regulations is that all relevant persons (sole traders and firms in the regulated sector) must be supervised in their compliance with the Regulations (with the Regulations only - not with POCA and TA). Therefore, all relevant persons must have a supervisory authority, which may issue guidance and must monitor their policies and procedures.

The Regulations assign supervisory authorities to relevant persons. The Regulations provide that the professional bodies listed in Schedule 3 of the Regulations are the supervisory authorities for their members. The bodies in Schedule 3 are currently:
- Association of Chartered Certified Accountants
- Council for Licensed Conveyancers
- Faculty of Advocates
- General Council of the Bar
- General Council of the Bar of Northern Ireland
- Institute of Chartered Accountants in England and Wales
- Institute of Chartered Accountants in Ireland
- Institute of Chartered Accountants of Scotland
- Law Society
- Law Society of Scotland
- Law Society of Northern Ireland
- Association of Accounting Technicians
- Association of International Accountants
- Association of Taxation Technicians
- Chartered Institute of Management Accountants
- Chartered Institute of Public Finance and Accountancy
- Chartered Institute of Taxation
- Faculty Office of the Archbishop of Canterbury
Insolvency Practitioners Association
Institute of Certified Bookkeepers
International Association of Bookkeepers
Institute of Financial Accountants

This list is liable to change from time to time. The IAB was added on 15 December 2007 by statutory instrument.

By virtue of the Regulations, relevant persons will have a number of supervisory authorities, equivalent to the number of their memberships of such bodies. However, the Regulations allow supervisory authorities, where they are faced with concurrent memberships, to agree between them that just one of them will act as sole supervisory authority. Otherwise they must cooperate with each other in the supervision of the relevant person. The exercise of choice of a supervisory authority by the relevant person is at the discretion of the supervisory bodies, and not as of right.

Your supervisory authority is obliged to make a SAR to SOCA if it comes by information which causes it to know or suspect that a person is engaged in money laundering or terrorist financing.

Rule (r.23, r.24, r.33)
- The professional bodies listed in Schedule 3 of the regulations shall be the supervisory authorities for their members.
- Supervisory authorities must effectively monitor their members and take necessary measures for the purpose of securing their compliance with the Regulations.
- Where a relevant person is a member of more than one supervisory body, the bodies may decide between them which will supervise that person, or otherwise cooperate in their performance of their functions under the Regulations.
- If, in the course of carrying out any of its functions under the Regulations, a supervisory authority knows or suspects that a person is or has engaged in money laundering or terrorist financing, it must promptly inform SOCA.
- Relevant persons without membership of a supervisory body will be supervised by HMRC.
- A relevant person may not carry out his profession [as an accountant] for a period of more than six months beginning on the date on which [HMRC] establishes its register unless included in the register.

Comment
The AAT is a supervisory authority for AAT members. However, the AAT has agreed policies with other Supervisory Authorities for members with concurrent memberships to determine who their sole supervisor should be. Such policies will be displayed on the AAT website.

The AAT’s ethos for supervision is to offer guidance, CPD materials and events, and possibly issuing update bulletins; and to monitor compliance by reviewing the practices of a number of members annually. The reviews will be conducted by desktop, telephone and practice visit.

The key words for monitoring are ‘tolerance’ and ‘advice’, particularly while the Regulations can be regarded as recent. The intention behind reviews is not to catch members out but to provide guidance and advice. No doubt, reviewers will advise some members to do more, but they are also likely to advise some to do less, in accordance with the risk based approach.
The AAT will be expected to use its disciplinary procedures in respect of anyone who acts in flagrant disregard or persistent breach of the Regulations. Those who attempt to apply the Regulation in proportionate manner are extremely unlikely to encounter the disciplinary process, even if they get it wrong. It is envisaged that the disciplinary process will be evoked in relation to those who fail to respond to AAT correspondence or otherwise fail to cooperate with a review. If you are contacted to take part in a review, you should, therefore, acknowledge the contact in a timely manner and cooperate with the review process.

HMRC will be the supervisory authority for anyone who is not a member of a professional body listed in Schedule 3 of the Regulations (unless licensed by the FSA). AAT students are not members of the AAT for the purpose of supervision. Such persons should register with HMRC for this purpose. The Regulations provide that anyone in practice after six months from the date HMRC establish a register will be guilty of a criminal offence.
Proceeds of Crime Act 2002

Summary
Part 7 of POCA is aimed at professionals rather than criminals. There are two reasons for this:

• The services of professionals provide activities relating to money laundering with the appearance of respectability, making them less likely to be detected.

• Skills possessed by professionals are often vital to the success of introducing 'dirty' money back into the legitimate economy.

POCA sets out measures to counter these effects, and to aid investigations by the authorities, by:

• Making it illegal for professionals to become involved in any arrangement which they know or suspect (actual subjective knowledge or suspicion – not the objective test of reasonable grounds) involves the proceeds of criminal conduct, unless they have reported their knowledge or suspicion and obtained appropriate consent to proceed with the arrangement.

• Requiring professionals to make a Report in relation to any person or property which they know, suspect, or have reasonable grounds to know or suspect is involved in money laundering. Although professional must make a Report when they have reasonable grounds to know or suspect, they can proceed with the arrangement without the need to obtain appropriate consent, if they do not actually know or suspect.

• Prohibiting professionals from disclosing that a Report has been made or that an investigation is underway or contemplated - but only if such disclosure is likely to prejudice any such investigation.

Rules

Part 7 POCA
Part 7 POCA sets out three distinct categories of offence:

• **Money laundering** - possessing or dealing in any way or encouraging or helping someone else to possess or deal in property (without the consent of a MLRO or SOCA, as appropriate) when knowing or suspecting that such property originates from criminal conduct (sections 327-329). These offences carry a maximum penalty of 14 years imprisonment and/or a fine.

• **Failing to make an authorised disclosure** - failing to report identifiable persons or property when knowing or suspecting or having reasonable grounds to know or suspect that such persons or property are involved in money laundering (section 330-332). These offences carry a maximum penalty of five years imprisonment and/or a fine.

• **Tipping off** - a person commits an offence if he makes a disclosure that:
  - he or another person has made a Report to a constable, HMRC, MLRO, SOCA; or
  - an investigation is being contemplated or carried out; and
  - the disclosure is likely to prejudice any investigation that might be conducted following the Report, or is being contemplated or carried out.

  Knowledge of the Report or the actual or contemplated investigation must have come to the professional in the course of business in the regulated sector for him to have committed an offence (sections 333* and 342). These offences carry a maximum penalty of two years and/or a fine.

Comment
The provisions on Reporting and tipping off have been amended to improve the intelligence quality of SARs and to dispel the fear and misunderstanding that surrounds the tipping off prohibition.

Before examining the particular provisions of POCA and TA, it is important to understand the concept of ‘knowledge’, ‘suspicion’ and ‘reasonable grounds to know or suspect’, upon which the AMLL relies.

Knowledge and suspicion
The legislation relies heavily upon the existence of knowledge or suspicion. The term ‘knowledge’ has its ordinary meaning (to denote certainty) but ‘suspicion’ has a particular meaning in the law. An understanding of the legal meaning of ‘suspicion’ is vital if you are to apply the law reasonably and in fairness to yourself and your clients.

‘Suspicion’ in the everyday sense could be to merely ‘think that a state of affairs might exist’. In this sense, a suspicion could be firmly held without any evidence to justify it. People who are quick to suspect without evidence are often described as having a ‘suspicious mind’. A suspicious mind is arbitrary and capricious, and unworthy of a professional. Professionals have a duty to uphold clients’ right to confidentiality unless the criteria for setting it aside are clearly established. And clients are entitled to expect a high level of consistency of treatment by all members of a profession. ‘Suspicion’ has a particular meaning in law, and all members should apply the same principles to the process of forming a suspicion.

The courts have provided limited guidance on the correct meaning of suspicion in the context of the AMLL. In the case of the Crown versus Da Silva (2006), the judges stated that in order to hold a valid suspicion, a person “must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice.”

This can only mean that a legitimate suspicion must be based upon evidence. A legal suspicion, therefore, could be thought of as to ‘think that a state of affair might exist because there is evidence to suggest that it does’. In this sense, one may think in terms of ‘suspicious circumstances’.

The evidence upon which to base a suspicion does not have to be strong and does not have to amount to ‘reasonable grounds’ (discussed later) – it could be fairly obvious evidence of, say, a discrepancy in accounts or between lifestyle and declared income; or the evidence could be less concrete, such as a client’s evasiveness to enquiries – but it must be sufficient to enable you to rationalise your suspicion. Ask yourself, ‘why am I suspicion?’ If you cannot identify particular circumstances which would support the existence of suspected facts, then you do not have a rational or legitimate suspicion.

Mere opportunity does not normally constitute suspicious circumstances. For example, a client may operate a high cash business, and therefore have the opportunity to under-declare income. This alone does not entitle you to suspect him of under-declaring income – otherwise you would suspect every taxi driver, builder, hairdresser, and all retailers. This would plainly be an absurd situation, and one that cannot have been intended by the AMLL.

As a professional, you must balance the conflicting interests of the AMLL with your professional ethics and your duty to clients. If you were to act upon an initial suspicion (on little evidence), you may well
satisfy the legislation but compromise your professional obligations to clients. But there is a middle
ground. The judges in Da Silva indicated that a person could,

“entertain a suspicion but on further thought, honestly dismiss it as being unworthy or contrary to
such evidence as existed or as being outweighed by other considerations.”

On this basis, you are encouraged to think of the forming of a legitimate suspicion as a 2-stage process
(in most cases), thereby achieving a reasonable balance between the requirements of the AMLL and
your professional obligations.

**Stage 1: is the ‘initial suspicion’ stage**
The ‘initial suspicion’ stage is where you encounter suspicious circumstances – circumstances which
reasonably give rise to a question over your client’s dealings.

**Illustration:** Your client is a builder who is in a position to work cash-in-hand, and you notice that his
expenditure for materials is disproportionately large compared to declared income. It would be
reasonable, on this evidence, to form a suspicion that the client has under-declared his income.
However, it would be extremely harsh on your client if you acted upon your initial suspicion without first
having tested it by, at least, providing your client with an opportunity to explain the apparent irregularity.
Your initial suspicion might be assuaged if the builder were to provide a reasonable explanation, such as,
‘he purchased materials in respect of a large contract which had fallen through and that he was still in
possession of the materials’.

You cannot expect clients to act perfectly in accounting matters – otherwise they would not need your
expertise. If you had acted upon your initial suspicion, you would have invalidated your professional role
to help your client submit correct accounts, and done him a disservice.

**Stage 2: is the ‘settled suspicion’ stage.**
To test your initial suspicion. You can do this by asking your client to explain the circumstances giving
rise to your initial suspicion. This is no more than your professional duty requires. Only if your initial
suspicion is confirmed at this stage, should you consider acting upon it. Whether you do act upon it may
depend upon your client’s subsequent behaviour.

To sound a note of caution, stage 2 might not be advisable in relation to circumstance that indicate
criminal conduct that cannot otherwise be explained as an accounting irregularity, such as if you suspect
your client of dealing in the proceeds from drug-dealing, people trafficking, burglary, credit card,
mortgage fraud, etc. You can never be expected to put yourself in a position of danger. In such
circumstances you should consider acting upon your initial ‘stage one’ suspicion. This must be a matter
for your professional judgement.

**How to treat your client’s explanation**
Stage 2 raises the question of how to treat your client’s explanation. In deciding whether your initial
suspicion is confirmed, you will have to assess your client’s explanation of the suspicious circumstances.
Again, you must not be arbitrary in your approach to this.

The law presumes that persons are law-abiding. So, you should accept a plausible explanation given by
your client. Of course, a presumption can be overturned by contrary evidence. If your client’s explanation
is self-contradictory or otherwise inherently implausible or if you are aware of contradictory evidence, you
should not accept it. Evasiveness to your inquiries could be evidence that you take into account. Whether you ask for evidence to confirm your client’s explanation is a matter for your professional judgement, taking account of your knowledge of the client and the risk sensitive approach.

Merely making reasonable enquiry into a client’s affairs will not amount to tipping off, so there is no need to feel inhibited in this regard.

**Reasonable grounds to know or suspect**
Reasonable grounds to know or suspect exist when circumstances would cause a reasonable accountant to know or suspect – even if you personally do not know or suspect.

**POCA money laundering offences**

**Summary**
The statutory definition of ‘money laundering’ is so comprehensive that it covers possession or dealing in any way with property which a person knows or suspects represents the benefit of criminal conduct.

**Section 327 concealing etc**
It is an offence for you to conceal, disguise, convert, transfer or remove criminal property from England and Wales, Scotland or Northern Ireland. You could commit a section 327 offence, for instance, if you:
- deliberately omit some of your client’s income from his tax returns, with an intention of wrongly depriving HMRC of tax
- list suspect income or expenditure under a legitimate heading
- facilitate your client’s purchase of shares or insurance from suspect funds
- transfer suspect funds from your client account to an offshore bank account.

**Section 328 arrangements**
It is an offence for you to become involved in an arrangement which you know or suspect facilitates the acquisition, retention, use or control of criminal property by another person. For example, you could commit a section 328 offence if you:
- provide a mortgage reference without making the proper checks that the information you provide is accurate
- complete a client’s tax return when it appears that he has not declared all of his income or has overstated his expenses
- provide accounts in relation to suspect funds in order to disguise them
- provide accounts in relation to a transaction or transfer of funds when there is no apparent commercial rationale for the transaction or transfer
- receive into and pay out from your client account funds that have no connection with a licensed service provide by you.

**Section 329 Acquisition, use and possession**
Accountants are unlikely to commit this offence but they should be wary of clients who have acquired property at an obvious undervalue. Prices of goods can vary greatly – an undervalue would be well below the market price.
Defences to allegations of money laundering (section 327-329 POCA)

Summary
The definition of criminal property (upon which the definition of money laundering is based) requires you to know or suspect that property represents a benefit from criminal conduct, if it is criminal property as far as you are concerned. Therefore, you cannot be guilty of a primary money laundering offence unless you possess actual knowledge or suspicion. Also, as the benefit must be from criminal conduct, the criminal conduct must have already been carried out. The rules also provide three statutory defences to allegations of money laundering under sections 327-329, below.

Rule
You will not commit an offence if you:
• make an authorised disclosure (Report) under section 338 and you have received the appropriate consent (from SOCA or your MLRO) before you carry out the prohibited act
• intended to make an authorised disclosure but you had a reasonable excuse for not doing so
• performed the prohibited act in carrying out a function you had relating to the enforcement of any provision of POCA.

Commentary
From the moment you acquire knowledge or form a [Stage 2] (page 48) suspicion that property is criminal property, you are prohibited from carrying out any act that would be an offence under 327-329. You could undertake preparatory work in anticipation of receiving appropriate consent but you could not make the work available to the client until receipt of such consent.

You must make a Report and receive appropriate consent before you do anything that would amount to a prohibited act, unless you have a reasonable excuse not to, or you carry out the prohibited act as a necessary result of complying with POCA. What amounts to a reasonable excuse has not been tested before the courts but its meaning is likely to be interpreted narrowly. Presumably, a real and reasonable fear of danger would be a reasonable excuse, as would the following of a supervisory authority’s guidance. Also, as supervisory and enforcement authorities advise against the reporting of purely technical offences, this would probably also amount to a reasonable excuse in relation to failure to report such offences. In other cases what would be reasonable would depend on all the circumstances. Where you do not make an authorised disclosure before doing the prohibited act, you should do so as soon as you can.

It may happen that knowledge or suspicion arises only after you have started to act in relation to a transaction, in which case you must still make a Report as soon as you can after you acquired such knowledge or suspicion.

Where there is obligation to make a Report, this does not compel you to continue to act for the client. You are entitled to refuse to act for a client for whatever reason, whether commercial or otherwise. A refusal to act for a client will not amount to tipping off, as long as you do not reveal that a Report has been made.

Even after a report has been made and appropriate consent received, you should remain vigilant for any linked transactions or instructions that cause you concern and which may need to be reported.
Rule
An extra defence applies to section 329. That is, where the property was acquired for adequate consideration.

Commentary
A section 329 (possession) offence is unlikely to be committed by accountants but you need to be aware of it and its defence when assessing a client’s conduct.

Adequate consideration means that the price paid for the property (whether in money, property or in kind) is not substantially below the market value. This does not prevent your clients from making a good bargain. The adequacy of consideration depends upon the circumstances and requires judgment in its assessment but inadequate consideration is often obvious when you see it.

The rationale to this defence must be that your willingness to pay the market rate is sufficient evidence that you did not know or suspect that the property represented a benefit from crime.

The need for appropriate consent, time limits and deemed consent
Once you have made a Report about a client under section 338 POCA, you must refrain from carrying out the client’s instructions until you receive consent from your MLRO, if you are an employee, or SOCA, if you are a sole practitioner or a MLRO.

Section 335 POCA sets out time limits for the granting of consent by SOCA (employed accountants must abide by their firms’ internal procedures and should not proceed without their MLROs’ approval). Consent by SOCA is deemed to have been given if the statutory time limits are not met. Those time limits are as follows:

- Once you have submitted a SAR, consent must be given or refused within seven working days (the “notice period”) starting the next working day after you submitted the SAR. If consent has not been refused by the end of the notice period, you may proceed with the client’s instructions.
- If consent is refused within the notice period, a “moratorium period” of 31 calendar days begins from the day on which you receive notice that consent is refused. You may proceed with your client’s instruction at the end of the moratorium period (or earlier if consent is granted earlier).

SOCA is currently responding to SARs in an average of 2.6 working days and is unlikely to refuse consent to an accountant, where the instructions do not involve the immediate dissipation of assets. SOCA also actively review the moratorium period and currently curtail it at an average of 19 days.

'Failure to report' offences – regulated sector
Summary
The Reporting requirement described above is a defence to the charge of money laundering – a charge that can be raised against anyone, whether they are in the regulated sector or not. There is an entirely separate and additional Reporting duty on persons within the regulated sector, which is intended to provide the authorities with investigation opportunities. Failure to comply with this duty is a criminal offence.

As an external accountant (unless you are acting in privileged circumstances) you have this extra duty to Report any other person, whether a client, a colleague, or third party, if three conditions are met. They are:
1. You know or suspect or have reasonable grounds to know or suspect that another person is engaged in money laundering
2. The information forming your knowledge or suspicion of reasonable grounds to know or suspect came to you in the course of business
3. You can identify the person or the whereabouts of the laundered property or your information may assist in identifying the person or locating the property.

Accountants within a group practice must make an Internal Report to their MLRO, while sole practitioners and MLROs must make a SAR to SOCA.

Rule (s.330)
You will commit an offence if:
- you know or suspect or have reasonable grounds to know or suspect that another person is engaged in money laundering
- the information on which your knowledge or suspicion is based or which gave rise to reasonable grounds for you to know or suspect came to you in the course of a business in the regulated sector
- you can identify the other person or the whereabouts of the laundered property, or it is reasonable for you to believe that the information may assist such identification*
- you do not make a disclosure to a nominated officer (if you are in a firm) or to SOCA (if you are a sole practitioner or MLRO) as soon as practicable after the information came to you.

*inserted by subsection 104(3) of the Serious Organised Crime and Police Act 2005.

But you will not commit an offence if:
- you have reasonable excuse for not disclosing the information
- the information came to you in privileged circumstances
- you did not actually know or suspect that the other person was engaged in money laundering and your employer had not provided you with the appropriate training.

In deciding whether you have committed an offence under this section, the court must consider whether you followed any relevant guidance issued by a supervisory authority or any other appropriate body, which was approved by the Treasury. Even if the Treasury has not approved such guidance, the courts are almost certain to consider it.

Commentary
A clarification of the terms used in s.330 may assist a better understanding of this requirement.

Privileged circumstances
Privileged circumstances are where you provide legal advice, such as ascertaining your client’s tax position (unless you believe that the client has sought your advice in order to commit or continue a criminal offence, such as tax evasion); or you act for your client in actual or contemplated legal proceedings. If you act in privileged circumstances you are exempt from this duty to report.

Reasonable grounds exist where circumstances would cause a reasonable accountant to know or suspect – even if you personally do not actually know or suspect. This is an objective test, which denies professionals any benefit from ‘turning a blind eye’ to information that may lead to actual knowledge or suspicion.
In the course of business
Information must come to you in the course of business. You are not on duty all the time and you may ignore any information that comes to you when not engaged in a regulated activity, such as when at a social gathering. Information received socially, for example, is often unreliable, being rumour, bravado or exaggeration. When acting in the course of business, you are likely to deal with evidence that is more reliable.

You must only report if it would be reasonable to assume that the information you have would assist in identifying the person or the location of the property. This rule was introduced to discourage the reporting of missing stock, when there was no chance of identifying the thief or recovering the property. But the rule is not necessarily confined to the stocktaking situation.

Reasonable excuse
Reasonable excuse has not been defined but it is likely to mean:
• real fear of repercussions
• that you followed relevant guidance from a supervisory authority or law enforcement agency.

A practical approach to the duty to report
Section 330 requires you to make a Report to your MLRO (if within a group practice) or to SOCA (if you are a MLRO or sole practitioner) if you:
• receive information in the course of business, which causes you to know or suspect (having followed the 2-stages to suspicion, page 48) or which provides reasonable grounds to know or suspect someone of dealing with the proceeds of crime; and
• the information would be reasonably expected to assist identifying the person or the location of the laundered property.

A strict application of the wording of section 330 would require you to report the most trivial of matters. However, there is a less pedantic approach. Supervisory authorities and law enforcement agencies discourage the reporting of technical or trivial breaches of the legislation. SOCA’s 2007 annual report focuses on efforts to improve the quality of SARs, and SOCA has stated in a publicly available consultation document (The Proceeds of Crime Act 2002 - Obligations to Report Money Laundering: The Consent Regime – March 2008) that ‘it is not in the public interest to pursue technical and trivial breaches’. This is consistent to the public interest criteria that must be satisfied before a public prosecution is brought. SOCA has pointed out that no one has been prosecuted for a purely technical offence. Clearly, SOCA encourages a common sense application of the money laundering regime.

Common sense or public interest approach
Public interest may be a better way to discriminate between different cases. Broadly speaking, public interest can be thought of as society’s benefit. You can ask yourself, will society benefit if I make a Report? The benefit to society is not necessarily dictated by the value of the criminal proceeds but by the nature of the underlying criminal conduct. The concept is perhaps best illustrated by example:

Illustration 1
Suppose that in the course of business, you have formed a suspicion that a potential client is in possession of a small amount of money derived from a criminal activity, say, low level dealing in marijuana. An investigation of the individual in question could lead up the supply chain to major drug importers and other major organised crime. Likewise, a SAR relating to burglary, mugging, credit card
fraud, etc could lead to other criminals, such as dealers in stolen goods. Society may well benefit from a Report in this scenario.

**Illustration 2**
Now suppose that in the course of business, you have discovered an accounting 'irregularity' - your client has failed to pay tax that is due and owing, and you have formed the opinion that the failure was deliberate. Therefore, you have formed the suspicion that the client has been engaged in tax evasion, but there is no evidence of a wider criminal network to investigate. After some grumbling and bravado about not paying HMRC another penny, the client agrees to put matters right. Any investigation resulting from a SAR in this case would be expensive to the public purse, divert attention from organised crime and merely conclude that your client owed tax and possibly a fine that he has already agreed to pay. Society is unlikely to benefit from a Report in such circumstances.

Clearly, society would benefit more from a SAR relating to conduct that is part of a bigger crime picture, than to an accountancy irregularity which can be regularised by your professional input.

The duty to Report is in relation to someone who “is” engaged in money laundering. An innocent non-payment of tax is not money laundering but a knowing and deliberate non-payment is. In the latter case, you could take the view that, from the moment the client begins the process of reconsidering his decision not to pay outstanding tax, he is no longer engaged in money laundering except in the technical sense and should not be the subject of a SAR.

**Section 331 – failure to report: offence by MLRO**

**Summary**
The reporting duty of MLROs is similar to that in section 330, except that the information must come to him by an internal disclosure under section 330.

**Rule**
A nominated officer will commit an offence if:
- he knows or suspects or has reasonable grounds to know or suspect that another person is engaged in money laundering
- the information giving rise to his knowledge or suspicion or reasonable grounds for knowledge or suspicion came to him in consequence of a disclosure made under section 330
- he knows the identity of the other person or the whereabouts of any of the launderer property, or the identity of the person or the whereabouts of any of the laundered property can be identified by the information, or it is reasonable to believe that the information may assist in identifying that other person or any of the laundered property*
- he does not disclose the information to SOCA as soon as practicable after the information came to him.

*inserted by subsection 104(4) of the Serious Organised Crime and Police Act 2005.

But a MLRO does not commit an offence if he has a reasonable excuse for not disclosing the information. In deciding whether the MLRO has committed an offence under this section, the court must consider whether he followed any relevant guidance issued by a supervisory authority or any other appropriate body, which was approved by the Treasury.
Commentary
The MLRO’s duty to Report is judged on the objective ‘reasonable grounds’ test. This means that, if a reasonable nominated officer would have known or suspected, the nominated officer in question should have known or suspected.

Although section 331 is similar in terms to 330, the nominated officer’s method of arriving at knowledge, suspicion or reasonable grounds to know or suspect is different to that of an employee. Once he receives an Internal Report, he does not merely decide whether or not to pass it on to SOCA; he must carry out checks against any information held by the firm relating to the person who is the subject of the Internal Report. Only then must he decide whether to submit a SAR. If the other criteria are met, he must submit a SAR if he knows the whereabouts of any part of the laundered property.

Again, the court has not determined what may amount to a reasonable excuse but what is reasonable will depend on all the circumstances. If the default was as a result of following relevant guidance, this would probably amount to a reasonable excuse, as would the real and reasonable fear of reprisal. Any other qualifying circumstances are difficult to predict. The nominated officer is not obliged to follow his own regulatory body’s guidance for the purposes of his defence. He may follow any other appropriate body’s guidance, as long as it is relevant. Even if the Treasury has not approved such guidance, the courts are almost certain to consider it.

Tipping off offences – sections 333 and 342
Section 333
Summary
If a money launderer knew that a Report had been made about him or that he is or maybe the subject of an investigation, he would very likely disappear and dissipate the proceeds of crime, frustrating any attempt by the authorities to investigate or confiscate the criminal property. To counter this problem, the POCA makes it an offence to divulge any information that is likely to tip off the subject that a Report has been made or an investigation commenced or contemplated. So, on the rare occasions when you have to make a Report to your MLRO or to SOCA, you must be careful not to commit a tipping-off offence. But, POCA provides a defence to tipping off offences to those who have divulged information in good faith.

Rule
*You will commit an offence if you know or suspect that either:
• a Report has been made to a firm’s MLRO, SOCA, HMRC or a constable
• an investigation is being carried out or is being contemplated following a Report
• you divulge information that is likely to (not might) prejudiced such investigation.

*this is a highly paraphrased version of section 333A POCA, as inserted by Article 4 of The Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007 No. 3398.

Commentary
Tipping off is an area of major concern to many professions, mainly due to so much misinformation about it having been disseminated over the years. This is a pity because a tipping off offence is not easy to commit inadvertently.

Many believe that tipping off occurs if a client guesses that a Report has been made, perhaps because there has been a delay in completing a transaction (while awaiting consent from SOCA). This is a mistaken belief – you cannot expect clients to be stupid, and some will guess where there is a significant delay in proceeding with their instructions – but you cannot commit a tipping off offence by merely
complying with the legislation. However, as SOCA take an average of 2.6 working days to give a response and are unlikely to refuse consent to accountants (unless assets are to be immediately dissipated), this is unlikely to happen to you.

In order to commit a tipping off offence, a Report must have been made or an investigation contemplated. If you haven’t made a Report, you can warn your client that you will make a Report if he does not accept your advice to regularise his affairs. The duty to Report is set out in the AAT’s standards letters of engagement, so clients should be aware of your obligations under the AMLL.

Even if you know or suspect that a Report has been that an investigation is being carried out or contemplated, to commit an offence, you must also know or suspect that the information you divulge is likely to prejudice such an investigation. If you divulge information to a colleague or other professional who is subject to the AMLL, it would be reasonable for you to believe that such divulgence would not be likely to prejudice an investigation – as they are also bound not to tip off.

Parliament has passed a statutory instrument to amend the tipping off provisions, which should give professionals comfort. The S.I. preserves the general permission to disclose, as discussed, but cites specific instances when you may divulge information. The instances cited (with one possible exception) fall within the general permission, so are not important to repeat but they include disclosure:

- to someone in your firm
- professional adviser to professional adviser
- to your supervisory authority.

Section 342 offence of prejudicing an investigation

Rule
A person commits an offence if he knows or suspects that a confiscation investigation, a civil recovery investigation or a money laundering investigation is being or is about to be conducted and he:

- divulges any fact or matter which is likely to prejudice the investigation
- he falsifies, conceals, destroys or otherwise disposes, or causes or permits the falsification, concealment, destruction or disposal of documents which are relevant to the investigation.

But a person does not commit an offence if:

- he does not know or suspect that the divulged fact or matter was likely to be prejudicial to any such investigation
- he does not know or suspect that the documents are relevant to the investigation
- he does not intend to conceal any facts disclosed by the documents from the investigation; or
- the divulgence is made in the exercise of a function under this Act.

Commentary
Anyone reading these sections as they appear in POCA should be aware that the term 'disclosure' has been used to two senses, to denote both the official Report to SOCA or a MLRO, and again, to denote the release of information to any other person. To avoid confusion the terms 'Report' and 'divulged' have been used respectively in the above paraphrasing to distinguish the senses.

You will have a defence to sections 333 and 342 if you did not know or suspect that a Report had been made or that an investigation was underway or pending, even if the information you divulge actually prejudices an investigation. This defence is highly unlikely to be available to the person who made the original Report.
Also, even if you are aware that a Report has been made or that an investigation is underway or pending, you may divulge information in circumstances in which it is not likely to prejudice an investigation. It is not clear how a divulgence will be judged to be ‘likely’ to prejudice an investigation. However, the test will probably be whether a reasonable accountant in the circumstances would think a divulgence likely to be prejudicial.

Care must be taken, not only in relation to what information is divulged, but also to whom it is divulged. For example, it may be reasonable to share the information with a MLRO, a partner, a trusted colleague or your regulatory body but unreasonable to share it with other staff members or anyone outside the firm. The only real practical guide is common sense.

You will not commit the offence of tipping off if you include in your letter of engagement an explanation of your Reporting duties. The AAT includes such information in its standard letters of engagement.

The second offence in section 342 (falsifying, concealing etc) is phrased in such a way to place a positive obligation on you to preserve and produce documents that are in your influence or control. For example, you cannot ask the office junior to shred relevant documents, or turn a blind eye if he does so. That is, unless you did not know or suspect that they were relevant to an investigation or you were still prepared and able to supply the information in the documents to the investigation. Practically, for this latter defence to be effective, the information contained in the documents would probably have to be preserved and available to the investigation in another form.

You can refuse and should to supply any information or documents that are subject to legal professional privilege. (See Priveleged circumstances and Privileged documents, pages 52 and 60).
Terrorism Act 2000

Summary
The following provisions are intended to disrupt the flow of funds to terrorist causes, whether they come from legitimate sources or from criminal activity. As with POCA, the TA captures all dealings in such funds.

Rule (s.15 - fundraising)
A person commits an offence if he:
• invites another to provide money or other property
• receives money or other property
• makes available money or other property
• and he intends, knows or has reasonable cause to suspect that the money or other property will or may be used for the purposes of terrorism.

Rule (s.16 - use and possession)
A person commits an offence if he uses money or other property for the purposes of terrorism; or possesses money or other property and he intends that it should be used, or has reasonable cause to suspect that it will or may be used for the purposes of terrorism.

Rule (s.17 - funding arrangements)
A person commits an offence if he becomes concerned in an arrangement as a result of which money or other property is made available to another and he knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism.

Rule (s.18 - money laundering)
A person commits an offence if he enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property:
• by concealment
• by removal from the jurisdiction
• by transfer to a nominee
• in any other way.

But it is a defence to s.18 for a person to prove that he did not know and had no reasonable cause to suspect that the arrangement related to terrorist property.

Commentary
The principles set out in the TA are similar to those in POCA. Much commentary relating to POCA offences also applies, with some minor adjustment for different terminology. For example, ‘reasonable cause’ is equivalent to ‘reasonable grounds’. An accountant is most likely to offend against the TA by providing professional services which breach of s.18.

In order to secure a conviction under sections 15 to 17 offence, the authorities would have to prove that an accused knew or had reasonable cause to suspect that the money or property would be used for terrorism purposes. In contrast, s.18 imposes a reverse burden of proof by requiring a person charged to prove that he did not know or have reasonable cause to suspect. Proving a negative is always difficult but
the standard of proof will be the lower standard of ‘balance of probability’. Reasonable CDD, on-going monitoring and related records should provide adequate protection in this regard. Further defences are set out below.

**Defences to sections 15 to 18 TA offences**

**Rule – (*21ZA - arrangements with prior consent)**
A person does not commit an offence under sections 15 to 18 by involvement in a transaction or an arrangement relating to money or other property if, before becoming involved he:
- discloses to SOCA his suspicion or belief that the money or other property is terrorist property and the information on which the suspicion or belief is based
- has SOCA’s consent to becoming involved in the transaction or arrangement.

**Rule (*21ZB – disclosure after entering into arrangement)**
A person does not commit an offence under sections 15 to 18 by involvement in a transaction or an arrangement relating to money or other property if, after becoming involved he discloses to SOCA:
- his suspicion or belief that the money or other property is terrorist property
- the information on which the suspicion or belief is based
- there is a reasonable excuse his failure to make prior disclosure
- the disclosure is made on his own initiative and as soon as reasonably practicable.

This defence does not apply if:
- SOCA forbids the person to continue involvement in the transaction or arrangement to which the disclosure relates
- the person continues that involvement.

**Rule (*s.21ZC – reasonable excuse for failure to disclose)**
It is a defence for a person charged with an offence under sections 15 to 18 to prove that:
- he intended to make a disclosure of the kind mentioned in 21ZA and 21ZB
- there is a reasonable excuse for the person’s failure to do so.


**Duty to report**

**Summary**
The TA imposes a duty equivalent to that in section 330 POCA – a duty to Report persons who you believe or suspect of committing a sections 15-18 offence, if the information on which your belief or suspicion is based came to you in the course of business (except in privileged circumstances). But there is no duty where there are merely reasonable grounds – belief or suspicion must be actual belief or suspicion.

**Rule (s.19)**
A person commits an offence if:
- he believes or suspects that another person has committed an offence under section 15 to 18
- the information on which his belief or suspicion is based came to him in the course of business
- he fails to disclose to SOCA or his MLRO as soon as reasonably practicable:
- his belief or suspicion; and
- the information on which it is based.

It is a defence for a person to prove that he had a reasonable excuse for not making the disclosure.

This rule does not apply where the information came to you in privileged circumstances.

General permission to report
A person may report to SOCA any genuine suspicion or belief in relation to terrorist property with impunity, free from any restriction on the disclosure of information imposed by statute or otherwise.

Tipping off (TA)
The tipping off provisions is identical to those under POCA (as amended). Please see 'Tipping off' in relation to POCA, page 55.

Privileged circumstances summary
It is important to the administration of justice that persons are able to obtain appropriate legal advice and defend themselves in litigation. To this end, they must be allowed to provide their legal advisers with all relevant information without fear of a breach of confidentiality. The definition of legal adviser now specifically includes accountants who give tax advice or act as expert witnesses in actual or contemplated court proceedings.

Rule
A professional legal adviser should not make a Report to a MLRO or SOCA if the information or other matter is communicated to him in privileged circumstances. Privileged circumstances exist where the information comes to a professional adviser:
- by or on behalf of a client seeking or receiving legal advice from the professional adviser
- by a person in connection with actual or contemplated legal proceedings.

But information is not privileged if it is communicated with the intention of furthering a criminal purpose.

Commentary
For the purposes of POCA and TA, a professional legal adviser includes accountants, their colleagues and staff connected with the particular matter, who receive information in privileged circumstances. There are two categories of privileged circumstances – relating to ‘advice’ and ‘litigation’.

Advice privilege applies to accountants who advise clients how to stay within the law, for example, by legitimately paying the minimum amount of tax. Advice intended to enable clients to commit or continue illegal acts, such as tax evasion, is not privileged. It is irrelevant whose intention it is to commit or continue the illegal act, whether that of the accountant, the client or a third party who manipulates an unsuspecting client. Litigation privilege applies to accountants who act as expert witnesses or advises lawyers or litigants in person in respect of actual or contemplated litigation. If you are in any doubt about any aspect of legal professional privilege you should seek expert legal advice.

Privileged documents
For a document to be privileged, it must be brought into existence for privileged purposes. Pre-existing documents are not privileged. Even documents brought into existence for the privileged purposes are not privileged if they form part of a criminal act or form part of communications which take place in order to
obtain advice with a view to committing or continuing a criminal act. If you are in any doubt about any aspect of legal professional privilege you should seek expert legal advice.
The duty of client confidentiality

The professional duty to protect clients’ confidential information is very important but often overlooked or undervalued. POCA, TA and the Regulations (and other statutes) oblige you to disclose information about your clients if particular specified criteria are met. Unless the requisite criteria are met, you must protect your client’s confidentiality and ensure that your staff does likewise.

When you do make a Report under the POCA or TA, such Report is not to be taken to breach any restriction on the disclosure of information, however imposed. Good faith, however, is an essential ingredient to such protection. Reports made in bad faith, without genuine justification, constitute a breach of the subjects’ right to confidentiality and are actionable in the civil courts.
Data Protection Act

A Report under the POCA will not breach the Data Protection Act. If your client asks for information under section 7 of the Data Protection Act, you should consider whether supplying a copy of a Report would constitute tipping off or prejudice an investigation. (NB. you have 40 days to comply with a section 7 request).

Section 29 of the Data Protection Act provides an exemption from the need to provide personal data where disclosure would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. Where disclosure would constitute a “tipping off” offence, the section 29 exemption would apply. Section 29 applies even to internal reports. When information is not disclosed because of the section 29 exemption there is no obligation to tell the client that the information has been withheld.
Letters of engagement

The standard letters of engagement issued by AAT include:

- an explanation of reporting obligations
- an exclusion clause denying liability for loss caused to the client by our members’ compliance with the money laundering and related legislation.

The standard letters of engagement can be obtained from the website www.aat.org.uk
Links

CCAB  www.ccab.org.uk
ICAEW  www.icaew.com  (search ‘money laundering’)
SOCA  www.soca.gov.uk
Treasury  www.hm-treasury.gov.uk/documents/financialsanctions
HMRC  www.hmrc.gov.uk
Office of Public Sector Information  www.opsi.gov.uk  (for copies of legislation)
Joint Money Laundering Steering Group  www.jmlsg.org.uk
Financial Action Task Force  www.oecd.org  (search ‘FATF’)
List of EEA Countries  http://europa.eu.int/comm/external_relations/eea