**ANTI-MONEY LAUNDERING Procedures**

These specimen procedures, which cover a wide range of issues, are basic examples that will require tailoring to specific circumstances. They should be read alongside guidance from regulators and adapted as required. We believe it is in the interests of practitioners to have draft documents on the basis of which, considering the guidance available, their own circumstances, and the relationship and work commitment with clients, they can draft appropriate procedures for their firm.

The money laundering reporting officer (MLRO) isinsert name

[If not combined then record both]

Name of person responsible with compliance with anti-money laundering (AML) regime: insert name

Name of nominated officer: insert name

The alternative MLRO within the firm isinsert name

[If not combined then record both]

Name of alternate person responsible for compliance with AML regime: insert name

Name of alternative nominated officer: insert name

The allocation of duties and responsibilities for these roles is not prescribed in the regulations. However, the allocation of the duties should be clear to the individuals assigned the duties, all relevant employees and the business’s AML supervisory authority. However, the combined roles (or MLRO) should:

* have oversight of, and be involved in, money laundering of terrorist financing (MLTF) risk assessments
* take reasonable steps to access any relevant information about the business
* obtain and use national and international findings to inform their performance of the role
* create and maintain the business’s risk-based approach to prevent MLTF
* support and coordinate management’s focus on MLTF risks in each individual business area; this involves developing and implementing systems, controls, policies and procedures that are appropriate to each business area
* take reasonable steps to ensure the creation and maintenance of MLTF documentation
* develop customer due diligence (CDD) policies and procedures
* ensure the creation of the systems and controls needed to enable staff to make internal suspicious activity reports (SARs) in compliance with the Proceeds of Crime Act 2002 (POCA)
* receive internal SARs and make external SARs to the National Crime Agency (NCA)
* take remedial action where controls are ineffective
* draw attention to the areas in which systems and controls are effective and where improvements could be made
* take reasonable steps to establish and maintain adequate arrangements for awareness and training
* receive the findings of relevant audits and compliance reviews (both internal and external) and communicate these to the board (or equivalent managing body)
* make written reports to the board (or equivalent managing body) at least annually, providing an assessment of the operations and effectiveness of the business’s AML systems and controls
* these reports should be supplemented with regular ad hoc meetings or comprehensive management information to keep senior management engaged with AML compliance and up-to-date with relevant national and international developments in AML
* the board (or equivalent managing body) should be able to demonstrate that it has given proper consideration to the reports and ad hoc briefings provided by the MLRO and then taken appropriate action to remedy any AML deficiencies highlighted.

**Policy and procedure on due diligence**

*Procedure*

Businesses must apply customer due diligence (CDD) principles

1. at the start of a new business relationship
2. at appropriate points during the lifetime of the relationship
3. when an occasional transaction is to be undertaken.

The required components of the CDD principles are:

1. identifying the client and then verifying their identity by obtaining documents or other information from independent and reliable sources
2. identifying beneficial owner(s) so that the ownership and control structures can be understood and the identities of any individuals who are the owners or controllers can be known and, on a risk-sensitive basis, reasonable measures should be taken to verify their identity
3. gathering information on the intended purpose and nature of the business relationship.

The business adopts a risk-based approach when deciding the degree of CDD to apply. Risks are assessed at the outset of a business relationship and updated.

**Enhanced due diligence (EDD)**

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

* seeking additional independent, reliable sources to verify information (including identity information provided to the business)
* taking additional measures to understand the background, ownership and financial situation of the client, and other parties relevant to the engagement
* taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship
* increasing the monitoring of the business relationship, including greater scrutiny of transactions
* examining the background and purpose of the engagement
* increasing the degree and nature of monitoring of the business relationship in which the transaction is made to determine whether that transaction or that relationship appear to be suspicious.

**Politically exposed person (PEP)**

In these higher-risk situations the business applies more stringent EDD measures. This represents part of the risk-based approach the business takes to MLTF compliance.

The business treats individuals as PEPs for at least 12 months after they cease to hold a prominent public function. However, family members and known close associates of PEPs are treated as ordinary clients (subject only to CDD obligations) from the time that the PEP ceases to discharge a prominent public function.

The business applies EDD measures to PEPs for more than 12 months after they cease to hold a prominent public function when the business has determined that they present a higher risk of MLTF.

If the business intends to enter into, or continue, a business relationship with a PEP it will carry out EDD, which includes:

* senior management approval for the relationship
* adequate measures to establish sources of wealth and fund
* enhanced monitoring of the ongoing relationship

The nature and extent of EDD measures will vary depending on the levels of MLTF risk associated with individual PEPs.

**Financial sanctions and other prohibited relationships**

The business will comply with any sanctions, embargos or restrictions in respect of any person or state to which the UN, UK or EU has decided to apply such measures.

<https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases>

If the business breaches any of these sanctions, embargos or restrictions it will report these to HM Treasury’s Office of Financial Sanctions Implementation (OFSI) in addition to making an external SAR to the NCA, if appropriate.

The firm complies with guidance issued by OFSI on ‘reporting information to OFSI – what to do’, which is relevant for external accountants, auditors and tax advisers.

<https://www.gov.uk/guidance/suspected-breach-of-financial-sanctions-what-to-do>

**When delays occur**

The business recognises, in accordance with the 2017 Regulations, that CDD will sometimes need to be completed while the business relationship is established, rather than before, but this will only be permissible when there is little risk of MLTF.

To ensure the reasons are valid, and should not give rise to suspicions of MLTF, such extensions will be considered individually and agreed by the MLRO.

If a prospective or existing client refuses to provide CDD information, the work will not proceed and any existing relationship with the client will be terminated. However, in some circumstances, such as an insolvency practitioner dealing with insolvencies etc, an appropriate risk-based approach will be adopted where the client’s management are not cooperative in providing CDD information.

Consideration will also be given to whether or not an SAR should be submitted to the NCA under POCA or the Terrorism Act 2000.

**Policy and procedure on assessing risk**

*Procedure*

The business will analyse the MLTF risks, and assess their nature and severity in order to produce a risk profile. The business will then act to mitigate those risks in proportion to the severity of the threats they pose.

The business designs and implements appropriate procedures to manage risks it identifies.

The risk analysis is conducted by the MLRO and approved by senior management. This includes formal ratification of the outcomes of the risk analysis, including the resulting policies and procedures.

The risk analysis is updated regularly by periodic reviews, the frequency of which depends on the MLTF risks faced and the stability or otherwise of the business environment. Whenever the business sees that events have affected MLTF risks, the risk analysis is updated by the event-driven review that may in turn require AML policies, controls and procedures to be amended (such as training programmes for relevant employees).

The business looks at its clients, markets and itself when designing an analysis process.

Risks are grouped into categories that include ‘client’, ‘services’ and ‘geographic location’.

When looking at overall risk, the business considers all the individual risk categories. For example, a particular industry and a particular location may each be considered to pose a moderate risk, but when they are considered together by a particular client or transaction then the combined risk may be considered high.

The business assesses the different services being offered and provided to clients when determining the risk profile of the business. The different services being provided give rise to different risks. The risk analysis allows resources to be targeted, and procedures tailored, to address those differences.

Services such as bookkeeping, preparation of accounts and personal tax returns are usually considered by the business to have a low risk profile, whereas insolvency, bankruptcy, recovery and audit are usually considered to have a higher risk.

The business has a risk-based approach to undertaking work in a new type of service or product or a new region. For example, if the business mostly deals with clients based in the UK, a potential client based outside of the UK may be treated initially as higher risk.

The business ensures that it has controls in place to address the risk arising from a new client before establishing the client relationship. The risk profile of the business shows where particular risks are likely to arise and where certain procedures will be needed to tackle them.

The business has client risk categories of low, normal and high. The business undertakes monitoring of the client relationship on a risk-based approach, with levels of monitoring varying depending on the MLTF risk associated with individual clients.

The client’s risk profile is determined on various factors, including:

* legal form of the client (eg individual person, company, plc)
* country in which the client is established or incorporated
* countries or regions in which the client carries on business
* industrial sectors in which the client operates
* nature of services or products being provided to the client
* channels through which the services/transactions are being delivered.

The business will assess the following risk categories:

* client risk
* service risk
* geographic risk
* sector risk
* delivery channel risk

**Client risk**

Identify the type of business each client is involved in and assess the risk of money laundering associated with each.

Identify any mitigating actions the business can take to reduce the risk, which may include carrying out EDD, preparing client due diligence more often, such as annually or biannually, hot file reviews on a frequent basis and staff training in specialised areas where client risks are high.

**Service risk**

The business identifies all the services it supplies and offers to clients and potential clients, and then assesses the risk of MLTF associated with each of these services.

The business identifies any mitigating actions in place or planned to reduce the risk. These may include internal or external review of the report being issued to a client, ensuring staff are properly trained and up-to-date (particularly in those areas with a higher risk) and considering ceasing to provide those services if judged to be too high a risk.

**Geographic risk**

The business identifies the countries each client is involved with. This would include:

* countries where the client has offices
* countries it has sites such as storage, factories etc
* countries from which funding is supplied
* countries where goods and services are purchased
* countries where sales are made.

The business assesses the risk of MLTF associated with each of these countries.

The business identifies any mitigating actions to reduce the risk. These may include internal or external review of specific overseas areas that are seen as particularly high risk, and ensuring that staff are familiar with any practices and procedures that may be different in the overseas areas relating to specific clients.

**Sector risk**

The business identifies the sectors in which each client is involved in.

The business assesses the risk of MLTF associated with each of these sectors.

The business identifies any mitigating actions to reduce the risk. This may include carrying out additional work in relation to high-risk sectors such as a client that makes a high proportion of sales in cash or deals in high-value moveable goods (such as works of art), and limiting availability of the business’s client money bank account for clients that appear to have a higher risk.

**Delivery channel risk**

The business identifies all the methods of delivering services to its clients.

The business assesses the risk of MLTF associated with each of these delivery channels.

The business identifies any mitigating actions to reduce risk. This may include arranging more face-to-face contact with clients, particularly during the engagement process, and providing the services directly to the client instead of via an intermediary.

**Policy and procedure on reporting**

*Procedure*

All ‘relevant employees’ should report their knowledge or suspicions of MLTF to the MLRO. This would normally be on the firms’ internal reporting form. If the form is not available then a report can be made by other means to prevent delay in making the report.

The MLRO will consider the internal report and if the MLRO also suspects MLTF, then the MLRO will submit an external SAR to the NCA.

The MLRO will inform the partner in charge of the assignment of any action that they need to take (for example, ceasing work until consent has been obtained).

If the MLRO is not available then the alternate will take over this role in their absence.

In exceptional circumstances the report can be made by the relevant employee to the NCA.

The key elements required for an SAR are ‘suspicion’, ‘crime’ and ‘proceeds’.

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

**Proceeds**

Relevant employees should not commit the offence of ‘tipping off’ This offence is committed when a relevant employee discloses that:

* an SAR has been made and this disclosure is likely to prejudice any subsequent investigation, or
* an investigation into allegations of MLTF is under way (or being contemplated) and this disclosure is likely to prejudice that investigation.

After making an SAR the MLRO will consider what information, if any, in the SAR can be disclosed to the client without ‘tipping off’ and these deliberations and the conclusions reached will be kept by the business.

Continuing work for the client may require that matters relating to the suspicions be discussed with the client’s senior management. This may be of particular relevance in audit relationships.

Relevant employees who have concerns about possible reportable offences can discuss their concerns with suitable employees/partners in the business to help them decide if an SAR should be made.

Investigations into suspected MLTF should not be conducted unless to do so would be within the scope of the engagement.

When more than one relevant employee is aware of the same reportable matter, a single SAR can be submitted to the MLRO, but it should contain the names of all those making the SAR.

It is the MLRO’s responsibility to decide whether the information reported internally needs to be reported to the NCA. If an SAR is made, the MLRO will also decide:

* whether consent is required from law enforcement for the engagement or any aspect of it to continue
* how client business should be conducted while a consent decision is awaited.

The MLRO will consider making reasonable enquires of other relevant employees and systems within the business, before making an external SAR.

If an SAR is to be made to the NCA, the MLRO (or deputy) will make the report using the NCA SAR Online System.

The SAR should contain the following essential information:

* name of reporter
* date of report
* name of the suspect or information which may identify them
* details of who else is involved, associated, and how
* facts regarding what is suspected and why
* relevant NCA glossary code (if applicable)
* whereabouts of any criminal property, or information that may help locate it
* actions that the business is taking that require consent.

The MLRO should keep records relating to SARs that include the following:

* all internal SARs made
* how the MLRO handled matters, including any requests for further information
* assessments of the information provided, along with any subsequent decisions about whether or not to await developments or seek extra information
* rationale for deciding whether or not to make an external SAR
* any advice given to engagement teams about continued working and any consent requests made.

The MLRO (and in exceptional circumstances the relevant employee making an internal SAR) will consider the ‘privileged circumstances’ exemption when making an SAR. As these matters can be complex, the MLRO will also consider if professional legal advice is required before making this decision.

**Consent**

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

* consent has been received or
* the notice period has expired or
* after consent was been refused during the notice period, the moratorium period has expired.

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

If consent is refused during the notice period, a further 31 days must pass, from the day of refusal, before the activity can continue. This is called the moratorium period.

The business will usually take legal advice before continuing the activity after the moratorium period.

After making an SAR report, the business will consider whether the suspicion is such that for professional or commercial reasons it no longer wishes to act for the client.

In most cases the business policy is not to share this information regarding suspicious activity with other advisers.

The business has other obligations, such as the reporting obligations as auditors or the reporting of misconduct by fellow members of a professional body. In these cases the offence of tipping off must be considered and avoided.

**Policy and procedure on record keeping (client due diligence and money laundering issues only)**

*Procedure*

The CDD form and consideration of money laundering issues documentation will be completed for all new clients and updated on at least an annual basis and when a significant transaction or change takes place.

When the original document was seen by a relevant employee, that person will endorse the copy to that effect, including the date on which it was seen.

When the copy originates from outside the business, the standing of the person who certified it should be considered and relevant employees should be aware of the risks associated with certified copies.

Where a document is not an original but could be mistaken for one, it is annotated to that effect. Such documents should carry an indication of the source and when they were obtained or downloaded.

The business will keep the AML documents for at least the period specified below.

The AML documents are:

* documents and information obtained to satisfy the CDD requirements
* sufficient supporting records in respect of a transaction that is the subject of CDD measures or ongoing monitoring to enable the transaction to be reconstructed.

The period is five years from

* the date the transaction is complete, for records relating to an occasional transaction
* the date the business relationship has come to an end for records relating to:

(i) any transaction which occurs as part of a business relationship, or

(ii) CDD measures taken in connection with that relationship.

The business will delete any personal data from the records if the documents are retained after the minimum retention periods referred to above.

When we cease to act for a client, this information will be archived in insert location with a date logged. It will be passed for confidential destruction after five years.

**Policy and procedure on third-party reliance**

*Procedure*

If the business relies on a third party to complete all or part of the CDD it will still carry out a risk assessment and perform ongoing monitoring.

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

The business will ensure that appropriate client identification steps are taken to comply with the requirements in the *ACCA Rulebook*, Section B2, which relates to AML.

The business undertakes verification procedures using a risk-sensitive basis. Appendix C of the *CCAB Anti-Money Laundering Guidance for the Accountancy Sector* contains a non-exhaustive list of documents that can be used for verification purposes.

Before using any electronic service the business questions whether the information is reliable, comprehensive and accurate. It considers the following:

* Does the system draw on multiple sources? A system that combines negative and positive data sources is generally more robust than a single-source system.
* Are the sources checked and reviewed regularly?
* Are there control mechanisms to ensure data quality and reliability?
* Is the information accessible? It should be possible to either download and store search results in electronic form, or print a hard copy that contains all the details required.
* Does the system provide adequate evidence that the client is who they claim to be?

**Policy and procedure on internal control**

*Procedure*

As detailed below, the firm will appoint an MLRO and where appropriate an alternative.

The MLRO will be given authority to implement the necessary changes in the firm’s procedures to ensure compliance.

All partners and relevant employees will be required to accept the changes to the office rules and partnership agreement that confer the necessary authority on the MLRO.

All partners and relevant employees will be required to make the necessary internal reports using the standard form when they have a suspicion in respect of a client.

All partners and relevant employees will be required to complete the fit and proper, confirmation of independence and annual declaration on an annual basis.

The firm will retain evidence of all partner and relevant employees screening relating to skills, knowledge, expertise, conduct and integrity both before, and during the course of, their appointment. This includes knowledge of the law relating to money laundering, terrorist financing and data protection as well as an assessment of conduct and integrity as part of the firm’s ethics training.

**Policy and procedure on compliance management**

*Procedure*

The MLRO will undertake a compliance review on an insert period basis. This review will include but is not limited to:

1. consideration of the annual declaration of fit and proper status, etc completed by all partners and staff
2. a review of a sample of files to ensure that the CDD pack has been completed and/or updated as necessary
3. consideration of the adequacy of the training given to all staff and partners
4. consideration as to whether staff working in high-risk business areas require specialised training or more frequent training.

**Policy and procedure on communication**

*Procedure*

All partners and relevant employees will be required to:

1. undertake training for any new regulations; these include the law relating to money laundering, terrorist financing and data protection
2. undertake training and assessment to ensure that they:

• are aware of their legal and regulatory duties

• understand how to put those requirements into practice in their roles, including training on ethics

• are continuously updated about changes in

(a) the business’s AML policies, systems and controls
(b) the money laundering risks faced

1. consider whether they need to undertake further training on an annual basis during the appraisal process
2. confirm their understanding of and compliance with the regulations and the firm’s policies and procedures as part of their annual declaration.

**Policy and procedure on training and awareness**

*Procedure*

The MLRO is responsible for ensuring that all relevant employees (and others if appropriate) undertake the AML training at the appropriate time.

The training includes the following:

* an explanation of the law within the context of the business’s own commercial activities
* the ‘red flags’ of which the relevant employees should be aware when conducting business, which would cover all aspects of the MLTF procedures, including CDD and SARs
* how to deal with transactions that might be related to MLTF (including how to use internal reporting systems), the business’s expectations of confidentiality and how to avoid tipping off
* the relevant data protection requirements.

The training programmes are tailored to each business area and cover the business’s procedures so that relevant employees understand the MLTF risks posed by the specific services they provide and types of client they deal with, and so are able to appreciate the approach they should be taking for each and every client they are involved with.

The business aims to create an AML culture in which relevant employees are always alert to the risks of MLTF and habitually adopt a risk-based approach to CCD and the work they undertake.

The business keeps records showing who has received training, the training received and when training took place. These records are used to decide when additional training is required, for example when the role of a relevant employee changes or the MLTF risk of a specific business area changes.

The relevant employees will be able to determine when to make an internal SAR to the MLRO and what information should be included in the report.

New relevant employees are provided with AML training as soon as possible after joining the business.

**GUIDANCE**

**Due diligence**

*Simplified due diligence (SDD)*

SDD is applied when a client is low risk, in accordance with the business’s risk assessment criteria. On-going monitoring for unusual or suspicious transactions is still required. When a client or potential client has been subjected to SDD, and a suspicion of MLTF arises then the SDD provisions are set aside and the appropriate due diligence procedures applied instead.

**Enhanced due diligence (EDD)**

Regulation 33 of the 2017 Regulations state that EDD must be applied in the following situations:

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

The business’s internal procedures clearly set out what constitutes reasonable grounds for a client to qualify for EDD and take into account at least the high-risk factors in Appendix E of the CCAB’s AML guidance issued in March 2018.

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

* seeking additional independent, reliable sources to verify information (including identity information provided to the business)
* taking additional measures to understand the background, ownership and financial situation of the client, and other parties relevant to the engagement
* taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship
* increasing the monitoring of the business relationship, including greater scrutiny of transactions
* examining the background and purpose of the engagement
* increasing the degree and nature of monitoring of the business relationship in which the transaction is made to determine whether that transaction or that relationship appear to be suspicious.

**Politically exposed person (PEP)**

PEPs, certain family members and known associates undergo EDD. The EED measures vary depending on the extent of any heightened MLTF risk associated with individual PEPs. PEPs are assessed on a case-by-case basis and appropriate EDD measures are applied, based on our assessment of the associated MLTF risks.

The business has in place appropriate risk management systems and procedures to determine whether potential clients or existing clients (or their beneficial owners) are PEPs, or family members/known close associates of a PEP.

The business considers factors including the country that has entrusted a PEP with a prominent public function when determining the level of MLTF risk associated with an individual PEP.

An individual identified as a PEP solely because of their public function in the UK may be categorised as a low-risk PEP if the business is not aware of any factors that would place the individual in a higher risk category. In these lower risk situations the business applies less onerous EDD procedures (for example, making fewer enquiries of a PEP’s family members or known close associates; and taking less intrusive and less exhaustive steps to establish the sources of wealth/funds of PEPs).

Regulation 18 of the 2017 Regulations and the risk factors guidance produced by the European supervisory authorities set out factors that might point to potential higher risk. Such factors might include:

* known involvement in publicised scandals
* undeclared business interests
* the acceptance of inducements to influence policy.

The Financial Conduct Authority (FCA) has published guidance on how relevant businesses should identify and treat PEPs:

<https://www.fca.org.uk/publications/finalised-guidance/fg17-6-treatment-politically-exposed-persons-peps-money-laundering>

The business will mitigate and manage any identified MLTF risks (such as those posed by PEPs) and will refuse business relationships only when such risk assessments indicate that they cannot effectively mitigate and manage these risks.

**When delays occur**

In some situations it may be acceptable to carry out CDD while commencing work because it is urgent. Such situations could include:

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

**Assessing risk**

*Client risk*

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

The client’s risk profile will impact on the checks performed on other associated parties, such as the beneficial owners of the client.

Indications of high risk would include undue client secrecy or unnecessarily complex ownership structures, as such factors are sometimes attractive to people involved in MLTF.

In cases where an individual client or a beneficial owner or a manager of a client is identified as a politically exposed person may be an indication of high risk.

Client risk may be assessed by considering the industry in which the client operates, the size of the client, the business structure (eg limited company, public limited company, listed, LLP etc), the directors and shareholders.

*Service risk*

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

The business assesses the products and services to be provided to its clients and carries out the appropriate checks on the client.

Whenever the business begins to offer a product or service that is significantly different from its existing range of products or services, it assesses the associated MLTF risks and takes the appropriate steps relating to any new or increased risks.

*Geographic risk*

Geographic risk is the increased level of risk that a country or region poses in respect of MLTF.

The business considers the perceived level of corruption, criminal activities and the effectiveness of MLTF controls in the country or region concerned.

The business considers to level of business the client has with a particular country or region. A client with limited exposure to a high-risk region may have a lower level of MLTF risk than a client with extensive operations in that region.

The business makes use of publicly available information when accessing geographic risk such as Transparency International (<https://www.transparency.org/>) and the Financial Action Task Force (<http://www.fatf-gafi.org/home/>).

*Sector risk*

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

The business considers the sectors in which clients have significant operations and takes this into account when determining a client’s risk profile. When considering what constitutes a high-risk sector, the business takes into account the findings of the most recent UK National Risk Assessment of Money Laundering and Terrorist Financing published by HM Treasury and the Home Office. The October 2017 publication can be found at:

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf>

*Delivery channel risk*

Delivery channel risk is the risk associated with the contact the business has with the client and the methods by which information is provided by and to the client.

Some delivery channels can make it more difficult to determine the identity and credibility of a client, both at the start of a business relationship and during its course. For example, delivery channel risk could be increased where services/products are provided to clients who have not met face to face, or where a business relationship with a client is conducted through an intermediary.

The business considers the risks posed by each delivery channel used when determining the risk profile of a client and whether an increased level of CCD needs to be performed.

**Reporting**

The key elements required for an SAR are ‘suspicion’, ‘crime’ and ‘proceeds’.

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

**Suspicion**

Suspicion is:

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

Suspicion is *not*:

* a mere idle wondering
* a vague feeling of unease.

An SAR must be made where there is knowledge or suspicion of money laundering, but there is no requirement to make speculative SARs.

Relevant employees should make enquiries that would reasonably be expected of someone with their qualifications, experience and expertise. These enquiries should fall within the normal scope of the engagement or business relationship.

**Crime**

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

UK law defines ‘money laundering’ as any criminal conduct that results in criminal property.

If a client is known or believed to have acted in error, they should have the situation explained to them. If they promptly bring their conduct within the law, they may avoid committing a money laundering offence. Where there is uncertainty (eg some legal issues lie outside the knowledge of the practitioner), the client should be advised to seek specialist advice.

In the UK the ‘money laundering offences’ are described in the Proceeds of Crime Act 2002 sections 327 to 333E. Individuals are not required to become experts in the wide range of criminal offences that lead to money laundering, but they are expected to recognise any that fall within the scope of their work.

**Proceeds**

Examples of criminal proceeds include:

* tax evasion that results in money being retained by an entity
* criminal property being used to acquire other assets, with those assets then becoming criminal property.

There is no de minimis (or threshold) value.

When deciding whether or not to make an external SAR, the MLRO will consider the following:

* Do I know or suspect (or have reasonable grounds for either) that someone is engaged in MLTF?
* Do I think that someone involved in the activity, or in possession of the proceeds of that activity, knew or suspected that it was criminal?
* From the contents of the internal SAR, can I identify the suspect or the whereabouts of any laundered property?
* Is an application for consent required?
* Do I believe, or is it reasonable for me to believe, that the contents of the internal SAR will, or may, help identify the suspect or the whereabouts of any laundered property?
* Can I provide the information essential to an external SAR without disclosing information acquired in privileged circumstances (if any)?

The following recommendations also apply to SARs:

* They do not include confidential information not required by POCA.
* The name of the business, individual or MLRO submitting the SAR is only included once, in the source ID field and nowhere else.
* Do not include the names of the relevant employees who made internal SARs.
* Include other parties as ‘subjects’ only when the information is necessary for an understanding of the external SAR or to meet required disclosure standards.
* Highlight clearly any particular concerns the reporter might have about safety.

A correctly made external SAR provides full immunity from action for any form of breach of confidentiality.

**Consent**

When making an SAR to the NCA the MLRO can apply for consent from the NCA. This in effect is asking the NCA if the proposed action can be taken by the business. The NCA can only give consent to activities that would otherwise be offences under Sections 327, 328 or 329 of POCA. Consent cannot be given for any other possible offences.

Under the Companies Act 2006 the business may be required to file an auditors’ resignation statement at Companies House. There is no legal mechanism for obtaining NCA clearance or consent for these statements. The business will consider these statements carefully to make sure that statutory and professional duties are met without including information that could constitute tipping off.

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

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

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

* reporting to the professional body if it is an anti-money laundering supervisory authority (ACCA is such a professional body)
* reporting a matter of material significance to the UK charity regulator (Charities Commission for England and Wales, Office of the Scottish Charity Regulator and Charity Commission for Northern Ireland).

**Third-party reliance**

If the business (A) provides services to another accountancy practice (B) relating to a client (C) of B, then A will consider whether its client is either B or C or both B and C. The CDD procedures will need to be carried out on the client(s). If C is considered to be a client of A, then A may consider relying on information provided by B when determining what CDD is required.

August 2018