Anti-money laundering policies, controls
and procedures template

The [Money Laundering Regulations (MLR)](https://www.legislation.gov.uk/uksi/2017/692/contents) require all businesses providing accountancy and/or trust or company services to have documented policies, controls and procedures in place to mitigate and manage effectively the risks of money laundering, terrorist financing, and proliferation financing.

These policies, controls and procedures must be documented and regularly reviewed, and must include:

* risk management practices
* internal controls
* customer due diligence
* reliance and record keeping
* the monitoring and management of compliance with, and the internal communication of, such policies, controls and procedures.

It is important that you assess and understand the risks of your firm being used for money laundering and make sure that the risk of money laundering is considered in the day-to-day running of your business.

The nature and extent of AML policies, controls and procedures depend on the nature, scale, complexity and diversity of the business; the geographical spread of client operations, including any local AML regimes that apply; and the extent to which operations are linked to other organisations.

This document is designed to help you meet this requirement but is for general guidance only and should be adapted to suit the needs of your practice. It is not intended to supply legal, regulatory, or professional advice. Compliance with the MLR in force is the legal duty of the licensed member and supervision by AAT does not transfer any part of those responsibilities to AAT. Please refer to the [Anti-Money Laundering and Counter-Terrorist Financing Guidance for the Accountancy Sector (AMLGAS)](https://www.ccab.org.uk/anti-money-laundering-and-counter-terrorist-financing-guidance-for-the-accountancy-sector-2022/) for further guidance on AML requirements.

**Requirements for sole practitioners**

Sole practitioners are still required to have the same written policies, procedures and controls in place, but due to the size and nature of the business, a sole practitioner who has no relevant employees need not:

* appoint a board member or member of senior management to be responsible for the business’ compliance with the UK anti-money laundering regime, as the sole practitioner will be held responsible
* appoint a nominated officer because the sole practitioner will be responsible for submitting external reports to the National Crime Agency (NCA), the Office of Financial Sanctions Implementation (OFSI) and Companies House
* establish an independent audit function for AML policies, controls and procedures.

|  |  |
| --- | --- |
| Document properties |  |
| Version | 1.0 |
| Date of issue | 02 September 2024 |

|  |
| --- |
| Change control |
| Version no. | Page | Changes made | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Please remove these cover pages and apply your own branding to the document before use.

**[Insert firm logo]**

**Name of firm: [Insert name of firm]**

**[Insert date document came into effect]**

**Introduction**

The Money Laundering Regulations in force require supervised firms to “establish and maintain policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified in any risk assessment undertaken by the relevant person”.

[Name of firm] is committed to adherence to the UK legislation enacted to combat money laundering and preventing criminals from being able to use this firm to help them launder money, or to finance terrorism. References to money laundering (ML), terrorist financing (TF), and proliferation financing (PF) in this document should be taken to mean ML/TF/PF.

**Client due diligence and Enhanced due diligence**

It is our policy to undertake client due diligence (CDD) and ensure that evidence of identity is obtained and retained as appropriate to that risk assessment for all clients. Enhanced due diligence (EDD) shall be performed where considered necessary. In practice, we obtain a client’s:

* name
* photograph on an official document which confirms their identity (passport/driving licence)
* electronic ID
* residential address and date of birth

The firm will document its CDD using [Insert own procedures on how the firm records its CDD. For example, using AAT’s client onboarding checklist].

All risks, including those not within a category, will be assessed in isolation and also when grouped together. These risks will be used to assess the customer due diligence process.

This evidence will be obtained before work for the client is commenced, and when periodic reviews are undertaken (if more evidence is required then, and when changes occur during the relationship with the client). In all cases where the evidence is not available, the matter will be referred to the Money Laundering Reporting Officer (MLRO).

[Please indicate your procedures on performing CDD. Are you using an electronic CDD identity verification system? Is it only the directors/partners/sole practitioner will deal with CDD/EDD or whether staff deal with this? Are there any authorisation rules in place?

The EDD measures when dealing with a politically exposed person (PEP) are making sure that only senior management approves a new business relationship; taking adequate measures to establish where the person’s wealth and the funds involved in the business relationship come from and carrying out stricter ongoing monitoring of the business relationship.

[Name of firm] is aware of the need to perform additional CDD/EDD monitoring measures, where appropriate, to prevent the use of products and transactions which might favour anonymity from being used to facilitate money laundering, terrorist financing, or proliferation financing. Further scrutiny will take place in any case where there are reasonable grounds, such as:

* there is a high risk of ML/TF/PF or in any other case which by its nature can present a higher risk of ML/TF/PF
* where either the client or other parties to the transaction or business relationship are established as being connected to a high-risk third country
* where either the client or other parties to the transaction or business relationship are established as being subject to financial or trade sanctions
* where the client or a beneficial owner of a client is a PEP, or a family member or known close associate of a PEP
* in any case where a client has provided false or stolen identification documentation or information on establishing a business relationship
* in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions which have no apparent economic or legal purpose.

[Include what EDD measures, as detailed in the Money Laundering Regulations, you have in place].

In all cases where the evidence is not available, the matter will be referred to the Money Laundering Reporting Officer (MLRO).

[If applicable, please insert your policy relating to your reliance on information obtained from appropriate third parties to complete all or part of the due diligence process. Include any details of the written agreement in place.]

**Risk management**

It is our policy to undertake a firm-wide risk assessment. The firm will assess the ML/TF/PF risks it faces and make proportionate responses to them. Risks are grouped into categories:

* Client risk
* Service risk
* Geographic risk
* Delivery channel risk
* Industry risk

The firm will document this risk assessment [Insert own procedures on how the firm records this assessment. For example, using AAT’s firm-wide risk assessment template].

To focus resources on the areas of greatest risk, [name of firm] uses a risk-based approach. A risk assessment is conducted at least annually, but with new and changing risks considered as and when they are identified.

[Insert who is the board member or member of senior management responsible for compliance to identify the risks and then develop risk-based procedures for taking on new clients.]

**Ongoing monitoring**

Client due diligence, periodic reviews and risk assessments are conducted on an ongoing basis and any additional information identified should be dealt with and further information obtained from clients where necessary. [Name of firm] considers the following red flags when dealing with both new and existing clients and uses them as indicators for our ongoing monitoring and when to submit a suspicious activity report:

* whether clients are overly secretive or evasive
* if the amount or source of funds seems unusual
* if there are odd discrepancies in client transactions or business activities
* if client activities involve complex business structures that make it unclear who is conducting a transaction or purchase
* the client has taken steps to hide their identity, or is the beneficial owner is difficult to identify
* where information or documents being withheld by the client or their representative, or they appear to be falsified
* high-risk geographical area
* financial or trade sanctions.

The firm will document its ongoing monitoring [Insert own procedures on how the firm records its ongoing CDD, risk assessments, and compliance monitoring. For example, using AAT’s Client monitoring review checklist and AML annual compliance review checklist.]

**Reporting**

**Suspicious activity reports**

It is a requirement that where [name of firm] knows or suspects (or has reasonable grounds for knowing or suspecting) that a person is engaged in ML/TF/PF as a result of information received in the course of the business or otherwise through carrying on that business then they must comply with:

*Part 3 of the Terrorism Act 2000;*

*Part 7 of the Proceeds of Crime Act 2002; and make a Suspicious Activity Report*.

All staff must report every instance where they have knowledge or suspicion of ML/TF/PF to the MLRO as soon as reasonably practical. This should be done by using the Internal Money Laundering Report form available to all staff [insert where document saved and details of where to send].

It is our policy to report all suspicions identified to the National Crime Agency (NCA) where required using the SAR online reporting service.

**Breaches of financial sanctions**

It is a requirement that where [name of firm] knows or suspects (or has reasonable grounds for knowing or suspecting) that a person is a designated person or has breached a financial sanction, they must inform OFSI as soon as practicable.

All staff must report every instance where they have knowledge or suspicion that a person is a designated person or has breached a financial sanction to the MLRO as soon as reasonably practical. This should be done by using the Internal Money Laundering Report form available to all staff [insert where document saved and details of where to send].

It is our policy to report all suspicions identified to OFSI where required using the OFSI Compliance reporting form.

Information about the approach OFSI takes to financial sanctions can be found [here](https://www.gov.uk/government/publications/financial-sanctions-faqs).

**Discrepancies in people with significant control (PSC) register**

It is a requirement that where [name of firm] identifies a reportable discrepancy between the information they hold about a PSC and information held on the PSC register, they must tell Companies House as soon as practicable.

All staff must report every instance where they identify a discrepancy between the information the firm holds about a PSC and information held on the PSC register to the MLRO as soon as reasonably practical. This should be done by using the Internal Money Laundering Report form available to all staff [insert where document saved and details of where to send].

It is our policy to tell Companies House about reportable discrepancies where required using Companies House online service.

Information about the types of discrepancies that must be reported and the definition of a PSC can be found [here](https://www.gov.uk/guidance/report-a-discrepancy-about-a-beneficial-owner-on-the-psc-register-by-an-obliged-entity).

**Record keeping**

It is our policy to maintain records of client identification and considerations of money laundering issues securely, for the entire period that we act for the client and for five years after we cease to act in accordance with the regulations.

If we are required to retain them under statutory obligation, or to retain them for legal proceedings, or by client consent, the records will be retained for not more than 10 years after we cease to act.

Clients are made aware of the data that will be collected about them, why the data is being collected and record retention through the engagement letter in place between the firm and that client and/or our privacy notice.

**Internal controls**

It is our policy to facilitate adequate internal control to allow for compliance with the regulations and other appropriate legislation.

[Insert name of appointed Director/Beneficial Owner] is responsible for [name of firm] compliance with the MLR and application of this policy and associated procedures. The appointed Nominated Officer/MLRO is [insert name] and employees have been made aware of how to report any suspicious activity to them. Any changes to this role, [name of firm] will notify our supervisor within 14 days of the appointment.

All information and guidance concerning AML compliance is communicated to all staff by way of [insert method. For example, staff briefings, email, intranet].

All staff are required to acknowledge receipt of the policies and procedures and confirm, in writing, they:

* Have read and understood the firm’s documented money laundering policies and procedures.
* Will fully comply with these policies and procedures.
* Have understood the obligation on them to report any knowledge or suspicion of ML/TF/PF to the firm’s MLRO.
* Understand what constitutes “tipping off” or prejudicing an investigation.

[Please insert details of how this declaration is captured and stored].

[Name of firm] will carry out screening of relevant employees appointed, both before the appointment is made and during the course of the appointment. This assessment is carried out [insert details of how and when].

**[OR IF A SOLE TRADER WITH NO STAFF]**

This practice is owned by and run by one principal who controls all aspects of the work undertaken. There are no staff members or sub-contractors and therefore no one else who I need to communicate with in relation to control of AML risk.

**Compliance review**

It is our policy to undertake a regular compliance review to ensure that the requirements of the regulations are being followed. A record of the review and actions identified is documented and maintained on file.

[Please include arrangements of who is responsible for carrying the review, when it will be done and how this will be recorded. For example, AAT’s Anti-money laundering annual compliance review checklist].

**Staff training and awareness**

It is the policy of [Name of firm] that all relevant principals and relevant employees (including all agents, such as subcontractors) who are working in a similar manner to staff are made aware of the MLR (and other relevant legislation) and are trained regularly on client due diligence and how to recognise and deal with transactions that may be related to ML/TF/PF, as well as to identify and report anything that gives grounds for suspicion. A written record of the training delivered is retained.

[Please include own arrangements of training undertaken, how often it will be done and how this will be recorded].

**[OR IF A SOLE TRADER WITH NO STAFF]**

I am aware of the requirements of the MLR and will undertake regular training to recognise and deal with transactions that may be related to ML/TF, as well as to identify and report anything that gives grounds for suspicion. I shall retain a written record of the training delivered is maintained.