**What Xama aims to do**

Xama Hub aims to give our clients one software platform to manage their entire AML process, from managing which clients are up for review, running the required checks, storing information obtained from external sources and recording risk assessments for clients.

The platform is supported by a framework for policy & procedures (this document) which each business should adapt for their needs.

**Guidance on how to use this document.**

The purpose of this section is to explain to the user how to use the policies & procedures below in conjunction with our software. This section (page 1) does not form part of the policies and procedure documents for your company, so don’t publish this page to all staff.

It is important to note that these documents set a framework for the MLRO (Money Laundering Reporting Officer) to set up your own policy & procedures for your business. See appendix below as reference to relevant guidelines. This area is ever evolving so requires periodic review and adapting by each MLRO.

The guidance in this document and the Xama Hub software platform, including the predefined risk assessment templates, should be seen as a framework for each MLRO to amend according to their understanding and interpretation of the guidelines and specifically tailored for their own business. Businesses could use different risk assessment / KYC templates and upload / link that to each client (amend guidance below if that is the case).

**Training**

We offer training sessions aimed at general areas which all staff should be aware of and more specific sessions for the admin team on how to get started, interpret results and use of the system. Refer to the training menu in the software for more information.

**Adopting and adapting these framework documents for your business**

**Configure for your business:**

1. Complete and adapt the policies and procedures below to apply to your specific business and processes taking into consideration the guidelines from your regulatory body.

Specifically tailor the sections on simple due diligence applied to low risk clients and on enhanced due diligence.

Items marked in blue\* are specifically for the MLRO to complete as policy options.  
Items marked in green\*\* are examples to be deleted and completed as applicable.

1. Amend the risk assessment templates in the software to fit your client base and policies by editing, adding or deleting questions.

It is important that the MLRO periodically reviews and signs off the Policies and Procedures. Xama Technologies and the resources we provide (software and otherwise) does not constitute formal advice or give any guarantees on compliance.

**Table of contents**

[1 Overview 3](#_Toc128660109)

[2 Factors specific to our business 4](#_Toc128660110)

[2.1 Key people and responsible parties 4](#_Toc128660111)

[2.2 Understanding our jurisdictions & services 4](#_Toc128660112)

[Normal jurisdiction 4](#_Toc128660113)

[Defined services 5](#_Toc128660114)

[3 Factors specific to each client 7](#_Toc128660115)

[3.1 Customer Due Diligence (CDD) collection & checks 7](#_Toc128660116)

[Identifying the client (individuals / sole traders) 7](#_Toc128660117)

[Identifying the client (business) 8](#_Toc128660118)

[Verifying the identity of the client (businesses) 8](#_Toc128660119)

[Determining beneficial owners 9](#_Toc128660120)

[Verification of beneficial owners 10](#_Toc128660121)

[Politically Exposed Persons (PEP) and Sanctions screening 12](#_Toc128660122)

[Review Customer Due Diligence (CDD) information 12](#_Toc128660123)

[Establishing intended purpose and relationship 12](#_Toc128660124)

[3.2 Understanding each of our clients 13](#_Toc128660125)

[Client’s services and location 13](#_Toc128660126)

[Our services to the client 13](#_Toc128660127)

[4 Evaluate client risk 14](#_Toc128660128)

[4.1 Compile the relevant risk assessments for each client 14](#_Toc128660129)

[4.2 Completing an overall client risk assessment (for MLRO) 14](#_Toc128660130)

[4.3 Enhanced Due Diligence (EDD) 15](#_Toc128660131)

[5 Ongoing Reviews 15](#_Toc128660132)

[5.1 Periodic or exceptional client review 15](#_Toc128660133)

[5.2 Review of policies & procedures 16](#_Toc128660134)

[5.3 Overall (firm wide) annual risk assessment 16](#_Toc128660135)

[6 Suspicious Activity Reporting (SAR) 17](#_Toc128660136)

[6.1 Internal Suspicious Activity Report (ISAR) 17](#_Toc128660137)

[6.2 External Suspicious Activity Report (ESAR) 17](#_Toc128660138)

[7 Records 18](#_Toc128660139)

[7.1 Record Keeping 18](#_Toc128660140)

[7.2 Retention of records 18](#_Toc128660141)

[8 Training 18](#_Toc128660142)

# Overview

The policy aims to comply with the risk-based approach to anti money laundering and terrorist financing required by regulations.

It takes an overview of the defined services provided by our business and the risk associated with each of them. The regularity, geographical location and sector in which services are delivered are all taken into account when determining the associated risks.

Furthermore, customer due diligence (CDD) is applied to establish the risk level associated with each client. By combining an overview of risk associated with a particular client and the risk of services being delivered, we ultimately determine the combined risk level associated with that client.

We understand that anti money laundering scrutiny cannot be applied in equal measure effectively across our entire customer base. The risk-based approach we are implementing allows us to classify our services and our customer base, in order that our resources can be prioritised to those areas deemed at the highest risk of money laundering and terrorist financing.

The policies are reviewed every 12\* months.

**Onboarding**

At a high level, the following process is described within this policy and procedures. This process is repeated across the client base.

Diagram

Description automatically generated

The period set between risk reviews is determined by both the risk level assigned to a client and also whether a significant event or transaction leads to a review of AML risk.

# Factors specific to our business

## Key people and responsible parties

The money laundering compliance principal (MLCP) is the ultimate authority in the organisation, responsible for money laundering. The Money Laundering Reporting Officer (MLRO) can be an officer who is responsible to regularly review and ensure this AML policy is up to date and relevant to the business.

|  |  |
| --- | --- |
| **Role** | **Person** |
| MLCP / member of the board of directors / senior management team. | <<Add first and last name>> |
| MLRO | <<Add first and last name>> |
| Deputy MLRO | <<Optional: Add one or more deputy MLRO>> |

*We understand the responsibilities and requirements of appointing an MLCO / MLRO as per guidelines of our professional body.*

## Understanding our jurisdictions & services

Defining the regional areas we work in and the type of services we offer, considering the risk of each, will act as a reference point when doing the risk assessment for each client.

It is important in doing the risk assessment for a client to note the relationship between jurisdiction and services offered to a client as the risk levels might vary depending on the combination of service / area e.g. we might be more familiar with a type of service in one jurisdiction than another.

### Normal jurisdiction

The business operates mainly within the following countries or economic areas (normal jurisdiction):

|  |  |  |
| --- | --- | --- |
| **Country** | **Status**  **(Core, Frequent, Ad Hoc)** | **Risk associated**  **(Normal, High)** |
| UK\*\* |  |  |
| Republic of Ireland\*\* |  |  |
| Other\*\* |  |  |

The business is aware that when providing services outside of the normal jurisdiction, these might present a higher risk. This is because our knowledge of the relevant rules and regulations in that jurisdiction are not on par with those of the normal jurisdiction.

### Defined services

The business understands that offering defined services which are either new or rarely provided can pose a higher risk. The type of service and sector play a role in the classification of the risk level associated with the service.

| **Service** | **Regularity of Service**  **(Often, Rare)** | **Is the service new**  **(Yes, No)** | **Risk level**  **(Normal, High)** |
| --- | --- | --- | --- |
| Accounting sector examples\*\* | | | |
| Self assessment\*\* |  |  |  |
| Year end accounts\*\* |  |  |  |
| Payroll\*\* |  |  |  |
| Company Formation\*\* |  |  |  |
| VAT Return\*\* |  |  |  |
| Crypto Transaction Processing\*\* |  |  |  |
| Audit\*\* |  |  |  |
| Liquidations\*\* |  |  |  |
| Legal sector examples\*\* | | | |
| Client bank accounts\*\* |  |  |  |
| Trust / company services\*\* |  |  |  |
| Wills and probate\*\* |  |  |  |
| Landlord services\*\* |  |  |  |
| Family law\*\* |  |  |  |
| Conveyancing\*\* |  |  |  |

# Factors specific to each client

The following approach is used to determine the risk of a new client during the onboarding process. The process takes into account the client ownership structure (beneficial owners) and a combination of the risk factors of the client relating to the services they sign up for and offer to their clients including the type of services, the geographical location of those and the delivery channels through which they are delivered.

Some of the information required can be gathered using software solutions, while other areas will require knowledge of the client and their business affairs.

The sections below references risk assessment templates in Xama Hub which have been specifically amended for our organisation.

When the information has been collated, the MLRO needs to review all factors and make an overall assessment of risk. During this process of review the MLRO might make a judgement that enhanced due diligence is required.

## Customer Due Diligence (CDD) collection & checks

The business will undertake customer due diligence on every new client. The following describes the actions taken during onboarding that relate to CDD and also the policy to undertake additional / ongoing CDD at appropriate times during the client relationship.

The requirements of good CDD consist of understanding:

1. **Our Client**
   * Identifying the client
   * Verifying the identity of the client
2. **Client Ownership Structure**
   * Identifying the beneficial owners (always individuals, not entities)
   * Taking reasonable measures to verify the identity of the beneficial owners and whether owners are politically exposed or have sanctions imposed against them
3. **Intended purpose and nature of the business relationship**
4. **Our client**

### Identifying the client (individuals / sole traders)

Where the client is an individual, the individual is also the beneficial owner. Therefore, the CDD carried out against the beneficial owner will cover the need for client identification and verification. This section (A) is not applicable in these circumstances.

### 

### Identifying the client (business)

Identification of a legal entity includes:

* Is the client registered with Companies House?
* If not registered with Companies House, is the entity registered with any other organisation, such as HMRC, Charity Commission, regulatory bodies outside the United Kingdom etc?
* Does the client have an online presence (website, social media etc)?
* Is it possible and clear to determine what the purpose of the business is?

### Verifying the identity of the client (businesses)

The following procedures are in place to verify the identity of a client. Some of these searches can be performed within Xama Hub,using the integration with Companies House or retrieving a full company report. Other information is found through google, client contact or other research. Where supporting documents are available these should be uploaded to the client record in Xama Hub and / or notes of research made on the risk assessment record.

|  |  |  |
| --- | --- | --- |
| **Verification** | **Xama Hub Searches** | **External sources** |
| Verification of Companies House | Verify company via Companies House link |  |
| The history (such as length of trading and filing of accounts) are taken into account as part of the search. | Company reports | Verify company via Companies House |
| Additional company information | Company reports provide a lot of information about the company. Our process is to check:   * \*\*Credit rating history * Shareholding structures * Negative information (County Court Judgements, bad debts) \*\*   to further improve our knowledge of a client. | \*\*Google search for the company to further evaluate its online presence and the purpose of the business.  Verify the key contact by phone via website telephone number.  Adverse media is also evaluated on this basis. \*\* |

**Low risk clients**

Low risk would normally only apply to publicly owned enterprises or financial institutions regulated by the FCA. Customer due diligence (CDD) measures are still required but the extent and timing may be adjusted to reflect the assessment of low risk.

1. **Ownership structure**

### Determining beneficial owners

Beneficial owners are those individuals who exercise control over the entity with whom we are engaging. Beneficial owners are always individuals.

*NB When engaging with a sole trader or individual, the beneficial owner is the individual and the below checks do not apply.*

These actions will be taken by the business to identify beneficial owners within entities:

|  |  |  |
| --- | --- | --- |
| **Verification** | **Xama Hub Searches** | **External sources** |
| PSC | Select via Companies House link  Add all |  |
| Directors | Select via Companies House link  Add directors if they are deemed to have managing control | Conversations with the client about control \*\* |
| Other individuals | Enter individuals’ details if they are deemed to have managing control | Conversations with the client about control\*\* |

The above mentioned data sources are the best available within the public domain but cannot be fully relied upon and should be scrutinised as part of the CDD process.

If the business becomes aware of a difference between the beneficial ownership and what has been registered with Companies House, the potential discrepancy will be discussed with the client to establish if it was an inadvertent error which will be corrected without delay. The outcome of any such discussion with the client will allow the business to conclude whether a material discrepancy exists and is reportable.

A discrepancy will be reported to Companies House as soon as practically possible, which should be within 15 days.

The MLRO should evaluate if any other individuals have significant control over decision making and benefit materially from the profits of the company, which might qualify them as a beneficial owner.

Where the ownership is more complicated, Xama Hub allows you to run company reports where detailed shareholding and ownership of the entity can be further investigated and a decision made on who to check as beneficial owners.

For more complex company structures and legal entities not covered by reports from Companies House or those available through Xama Hub please refer to Appendices regarding the regulatory body guidance.

### Verification of beneficial owners

For each beneficial owner the following procedure is completed to verify their identity:

| **Verification** | **Xama Hub Searches** | **External sources** |
| --- | --- | --- |
| Collection of an identity document (passport or driving licence) | Via an onboarding request sent from Xama Hub to the client. | Enter information collected in person. |
| Proof of address document  *See (a) below* | Via an onboarding request sent from Xama Hub to the client. \*Specify if done for all clients or select group or none as standard.\* | Collect information and attach in Xama Hub |
| Verification of the document | Automatic when the contact completes an onboarding request.  Verification report along with all the relevant electronic checks are stored against the contact record. Checks carried out include the validity, quality, expiry date of the document and digital tampering. | If doubts about whether the document belongs to the individual, further verify the person's identity through a meeting or video call. |
| Capturing data from collected documents | Date of birth, given names and document numbers are extracted from the identity document to assist with further verification checks. The collection procedure also collects the current home address as provided by the contact. |  |
| Reviewing captured data | Collected and extracted information is reviewed, edited and commented on before a decision is made to accept or reject it.  Once accepted, the details for the individual are added to the contact record within Xama Hub without rekeying of data. |  |
| Electronic identity check (commonly referred to as an AML check)  *See below (b)* | Checks can be run against an individual using all available data.  The full report of the identity check is stored against the contact record within Xama Hub. |  |

**a) Proof of address document**

A document to further verify the residential address linked to the individual will [always be requested] / [requested for non-UK residents] / [be requested when a PASS result was not obtained through the electronic check].

A valid proof of address document is:

* + Utility bill (gas, electric, water) no older than 3 months.
  + Bank statement no older than 3 months.
  + Official HMRC correspondence no older than 3 months.
  + Council tax bill no older than 12 months.
  + \*Insert as applicable\*

**b) Understanding AML checks**

Before you run the checks you should confirm you have most of the information below as it is helpful to increase PASS rates:

* + First and last name
  + Residential address
  + Date of birth
  + Passport or driving licence number
  + Identity document expiry date

The AML check on an individual can return three possible results. PASS, REFER or ALERT.

* + **PASS** indicates that there has been at least two good matches against independent data sources such as the electoral roll or UK credit header. Verification of document numbers can also assist in obtaining a PASS result.
  + **REFER** indicates that sufficient matches could not be found. This can be due to a recent change in address or incorrect input information e.g. shortened first name.
  + **ALERT** most typically indicates that the person has been recorded as deceased at the address listed. Further investigation is done on the individual, such as a face to face verification, if an ALERT result is generated.

### Politically Exposed Persons (PEP) and Sanctions screening

For each beneficial owner, as part of the AML check, a screening is carried out against international PEP and sanctions data sources.

|  |  |  |
| --- | --- | --- |
| **Verification** | **Xama Hub Searches** | **External sources** |
| Politically exposed persons | Any potential matches are flagged as part of the AML check | Searches & research to confirm or dismiss possible match |
| Sanctions data sources | Any potential matches are flagged as part of the AML check | Searches & research to confirm or dismiss possible match |

The following should be noted:

* + Persons with political exposure are at higher risk of money laundering offences.
  + In the UK, PEPs generally refer to high ranking officials with influence over government policy and would exclude lower ranking officials, such as local councillors.
  + PEPs in countries with reduced money laundering regulations carry the highest risk.
  + Where a match to the sanctions list is confirmed, the business will evaluate whether any business relationship may be established with the client.

### Review Customer Due Diligence (CDD) information

Within Xama Hub the following review processes are in place:

* + Review and pass or fail a flagged identity document
  + Review and pass or fail any check which has returned a REFER or ALERT result
  + Review and confirm or dismiss a possible PEP or sanctions match

Review notes are recorded as part of each review carried out and notes fields available to state why a manual pass or fail was attributed to a result.

### Establishing intended purpose and relationship

**C) Intended purpose and relationship**

The MLRO needs to establish if the relationship with the client is normal for our organisation and for the client. This includes:

* + How the client was introduced to our organisation
  + What delivery channels are used for our services to the client
  + Whether it makes sense for the client to buy these services from our organisation

*The relevant sections in the risk assessment templates in Xama Hub have been tailored by the MLRO to apply to our organisation.*

## Understanding each of our clients

The MLRO needs to have a good understanding of the type and geographical location of the client’s services, the services we offer to the client and what risk factors they represent. These include:

### Client’s services and location

**Business activities and sector**

**Geographical risk**

Refer to appendix for links to find countries currently on the global watchlists.

### Our services to the client

**Delivery channels**

Face to face delivery has less risk than services delivered through an intermediary.

**Defined services**

Refer to defined services and risk associated with them above.

*The relevant sections in the risk assessment templates in Xama Hub have been tailored by the MLRO to apply to our organisation.*

# Evaluate client risk

It is the responsibility of the MLRO to review the searches that are carried out and ensure that the findings are sufficient for identifying and verifying the identity of a client and the beneficial owners. Where results are deemed insufficient, additional external searches may need to be carried out. The results of these searches should then be stored in Xama Hub for record keeping.

## Compile the relevant risk assessments for each client

Our risk assessment templates are designed for us to “know your client” and need to be completed for each client. People involved in the collection of information should complete these for the relevant client and then submit them for review.

## Completing an overall client risk assessment (for MLRO)

The end result of an assessment is to assign an overall risk to the client taking into account all the information collected (sections above). Following the processes above, all the information required for the risk assessment should be available in Xama Hub.

**The risk level to be assigned and corresponding action for each client is:**

|  |  |  |
| --- | --- | --- |
| **Risk level assigned** | **Factors** | **Action** |
| Low | Low risk is only assigned to those clients who \*Insert as relevant for your organisation\* e.g. \*\*client who is a public administration, or a publicly owned enterprise.\*\* | Review periodically as per policy for risk level\*\* |
| Normal | No factors or combination of factors deemed to be high risk | Review periodically as per policy for risk level\*\* |
| High | Any factors or combination of factors that is deemed high risk | Enhanced due diligence and periodically as per policy for risk level\*\* |

## Enhanced Due Diligence (EDD)

Where a client’s risk assessment result is deemed as high risk, the business will evaluate the client further and apply the following enhanced due diligence actions as appropriate.

The following actions will be taken in this case:

* + \*\*Face to face interview to alleviate any specific concerns.
  + Source of funds evaluation.
  + Specific checks by a director on services provided related to potential money laundering activity.
  + Capturing additional identity documentation, such as a second identity document.
  + Additional searches, such as adverse media.
  + Director reports to identify disqualified directors.
  + More searches on the companies and individuals to better understand the beneficial owners and their business activities. \*\*

Any resulting documentation and search results will be recorded within Xama Hub.

The following actions will be taken during the servicing of the client to manage risk:

* + \*\*Additional scrutiny of material transactions
  + Additional sign off by senior management of any payroll transactions
  + Additional review and sign off by senior management of formal report
  + Add other\*\*

# Ongoing Reviews

## Periodic or exceptional client review

The business will periodically review CDD across its client base.

**Periodic review will be done as based on:**

* + Clients classified as Low risk, will be reviewed every 2 years\*
  + Clients classified as Normal risk, will be reviewed every 1 year\*
  + Clients classified as High risk, will be reviewed every 6 months\*

**Additionally reviews will take place in the following circumstances:**

* + Before any large transaction falling outside the normal scope of the engagement.
  + When a significant change to the client engagement warrants such a review. This can include scenarios where the defined services the client subscribes to changes or if there is a significant change in beneficial ownership or structure of the client.

**Review procedure**

* + Identify any new beneficial owners and follow standard CDD steps above
  + For previous beneficial owners that remain as such, the following should be done:
  + \*Run and review AML checks including PEP and sanctions
  + Request up to date ID verification where expired
  + Add & edit as appropriate\*
  + Review, copy and update the previous risk assessment for that client, taking into consideration:
    - * Changes to services engaged with by the client
      * Changes to beneficial owners
  + Review and reassign the overall risk level associated with the client
  + The new risk assessment is then submitted for review by the MLRO, submitted and recorded against the client record within Xama Hub.

## Review of policies & procedures

These policies and procedures surrounding AML and client due diligence, will be reviewed annually\* by the MLRO. This includes a review of the risk assessment templates.

Changes to regulations will be considered and changes communicated to all relevant staff.

## Overall (firm wide) annual risk assessment

Our annual risk assessment is done in line with the requirements of our regulator, including:

| **Area** | **Description** | **Record keeping** |
| --- | --- | --- |
| Policy review | Confirmation that the policies and procedures have been reviewed in the last 12 months. | \*\*Last date of review entered here by MLRO\*\* |
| Staff training | Confirmation that all staff have been adequately trained on AML. | \*\*Insert where records are held.\*\* |
| Clients risk profiles | Following the current guidance / templates from our regulator, summarise the risks associated and mitigation measures for each of the risk areas as set out in above sections. | \*\*All data held within Xama Hub.\*\* |

## 

# Suspicious Activity Reporting (SAR)

## Internal Suspicious Activity Report (ISAR)

Where there is suspicion of money laundering activity, staff must report this to the MLRO.

* The activity must be clearly defined and include as much detailed information as possible.
* It is the MLROs responsibility to evaluate the ISAR and decide whether or not to raise an External Suspicious Activity Report (ESAR).
* It is important for the MLRO to consider what information is shared with internal staff, taking into consideration the risk of a “Tipping off offence” or “Prejudicing an investigation offence”.

**Record keeping**

Record keeping is key and our policy is:

* To report a suspicion, staff can find the internal SAR here: INSERT
* The form should be submitted to the MLRO and should not be visible to any other staff
* The MLRO will record its findings in the same way

*Note that the aim is for the management of ISARs to be made available within Xama Hub in 2023. There is no set timeline for the release yet.*

## External Suspicious Activity Report (ESAR)

When deciding whether to report a suspicious activity to the NCA the MLRO will refer to the detailed guidelines as provided by their regulator. Deciding whether to submit an external report and the factors to take into account when doing so can be complicated and the business will first evaluate whether to seek external legal counsel before commencing the reporting procedure.

At a high level, the following will be considered:

* + Whether the offence meets the criteria for submitting an external suspicious activity report.
  + Whether a defence against anti money laundering is required.
  + What precautions should be taken as to not commit a “Tipping off offence” or “Prejudicing an investigation offence”.

## 

# Records

## Record Keeping

The following records in relation to CDD should / are maintained within Xama Hub:

* Electronic records of all client risk assessments.
* Any searches, investigations, review notes and notes on decisions taken, carried out as part of the CDD process, should be / are stored as documents within Xama Hub and linked to the appropriate contact, client or risk assessment.
* The identity information of all beneficial owners, along with any electronic checks carried out against them are maintained within Xama Hub.
  + Copies of identity documents, proof of address documents and any other supporting documents to verify the identity of a beneficial owner are stored against the contact record of the beneficial owner.
  + PEP and sanctions screening records are stored and maintained against the relevant contact.

## Retention of records

Records related to the CDD of clients will be maintained within Xama Hub for five years after the engagement with a client terminates.

In accordance with data protection laws records will be purged five years following the offboarding date of a client.

# Training

Appropriate AML training is provided to staff annually that includes:

* Making staff aware where to access this AML policy and procedures document.
* An understanding of the risk-based approach adopted by the business to prevent money laundering activity.
* How to identify money laundering activity within the defined services offered by the business.
* Where suspicious activity arises, how to report this to the MLRO in the form of internal suspicious activity reports.
* Understanding offences and consequences.

A record of training offered and completed by appropriate staff are kept in: \*<<Insert>>

Training is also included in induction training for new staff to ensure compliance.\*

**Appendix A: Guidelines considered**

Guidelines, risks and trends for money laundering are constantly changing. It is the responsibility of the Money Laundering Reporting Officer (MLRO), to keep up to date with relevant materials and especially the risks associated with their business.

The guidance in this document, the generic risk assessment templates and the Xama Hub software platform should be seen as a framework for each MLRO to amend according to their understanding and interpretation, specifically tailored for their own business.

The main sources considered for creating these frameworks are:

**Accountancy sector**

* CCAB guidelines of May 2022 as approved by HM Treasury

<https://www.ccab.org.uk/wp-content/uploads/2022/05/1_AMLGAS-Final-May-2022.pdf>

This guidance has been adopted by all regulatory bodies within the accountancy and bookkeeping sector.

Also reference the link below for more information : <https://www.ccab.org.uk/anti-money-laundering-and-counter-terrorist-financing-guidance-for-the-accountancy-sector-2022/>

* National risk assessment of money laundering and terrorist financing as provided by HM Treasury and Home Office. Please refer specifically to chapter 9 for accountancy services.

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf>.

**Legal sector**

<https://www.lawsociety.org.uk/topics/anti-money-laundering/anti-money-laundering-guidance>

**Countries on the watchlist**

Commonly referred to sites for countries on the watchlist globally are:

[*https://www.fatf-gafi.org/en/home.html*](https://www.fatf-gafi.org/en/home.html)

**Other**

Other relevant reading includes, but is not limited to:

* National risk assessment of money laundering and terrorist financing 2020

<https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2020>

* The Money Laundering, Terrorist Financing and Transfer of Funds

<https://www.legislation.gov.uk/uksi/2017/692/contents/made>

<https://www.legislation.gov.uk/uksi/2019/1511/contents/made>

* FATF Guidance on the Risk-Based Approach for Accountants

[*https://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Accounting-Profession.pdf*](https://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Accounting-Profession.pdf)

* Review the National Crime Agency website

[*https://www.nationalcrimeagency.gov.uk/*](https://www.nationalcrimeagency.gov.uk/)

* Terrorism Act 2000

[*https://www.legislation.gov.uk/ukpga/2000/11/contents*](https://www.legislation.gov.uk/ukpga/2000/11/contents)

* Proceeds of Crime Act 2002

[*https://www.legislation.gov.uk/ukpga/2002/29/contents*](https://www.legislation.gov.uk/ukpga/2002/29/contents)