



# Financial Crime Best Practice Guide

**Version 1.1**

April 2022

## About TISA

**The Investing and Saving Alliance (TISA)** is a unique, rapidly growing membership organisation for UK financial services.

**Our ambition is to improve the financial wellbeing of all UK consumers.** We do this by focusing the convening the power of our broad industry membership base around the key issues to deliver practical solutions and devise innovative, evidence-based strategic proposals for government, policy makers and regulators that address major consumer issues.

TISA membership is representative of **all sectors of the financial services industry**. We have **over 200-member firms involved in the supply and distribution of savings, investment products and associated services**, including the UK's major investment managers, retail banks, online platforms, insurance companies, pension providers, distributors, building societies, wealth managers, third party administrators, Fintech businesses, financial consultants, financial advisers, industry infrastructure providers and stockbrokers.

As consumers, the financial services industry and the economy react to and recover from the effects of the pandemic, the importance of the three key pillars of work that TISA prioritises has never been more apparent:

- **Strategic policy initiatives that influence policymakers** regarding the financial wellbeing of UK consumers & thereby enhancing the environment within which the industry operates in the key areas of **consumer guidance, retirement planning, later lifetime lending, vulnerable customers, financial education, savings and investments**.
- TISA is recognised for the **expert technical support provided to members** on a range of operational and regulatory issues targeted at improving infrastructure and processes, establishing standards of good practice and the interpretation and implementation of new and existing rules and regulations covering **Financial Crime prevention, CASS, ESG/RSI, operational resilience, Governance, Conduct and Culture** and a range of other areas.
- **Digital transformation initiatives** that are driving ground-breaking innovation and the development of industry infrastructure for greater operational effectiveness and revenue promoting opportunity for firms. TISA has become a major industry delivery organisation for consumer focused, digital industry infrastructure initiatives – **TISAtch** (a digital marketplace that brings together financial institutions and FinTechs for greater collaboration and innovation) and **TURN** (TISA Universal Reporting Network – a digital platform providing a secure data exchange for financial services using blockchain technology) – alongside projects **Digital ID** and **Open Savings, Investment & Pensions**. This reflects TISA's commitment to open standards and independent governance.

## Contents

1	Introduction .....	5
2	Investment Fraud and Impersonation.....	6
	2.1 Introduction .....	6
	2.2 Legal And Regulatory Background.....	6
	2.3 Harms We Are Seeking To Prevent.....	7
	2.4 Recommendations For Firms .....	7
	2.5 TISA Customer Guide .....	10
3	Cannabis Related Investment Restrictions .....	17
	3.1 Introduction .....	17
	3.2 UK Legislative and Regulatory Landscape.....	17
	3.2.1 Recreational Cannabis.....	17
	3.2.2 Medicinal Cannabis .....	17
	3.3 Risks of investing in cannabis related stocks .....	18
	3.3.1 Active vs. passive decision-making .....	18
	3.3.2 Primary market or secondary market investment.....	18
	3.4 Defence against Money Laundering.....	19
	3.4.1 Adequate consideration defence.....	19
	3.4.2 Production under licence .....	19
	3.4.3 Suspicious Activity Reports.....	19
	3.4.4 De minimus principle .....	20
	3.4.5 Placing reliance on FCA vetting.....	20
	3.4.6 Pragmatic/purposive approach .....	20
	3.5 Navigating a Risk Based Approach .....	21
	3.5.1 Potential risk scale .....	21
	3.6 Investment restriction support (data, lists and screening).....	21
	Appendix 1 Taxonomy .....	23
	Appendix 2 Useful links .....	24
4	Anti- Money Laundering Transaction Monitoring.....	25
	4.1 What is transaction monitoring?.....	25
	4.2 Risk based approach .....	25
	4.3 Manual vs. automated monitoring.....	26
	4.4 Nature of relationship.....	26
	4.4.1 Relationship Managed.....	27
	4.4.2 Direct clients .....	27
	4.4.3 Online Only Customers.....	27
	4.4.4 Telephone/email.....	27
	4.4.5 Advisory firms .....	28
	4.5 Monitoring customer activity.....	28
	4.5.1 Transactional activity .....	28
	4.5.2 Behavioural activity.....	29
	4.5.3 Negative media and other sources .....	29
	4.5.4 Contact from external parties.....	29
	4.6 Periodic review of TM framework.....	30
	4.7 Sources and further reading .....	30
	4.8 Transaction Monitoring – Practical examples.....	30
	4.8.1 Transactional activity .....	31
	4.8.2 Behavioural activity.....	31
5	Anti Bribery and Corruption.....	35
	5.1 Introduction .....	35

5.2 Anti bribery and corruption framework .....	35
5.2.1 Governance and management information .....	35
5.2.2 Culture and tone from the top .....	35
5.2.3 Senior management sponsorship .....	35
5.2.4 Roles and responsibilities .....	36
5.2.5 Independent review .....	36
5.3 Assessing bribery and corruption risk.....	37
5.3.1 Assessment methodology.....	38
5.4 Policies and procedures .....	39
5.4.1 Documented, risk based policies and procedures .....	40
5.4.2 Remuneration structures .....	40
5.4.3 Code of ethics .....	40
5.4.4 Third parties and intermediaries .....	40
5.4.5 Whistleblowing, investigation and dismissal.....	40
5.4.6 Gift and hospitality .....	40
5.4.7 Facilitation payments .....	41
5.4.8 Political and charitable contributiosn and public officials definition.....	41
5.4.9 Books and record keeping .....	41
5.4.10 Training and awareness.....	41
5.5 Monitoring for compliance .....	42
5.6 Anti bribery and corruption in financial services .....	43
5.7 Links to useful resources.....	44
5.8 TISA Bribery and corruption high level risk assesment template.....	45
5.8.1 Purpose of the template .....	45
5.8.2 Key definitions .....	45
5.8.3 TISA Bribery and corruption high level risk assesment template .....	46
6 Application of the three lines model to AML /CTF.....	56
6.1 Purpose of this review .....	56
6.2 Introduction to the three lines of defence (3LOD) model .....	56
6.3 Application of the three lines model to AML /CTF and the role of the MLRO .....	57
6.4 FCA expectations of firms .....	58
6.5 Conclusion.....	59
Appendix 3.....	60

Version history:

1.0 August 2021 – Published January 2022

1.1 April 2022 – Updates to sections 4.6 & 5.4.1. Published April 2022

## 1. Introduction

The TISA Financial Crime Risk Best Practice Group, consisting of representatives from a wide range of firm types, has produced this Guide in the form of a number of separate documents, on discrete topics. Each document was written by one or more members of the group and reviewed by all members of the group, to provide a balanced view of each key area relating to the prevention of financial crime and managing financial crimes risks.

Please remember that the information contained within these statements is for informational purposes only and is not intended as a substitute for the need of each firm to understand the financial crime risks that relate to its business model and determine its own financial crime prevention policies and procedures that are relevant to its business. The information contained is for general guidance only, is not exhaustive and may change from time to time.

## 2. Investment Fraud and Impersonation

### 2.1 Introduction

Scams have become increasingly prevalent, even more so during the disruption and uncertainty caused by the Covid-19 pandemic. Over the course of 2020, Action Fraud received over 300,000 separate reports of fraud, with over £2bn reported to have been lost by consumers in the UK.

This has led to one body, The Royal United Services Institute (RUSI) to demand that the Government treat fraud as a national security threat.

A recent common trend in scams has been an increase in firm impersonation or 'cloned firm' fraud.

This sees a fraudster establish fake websites, email domains and documentation which have similar brand identity to that of regulated financial services firms and household brands. In addition to the traditional out-of-the-blue contact usually experienced from these scammers; an investment opportunity will be advertised and identified by the consumer via an internet search. Potential investor information will be requested and will need to be submitted on the website. The potential investor will then be contacted by telephone by a fraudster pertaining to represent the regulated firm. The fraudster will then provide information about the investment opportunity, usually with a limited time period to invest, and focusing on the 'fact' that the investment is covered by the FCA. Should the investor be interested they will send an application by email. The documents will look like the regulated firm's brand and may be a mixture of 'true' and fake documentation. Once complete the investor will submit the application and pay funds into the fraudster's bank account. Due to the original type of investment being advertised as a long-term investment, it may not be until months have passed and the investor has not received any investment return payments that they contact the 'real' regulated firm, and the fraud is identified.

To combat this ever-growing threat, the TISA Financial Crime Working group have compiled this guidance document for members. Following this guidance, member firms can be assured that they are well positioned to counter the activities of these fraudsters and the inclusion of an informational tool designed for consumers ensures a proactive and joined up response.

### 2.2 Legal & Regulatory Background

Since 2008 City of London Police have been the National lead police force for fraud. This is a broad role that encompasses many aspects of the volume economic crime landscape, from investigating some of the country's most complex frauds to hosting the National fraud and cybercrime reporting centre, Action Fraud.

Action Fraud is the only national crime reporting system in the UK. All frauds and a majority of cybercrime in England, Wales and Northern Ireland are reported to Action Fraud. These reports are then analysed by the National Fraud Intelligence Bureau (NFIB), also hosted by City of London Police, and then either sent on to the police force where the suspect resides or retained within the NFIB to inform disruption and warning activity.

For those members based in Scotland, frauds are usually investigated by the Police Service of Scotland, which has regional specialist units within its Specialist Crime Division to deal with complex economic crime cases. Serious and complex fraud and other economic crimes are investigated under the direction of the Economic Crime Unit, part of the Serious Organised Crime Division of the Crown Office and Procurator Fiscal Service (COPFS) which is Scotland's prosecution service.

The Financial Conduct Authority has as one of its statutory objectives the reduction of financial crime, which includes fraud. Regulated firms must have adequate policies and procedures in place to counter the risk that they may be used to further financial crime. Individuals authorised by the FCA must act with integrity in carrying out their accountable functions. The FCA is empowered to enforce against firms and individuals for breaches of the relevant rules. The Prudential Regulation Authority (PRA), which is responsible for the prudential regulation and supervision of various financial institutions, has similar rules and means of enforcement to the FCA.

The FCA's 2021 Financial Crime Guide provides guidance to firms on steps they can take to reduce their financial crime risk across several areas, including fraud. The guidance is non-binding but is an indicator of the FCA's expectations and provides examples of good and poor practice.

### **2.3 Harms we are seeking to Prevent**

The ability for a consumer to lose their money to fraudsters is sadly quite high. Being a victim to a scam can have a devastating effect on the individual's financial and mental wellbeing. Once an individual has become a victim to a scam, history has demonstrated that they are contacted by fraudsters again.

Cloned firm impersonation fraud sees the consumers access scam websites since they can feature in search engine results. As of June 2021, current legislation fails to ensure that search engine providers have a duty not to enable fraudsters to advertise scam websites in their results.

By removing these results, consumers would have less opportunity and be less likely to discover scam websites and therefore become victims of fraud.

Cloned firms are not likely to be legally liable for any losses suffered by victims to this type of scam, but there may be other negative impacts, such as reputational damage and reduced investor confidence in this sector.

### **2.4 Recommendations for Firms**

The existence of investment and impersonation fraud takes advantage of unsuspecting innocent parties and can drastically impact the victims both financially and emotionally. It is therefore important that firms provide guidance to their customers on how to spot and avoid such scams.

By producing such guidance this can help to increase understanding across our customers and support the ongoing process of disrupting such fraudulent activity using a program of continual awareness.

Key to disrupting such behaviour is helping customers to recognise the various approaches used by criminals to undertake the scam by:

- convincing the customer that something is genuine by impersonating an individual, firm/well-known brand;
- using fraudulent advertising and or a website; and
- taking advantage of situations (e.g. COVID-19)

Scams take many forms and are continually changing. Therefore, if firms can explain to their customers the steps to follow to establish if something is genuine this will help greatly to minimise the potential of someone falling victim to such scams.

Below outlines industry guidance that a firm should consider following when dealing with and taking action on such reports. When discussing any of the information with the customer throughout the investigations, the customer should be kept informed. Given time is of the essence in a lot of cases, it is advised that telephone conversation is the first port of call when gathering information from the customer. A follow up written communication would then suffice to confirm discussions and advice.

**When being notified of a possible scam from a customer or member of the public, a firm should obtain the following key information for investigation, and provide certain information to the customer:**

- Full name and contact details of the caller.
- **Firstly, it is important to ask if they have sent any money – If they have, particularly if it is a recent payment, they need to report this to their bank immediately to understand if they can recall or reimburse the payment, and if there are any further protective measures the bank can take to secure the account.**  
Time is of the essence so consider insisting that the caller hangs up, contacts the bank and then rings back.
- Advise of the Authorised Push Payment code of practice and encourage them to make a claim against their bank, help and support with this is provided in the following link: <https://www.which.co.uk/consumer-rights/advice/how-to-get-your-money-back-after-a-scam-amyJW6f0D2TJ>
- Check if the caller is an existing customer and if they have provided any details to the fraudster about their holdings or account.
- Assess any potential vulnerability of the caller. Encourage them to speak with a trusted friend or family member for support or assistance if needed. A useful resource is the BSI Protecting customers from financial harm as a result of fraud or financial abuse. Code of practice PAS 17271.
- How they first came into contact with the fraudster (did they see something online, receive a cold call etc.).
- When they first made contact, together with dates and times of any contact they can recall.
- How the contact communicated was made- Email/Postal/Telephone.
- Details of any websites, social media pages, sales brochures, email addresses, phone numbers and names the fraudster used to contact the customer, as well as requesting any emails sent to them as part of the scam for further investigation - request that the emails be sent by attaching them to a new email (rather than simply forwarding), so that your information security team can see the domains behind the emails, in the metadata.
- The type of investment offered and how it was described to them.
- Bank details provided by the fraudsters (whether payment has been made or not).
- **If payment has been made:** Details of any payments made, include dates and amounts.
- Information the caller has provided to the fraudster, including personal information and documentation (such as passports, bank statements, utility bills etc.).
- Any other information they may be able to provide.
- **If the caller has NOT paid away funds** but is enquiring as to the legitimacy of this, then tell them this is a scam - gather the details as above and advise them to have no further contact with the individuals concerned.

**Advise the customer to take these next steps:**

- Report the matter to the UK National Reporting Centre for Fraud and Cyber Crime - Action Fraud on 0300 123 2040 or via [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

- Notify the FCA by telephoning their Consumer Helpline (0800 111 6768) or by filling in an online form (<https://www.fca.org.uk/consumers/report-scam-unauthorised-firm> )
- Visit the Financial Conduct Authority's ScamSmart information to learn more about investment scams and some useful tools to assist in avoiding such frauds [www.fca.org.uk/consumers/protect-yourself-scams](http://www.fca.org.uk/consumers/protect-yourself-scams)
- Consider whether any other financial accounts may be at risk and to get in touch with them as soon as possible to alert them of the situation. The firms may be able to take extra steps to ensure the security of their accounts.
- Forward suspicious **phishing emails** to the National Cyber Security Centre [Suspicious Email Reporting Service \(SERS\)](#)
- Forward spam texts to Ofcom using the number 7726.
- Contact CIFAS, a charity fraud prevention organisation, to affect a protective registration marker (<https://www.cifas.org.uk/services/identity-protection/protective-registration>), which will alert them of any unauthorised activity.
- Keep an eye on their credit file in case of any further activity (even if unsuccessful, many have parted with personal information). They can register (usually for free) with one of the credit reference agencies for a regular update on their credit report – e.g. <https://www.creditkarma.co.uk/> , <https://www.experian.co.uk/> , <https://www.equifax.co.uk/>
- In the coming weeks/months be very cautious of anyone other than their bank offering to recredit them with money, especially if they ask for a fee in order to proceed.

**Once the firm has been advised of the potential scam, it should seek to build a file in preparation for reporting to the relevant authorities by performing the following investigations:**

- Check the FCA website - Known Unauthorised Firms – remember though **if a firm is not on the list this does not mean they are bona fide**. You can also check the FCA register to see whether the firm is listed, or if there is a close match to a regulated firm.
- Check how long the website has been established – [www.who.is](http://www.who.is). – A genuine company should have a few years internet presence and be clearly registered (rather than registered privately).
- Perform online searches on the company and/or investment – If the caller has been contacted by a scam, it is likely that others have too.
- Check to determine if the fake website has lifted text from other reputable sites and pasted onto their own.
- Check [www.scamadviser.com](http://www.scamadviser.com) – this site gives a breakdown of the website and what the details of it may indicate based on location, time active, ownership of site etc.
- Check the company is registered on the relevant 'Companies House' website for the country they claim to be operating. In addition, if they claim to be/appear to be a financial services firm they should be regulated by the appropriate regulatory authority. Use [Companies House - Government Links](#) and [Regulatory Authorities by Country](#) to help check registrations.
- Review any letters/emails that the customer may have been able to provide. Sometimes email addresses can appear suspect along with numerous grammatical and spelling errors which may be missed from the untrained eye.

**Next steps for the firm to take:**

- Report the fraud to law enforcement - Action Fraud on 0300 123 2040 or via [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

- Consider whether, as a result of what has been learned, a Suspicious Activity Report (SAR) filing is appropriate – for instance if payments have been made and the details are known.
- Firms should remember that they can submit a ‘vulnerable person’ SAR, if this would be appropriate: <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/45-guidance-on-sars-reporting-routes-relating-to-vulnerable-persons/file>
- If firms are aware that other firms have suffered from the same fraud then they may wish to submit a Super-SAR, under section 11 of the Criminal Finance Act 2017. This involves them, with the consent of the NCA, collecting information from other firms subject to the fraud, collating the information and submitting the consolidated intelligence report to the NCA.
- Consider the need to contact the FCA with details of the fraud. The FCA have pages dedicated to alerting members of the public about firms which have had their brand cloned along with the ability to add warnings.
- Firms should ensure that their contact centres are aware of current types of fraud, the red flags and receive training on how to deal with contact from those who have suffered such frauds. They should be aware of what to ask, and how to offer suitable help.
- Review the fraud section on the firm’s website and update it if necessary. Consider whether a warning should be placed on the website to alert customers and other visitors.
- Consider communication initiatives for customer education.
- Fake adverts identified online should be reported to The Advertising Standards Agency (ASA) – their website has a section on [reporting online scam adverts. Fake adverts on Social Media platforms can also be reported directly.](#)

#### **If the firm has been cloned:**

- Take down any websites by contacting the site owner, law enforcement agencies, the internet service provider (ISP) or the domain registrar - Services such as [WHOis](#) can provide this information. Note that evidence of the fraud will be required by the ISP or registrar.
- Take detective steps to identify any fraudulent websites that may have been set up to appear legitimate using almost replicates of the real URL. [DNS Twist](#) is an example.
- Services such as [URLCrazy](#) enable you to take preventative steps through generating and testing domain variations to detect typo squatting, URL hijacking, phishing, and corporate espionage.
- If website take down is successful, try to prevent similar events from happening, consider making a complaint to the ISP or registry – use [Nominet](#) for UK domains and non-UK [here](#).
- Notify the FCA who will be able to place a warning on their unauthorised firms list.
- If legitimate phone numbers have been spoofed by the fraudsters, consider protecting these numbers with Ofcom, who can add the number to their ‘do not originate’ list. Note however that this only applies to numbers which are only ever used to contact the firm, and from which no calls are ever made.

## **2.5 TISA Customer Guide:**

The following section is intended as an information template for firms to publish to Customers either as TISA guidance, or to use as a basis to form their own branded document. Additional guidance can be found <https://www.actionfraud.police.uk/a-z-of-fraud>. If publishing as TISA guidance, no changes should be made to the wording:

# TISA Guide to Investment Fraud

## What is Investment Fraud?

There are many different types of investment fraud. They are often difficult to spot because they're designed to look like genuine investments and the scammers may have a professional looking website and documents.

It often involves criminals contacting people through cold calls and out-of-the-blue offering an opportunity to invest into a scheme, investment or product that is either worthless or doesn't exist – including offers for the victim to purchase historical shares that are no longer trading, or offers to purchase shares victims hold and an attractive price, for an advance fee. These types of scams often operate out of what is known as 'Boiler Rooms'.

For many fraudsters, it is a full-time job meaning they have the time to build a relationship with their victim and make them more vulnerable to their exploits. Their aim is to take the victim's money and convince them that they have invested into something worthwhile.

Once monies have been paid to the criminals, usually via bank transfer, it is unlikely they will be recovered and contact from the offenders is likely to cease.

## What is Impersonation/Clone Fraud?

Impersonation/clone fraud is an iteration of an investment scam. Impersonation fraud involves an imposter posing as an individual or legitimate firm with the aim to convince their victim to make payment or provide their personal or financial details.

Clone firm investment scams involve fraudsters using literature and websites that mirror the details of trusted and authorised organisations. They'll try to convince their victim that they work for a genuine company and use high-pressure selling tactics to get you to buy 'investments' which, of course will be worthless and often aren't even offered by the company they're pretending to be.

It is worth highlighting that in some, more recent, versions of this type of scam, fraudsters have obtained their victim's details via online comparison sites they have set up, or scam online adverts where individuals are searching for investment/savings opportunities into vehicles such as ISAs and bonds. The initial call or contact from the fraudsters is then essentially expected rather than the typical 'out-of-the-blue' contact usually experienced in investment scams.

Criminals may use a tactic called 'spoofing' to make their call or text appear genuine by cloning the number or sender ID which the organisation uses. Whilst legitimate firms do use texts as a part of their service to notify customers of certain activity, it is important to familiarise yourself with what a legitimate message would look like and what would be deemed a suspect message. Banks and other trusted institutions would never ask you to disclose any security credentials, personal or financial information this way.

Fraudsters are also creating fake social media accounts purporting to be the legitimate firm and communicating with victims in this way. Again, it is important to understand how a firm will legitimately communicate with you.

Clone scammers selling fake investment products pocketed over £78 million from UK citizens in 2020, with victims losing £45,242 on average.

## What are the Red Flags?

There are several 'red flags' that you should be aware of that may indicate that the investment opportunity may be fraudulent, these include:

- Involvement of unregulated/ unlicensed investment professionals.
- Investment offers found on social media or through internet searches.
- The promise of guaranteed returns.
- Being targeted by an aggressive seller who may provide exaggerated or even false credentials.
- Tempting offers that sound 'too good to be true' including saying things like "everyone is buying it".
- The usage of language such as "risk-free" investment opportunities.
- The promises of great wealth and guaranteed returns.
- Pressure to invest right now, with sales needing to be concluded within a small time period to obtain the deal, including the use of couriers to bring or collect documents to your home.
- The usage of over-the-top or sensational reviews for investments.
- Cold calling / unsolicited emails seeking to obtain your personal information.
- Being asked to pay for investments by credit card, gift card, or sending money abroad or to a personal account.
- The investment is alleged to be 'protected' by the FCA rather than the FSCS.

## What to do If I have received contact from a scam?

Fraudsters will impersonate well known financial institutions with the intention of enticing you into sending money to them. These criminals are highly sophisticated and will create the impression of being genuine through means such as literature and websites.

Do not send any money as the likelihood is that any money sent will be lost.

Do not respond to any future communication from them including requests for personal information or money to be sent. Fraudsters will often try and use tactics to pressure you into sending information or money, such as advising that the offer is only available for a limited time to get you to make rash decisions or telling you there is little risk.

## Who do I contact if I have fallen victim?

### Speak to your bank

Any victim of investment fraud, including investment firm impersonation fraud, should speak to the bank they used to initiate the payment as soon as possible. The bank will have the full transaction details and may have the ability to notify the receiving bank of the fraud and potentially reclaim any fraudulently paid funds, depending on the circumstances of the transaction.

If the money sent cannot be reclaimed, the chief means of restitution which victims have reported benefiting from is the Contingent Reimbursement Model (CRM) Code for Authorised Push Payment (APP) scams. This is a voluntary code which a number of major banks have signed up to and sets out the circumstances of when a bank may compensate a customer who has fallen victim to a fraud, even where they authorised the payment.

It should be stressed that reimbursement is not a guarantee, and not all banks have signed up to the code; however, it is strongly recommended that victims who have suffered losses ask their bank to provide confirmation about whether the circumstances of the transaction(s) meet the grounds for reimbursement under the Authorised Push Payment Scam Code.

Before contacting the bank, you may also wish to refer to the following article for further information about reimbursement under the APP Scam Code: <https://www.which.co.uk/consumer-rights/advice/what-to-do-if-youre-the-victim-of-a-bank-transfer-app-scam> . The article also includes steps that you may take if your bank is not signed up to the APP Scam Code.

### Government fraud reporting organisations

Report your concerns to the FCA and Action Fraud for them to investigate further

FCA – Contact their consumer Helpline on 0800 111 6786 or report it online at <https://www.fca.org.uk/consumers/report-scam-us>

Action Fraud - [www.actionfraud.police.uk](http://www.actionfraud.police.uk) or 0300 123 2040.

Both the FCA and Action Fraud provide further information on Investment Scams and what action you can take to help prevent to help stop yourself becoming a victim of fraud.

To assist with their enquiries, try to provide the following information:

- How you were first made aware of the investment offer;
- If you were cold called, or further information was requested through routes such as internet comparison sites or social media;
- Copies of all correspondence with them that you can provide;
- Details of further communications you had with the fraudster;
- Details of any personal or confidential information you have sent to the fraudster, including any documents;
- Details of any money you have been asked to send. If so, the bank account details that money was sent to and what payments have been made;
- Confirmation of if you are willing for your contact details to be shared with the Police; and
- Any other details you think may be relevant.

## Other protective steps

If you think that the fraudsters have any of your personal details that could potentially be used for other fraudulent purposes, such as identity theft, then you may want to consider, for your own peace of mind, registering with the Credit Industry Fraud Avoidance Scheme. This enables financial organisations to be alerted to the fact that your details may have been compromised if any future account applications have been made in your name. They may respond by seeking additional identity information to ensure the application was genuine. Note that there is a small charge for this service. Further details can be found at [www.cifas.org.uk](http://www.cifas.org.uk).

It is also advisable to contact other financial organisations who you hold accounts with to let them know that your personal information has been obtained by scammers and you may be at a higher risk of fraud.

## Support agencies

Falling victim to fraud can have a huge emotional impact as well as being financially crippling. Victims can often feel embarrassed and don't want to tell people what's happened, even though they're not the ones to blame. As a result of what has happened, there is also an increased vulnerability to be targeted for further scam campaigns, such as fraud recovery scams suggesting they can help get any lost monies back.

There are a number of organisations available to offer their services to those who may be struggling with coming to terms with what has happened to them:

### Victim Support

An independent charity dedicated to supporting victims of crime and traumatic incidents in England and Wales. Can be contacted online or via their support line **0808 168 9111**.

### Think Jessica

A charity committed to protecting older people from fraud and scams. Visit: <https://www.thinkjessica.com/> to find out more about the more common methods used by fraudsters to target the older generation, such as telephone scams, postal fraud and doorstep crime.

### The Samaritans

Can be contacted any time of the day or night and can offer the chance to speak to someone who understands, on **116 123**.

### Citizens Advice

If a scam has left a victim struggling financially, they can contact Citizens Advice. They can speak to an adviser to help find a way forward, via their Adviceline. They are available 9am to 5pm Monday to Friday. If in England call **0800 144 8848**. If in Wales call **0800 702 2020**.

### Citizens Advice Scotland

Citizens Advice Scotland runs a dedicated online scams advice service which offers free, confidential, impartial advice. The Scams Action Service also undertakes scams prevention work to identify, tackle and raise awareness of online scams. To report an online scam and seek advice, call the free helpline on **0808 250 5050** or get in touch with via the webchat option. Advisers can be contacted via either of these ways from Monday to Friday from 9am to 5pm

### Victim Support Scotland

Free, confidential help from Victim Support Scotland for individuals affected by a scam. Consumers can: call the Victim Support Scotland Helpline for free on **0800 160 1985** (Mon - Fri 8am-8pm)

## Beware of Fraud Recovery Fraud

Whenever someone falls victim to an investment fraud, or any type of scam where money has been lost, a key consideration should be the risk of future 'fraud recovery fraud'.

Sadly, fraudsters retain the details of their previous victims and will often target them again in the future for another scam. Fraud recovery fraud is a particular type of scam where the fraudsters falsely claim to be pursuing the perpetrators for the money lost to the investment fraud. They may convincingly pose as a financial institution's fraud team, a government agency, the police or a law firm. Ultimately, they require payment of a fee or trick the victim into disclosing banking information, allegedly to secure the reimbursement of the original money which was lost; however, this is simply a second stage to the original fraud.

Victims of an investment fraud should be extremely cautious of any future contact from someone purporting to be able to reclaim funds lost to a scam, as it is highly unlikely that an unfamiliar person will legitimately contact victims for this reason. The default assumption should be that this contact is likely to be from a fraudster. The victim should question where their contact details have been obtained from and should ensure they are able to authenticate that the contact is genuine by obtaining contact details for the organisation from an independent and reliable source.

Victims may refer to the following article for additional information on red flags for fraud recovery fraud: <https://www.actionfraud.police.uk/a-z-of-fraud/fraud-recovery-fraud>

## Other Online Safety Tips

### Choose secure passwords/pass-phrases

A secure password helps keep you safe online. It also helps identify you when you log in as part of a multi-factor authentication process. The key to your password being secure is its strength and memorability. If you are concerned about the security for any of your online accounts, please update your passwords immediately.

- Never use your PIN, name in any form (first, middle, last, maiden or nickname) and / or date of birth as your password.
- Putting together a few words or phrases makes a longer password that can be easier to remember.
- Use a combination of letters, numbers and special characters. Using less common special characters will help strengthen your password.
- Change your password regularly. There's no set rule on this, but the more frequent the better.
- Always use different passwords on key accounts that hold financial or personal information. This way, even if one password is compromised, your other accounts will remain protected.

### Visiting websites

If you have not visited a website before, spend some time investigating the 'About us' section. If it contains poorly written English this could be a red flag. You can also check a site's authenticity by researching it using a respected search engine or an established customer or business review site.

## Protect your computer:

Many of us see these vital tasks as being a bit of a pain. Yet they are essential to keeping individual's safe online. Here's how:

Dos and Don'ts when using a computer	
Do	Don'ts
Keep your devices updated with the latest security patches and system software to guard against evolving threats. You can find out more from <a href="#">Microsoft†</a> and <a href="#">Apple†</a> .	Provide personal information into sites without first checking the FCA scam guidance <a href="https://www.fca.org.uk/scamsmart/warning-list">https://www.fca.org.uk/scamsmart/warning-list</a> .
Keep your antivirus software updated to reduce the risk of malicious software and viruses being installed on your computer.	Open attachments or download forms from an unsolicited email.
Your home Wi-Fi router is your online front door allowing your devices to connect to the internet, so it's really important that you keep this secure. One of the keyways to protect your router is to change the default admin password as the one set by the manufacturer can easily be discovered by attackers.	Assume that an advert on the internet is legitimate. Sadly, Google, Facebook/other social media platforms are used by fraudsters to target individuals.

## 3. Cannabis related investment restrictions

### 3.1 Introduction

The risks surrounding cannabis related investment activity are complex and management of them depend upon each firm's own risk appetite and risk-based approach. There is, however, some useful regulatory and industry guidance available that can help firms identify the risks that they want to manage. This guidance document has been written for TISA members to support identification of risks, mitigating controls available and how to approach defence against money laundering under the Proceeds of Crime Act 2002 (POCA) in relation to cannabis investments. The guidance does not provide answers to which risks are acceptable or not. In the document there will be references made to higher risk and lower risk. If a risk is unacceptable will be up to each user to define.

The guidance is focused on UK based investment managers. International firms may need to consider relevant laws and regulations in their areas of operation and where their clients are located. To support the reader in terms of definitions around cannabis types and thresholds, a supporting cannabis taxonomy can be found in Appendix 1.

### 3.2 UK Legislative and Regulatory Landscape

#### 3.2.1 Recreational Cannabis

Cannabis is a Class B drug and cultivation, possession or supply without a license is illegal. Under POCA, 'criminal property' is given a wide definition that includes property which represents a person's benefit from any conduct which would amount to a criminal offence in the UK if it were to occur in the UK. Profits made by an overseas recreational cannabis related business may therefore be regarded as 'criminal property', even if the firm is operating in a country where this business is legal. The Financial Conduct Authority (FCA) is the only government agency which has communicated a clear view on this subject, stating that "proceeds from recreational cannabis companies, even when they are located in those jurisdictions that have legalised it, are the proceeds of crime under POCA" (see <https://www.fca.org.uk/news/statements/listings-cannabis-related-businesses>).

A firm engaged in recreational cannabis cultivation is not admitted to listing on the Official List maintained by the FCA in its capacity as the UK Listings Authority in the UK.

#### 3.2.2 Medicinal Cannabis

Medicinal cannabis cultivation and supply is legal in the UK since 2018 but only when operating with appropriate Home Office licences. Any firm engaged in cannabis related activities that does not hold such licence is committing a criminal offence. Cannabis related wellness products, such as CBD oils, may also be sold in the UK where the THC content does not exceed 1 milligram. The legal position of purely UK-based medicinal cannabis companies, and cannabis oil companies, is therefore clear. With the appropriate Home Office licence, a UK-based medicinal cannabis company can be admitted to the Official List.

The situation for overseas firms is more complex if they *could* qualify for the UK licence requirements, but if they do not have such a licence in place. Proceeds from overseas medicinal cannabis business *may* constitute 'criminal property' for the purpose of POCA, as it is currently unclear whether the dual criminality transposition test includes where the company possesses a licence issued by an overseas medicines or pharmaceuticals licensing authority. UK firms could therefore technically be in breach of POCA if they invest in an overseas medicinal cannabis producer

or supplier or if they facilitate such investment activities (e.g. as a financial institution, broker or investment house engaged in a client relationship, or allowing clients to invest in related stock).

There is no clear guidance available to clarify where the line goes between investments related to cannabis stock *being* criminal property or where it *may* be considered criminal property. UK investors in listed cannabis production/distributions companies, based in countries that have fully legalised the production, sale and use of cannabis, may be breaching UK's anti-money laundering laws.

### 3.3 Risks of investing in cannabis related stocks

It is a principle under s340(3)(a) of POCA that property is criminal if it “constitutes a person’s benefit from criminal conduct or it represents such a benefit (in whole or part and whether directly or indirectly)”. In theory at least, if only a small proportion of a business activity was cultivating cannabis in breach of UK laws, then the whole business could be tainted. Even so, and it is necessary for a firm to consider its own risk appetite, one can outline different types of investment and scenarios that are likely to be higher or lower risk of prosecution, regulatory action, or reputational damage. For ease this has been broken down into two areas; the nature of decision-making/regulatory activity concerned and whether the investment has been made on a primary or secondary market.

#### 3.3.1 Active vs. passive decision-making

One aspect to consider is whether the investment is undertaken in an active way. When there is an active investment, there is a decision taken by a representative of the firm to invest in a particular security that may fall foul of POCA. In such situations it may be considered that such active decisions result in higher risks compared with passive strategies.

The same logic could be applied to third party funds. Where a Fund A is investing itself in a Fund B which contains a security that may fall foul of POCA the link between Fund A and the potential criminal activity concerned may also be considered somewhat removed. There will also be the question of whether full visibility of all the underlying constituents of a fund is available.

In the case of direct instructions from clients to invest in a security that may fall foul of POCA, i.e. an “execution only” instruction, the position appears unclear whether allowing a client to undertake an activity that may fall foul of POCA is any different to the firm itself making such an investment decision. Where the security is to be held in a firm’s custody the risks are likely to be higher than where custodianship is not provided.

The position regarding corporate actions is again likely to be nuanced due to the varying actions that can apply. However, it again appears reasonable to consider that if actively participating in a corporate action that results in exposure to a cannabis related security runs a higher risk than simply benefiting from a corporate action that requires no positive action.

#### 3.3.2 Primary market or secondary market investment

Whilst there is again no official guidance in this space, conceptually where investing directly in a security that may fall foul of POCA the risks are likely to be higher investing in the primary market than on the secondary market. Even though it can be argued that in both situations s327 and s328 of POCA applies it appears reasonable to consider that providing monies directly (in effect) to an entity that is falling foul of POCA is a higher risk than simply trading in the securities of the company on the secondary market and seeking to make profits from supply/demand factors.

### 3.4 Defence against Money Laundering

Legal commentators and member firms have proposed or reported establishing a cannabis investment strategy on the basis of one or a combination of the following defences and rationales.

Due to the lack of previous prosecutions for cannabis related investment activities, these proposed defences and rationales are untested and their inclusion below is not intended to provide assurance that they would provide a valid defence; firms should ensure they obtain proper legal advice before relying on any defence referenced below.

#### 3.4.1 Adequate consideration defence

POCA 329(2)(c) contains a defence to the section 329 offence of acquiring, using or having possession of criminal property where the property was acquired for adequate consideration. There appears to be a reasonable argument that the purchase of a cannabis related security for its fair value on a regulated market meets these requirements.

It could be argued that there is greater risk that the subsequent receipt of dividends or coupons from the issuer of the security would not be covered by this defence, either because of the view that this criminal property (the dividend/coupon payment) is distinct from the acquisition transaction and the payments have not been purchased for adequate consideration and/or due to the payment being received directly from a cannabis related company and therefore being at higher risk of being construed as criminal property. An untested response to this concern is that there is no such distinction between the transactions because the acquisition of the security includes acquiring the rights to benefit from it and these rights are a fundamental consideration when assessing its value.

A further potential issue with relying solely on the adequate consideration defence is that it is not available for the section 328 of entering into or becoming concerned in an arrangement which facilitates the acquisition, retention, use or control of criminal property by another person.

#### 3.4.2 Production under license

Another challenging area is the ambiguity surrounding the equivalence test for overseas licensing regimes. Under UK law, cannabis related activities would be deemed to be an offence if they took place in the UK. If the activities are licenced in the relevant country, they could be deemed equivalently licenced. However, there is only acknowledged equivalence for those that have explicitly applied for a UK licence.

Section 7 of the Misuse of Drugs Act 1971 permits the cultivation, production, supply and possession of cannabis if done under license or authority provided by the Secretary of State. The sale of cannabis under another country's licensing regime could therefore be argued to be equivalent and permissible. This is potentially more likely to be the case if the license is for medicinal rather than recreational purposes, but the argument has been made that there is scope for both as there is no judicial precedent for this test.

#### 3.4.3 Suspicious Activity Reports

Legal commentators and member firms have reported making use of the suspicious activity reporting regime as a defence when undertaken cannabis related investment activity, either to request a defence against money laundering or as a disclosure after an investment has come to light. The making of an authorised disclosure is a defence which is available for all three money laundering offences under POCA (s327(2), s328(2) and s329(2)) and it therefore appears to be a relatively common risk mitigation strategy reported by firms participating in cannabis investment activity.

The establishment of a SAR process for cannabis related investment transactions may be burdensome for the firm's nominated officer and internal staff, as each disclosure must relate to

specific activity/transaction(s). Firms may take a view on which types of activities warrant disclosure in this way.

#### **3.4.4 De minimis principle**

Notwithstanding section 340(3) of POCA (as referenced above), some firms may adopt an approach which incorporates materiality thresholds for practical reasons and as an application of the de minimis principle. For example, a firm may take the view that the de minimis principle renders investment into a company which only generates less than x.x% of its revenue from cannabis related activities or a fund with a large number of other portfolio constituents as presenting low legal or regulatory risk.

There are no known specific materiality thresholds for the purposes of cannabis related investment activities which have a rationale or basis in UK law.

#### **3.4.5 Placing reliance on FCA vetting**

It is noted that the FCA has adopted a policy of refusing to admit recreational cannabis companies to the Official List and assessing medicinal cannabis companies on a case by case basis. The FCA guidance issued in relation to firms allowed, or not allowed, onto the Official list, states that only firms where the FCA are “satisfied POCA does not apply and they otherwise satisfy the criteria for listing” will be granted admitted to the Official List, thus suggesting that investments in these firms would not constitute an offence under POCA.

#### **3.4.6 Pragmatic/purposive approach**

Some firms may have chosen to take a pragmatic approach based on the view that officially traded cannabis related investment activity is theoretically criminalised due to a quirk of the law rather than intentional public policy. As a result, there may be a perceived low likelihood of prosecution or regulatory action and some firms have chosen to impose limited or no restrictions on the cannabis related investment activity which it participates in.

The adoption of this approach may stem from considerations such as the lack of previous prosecutions, absence of definitive or consistent comment from government bodies on this topic, perceived public mood shifting towards tolerance (particularly in relation to medicinal usage), the high volume of public participation in cannabis related investment activity and the view that any prosecution is unlikely to be in the public interest. However, any firms taking this view should consider whether there are any implications from the FCA’s statements on cannabis related investments.

### **3.5 Navigating a Risk Based Approach**

With the legal and regulatory picture around investment in cannabis related stock remaining unclear, many financial institutions navigate a carefully considered risk-based approach to cannabis investment. There are many nuances in the potential type of exposure to cannabis investment which will impact the level of risk faced.

A firm may choose to respond to this topic in accordance with its risk-based approach in the following ways:

- Carrying out an assessment of the types of investment activity the firm engages in where there may be exposure to cannabis, whether as part of its AML risk assessment, a standalone risk assessment process or via another method. This may include an analysis of the firm’s existing investment holdings, its fund or investment product objectives, the

markets or jurisdictions which it invests in, its investment teams' strategies or its client types (where clients trade in individual securities on their own account).

- Development of a 'house view' on the topic in light of the available legal and regulatory guidance and any relevant reputational considerations, including: forming a judgment on what is or is not permitted or is at a higher risk of being deemed illegal; any risk management processes or available defences, such as when a SAR should be filed; whether to impose any firm-wide prohibitions; and the use of any materiality thresholds. Appropriate escalation and approval of the house view by senior management, if relevant.
- Incorporation of the house view into company-wide policies, procedures and training, including general education on the issue and any obligations which staff have, such as complying with a ban on specific activities or submitting internal SARs.
- Incorporation of the topic into the firm's external SAR reporting procedures.
- The use of internal or externally sourced data on securities where there is exposure to cannabis-related activities and using this data for pre-trade, post-trade or periodic screening against investment holdings.
- Agreement on the way in which the firm's house view will be communicated to clients, if relevant, including in any terms and conditions or due diligence questionnaire responses.
- Consideration of any due diligence which should be performed on any key third party relationships or relevant contractual provisions inserted; for example, where investment management is delegated.
- Ongoing monitoring of the evolving legal and regulatory picture around this topic, including output from government bodies, trade associations and legal bulletins.

### 3.5.1 Potential risk scale

Risk scale	Security type	Cannabis related activity	Transaction type	Materiality	Strategy
	Equity and bonds issued by cannabis related company	Recreational cannabis cultivation and supply	IPOs/lending/purchase of security on the primary market	All/high proportion of issuer's revenue generated by cannabis related activity	
	Third party fund designed to gain exposure to cannabis securities, including recreational cannabis	Overseas company producing and supplying CBD products with THC content exceeding 1 milligram	Receipt of dividends/coupons	Non-cannabis related company with a subsidiary or a significant interest in a cannabis related company. Revenue generated by cannabis related activity above firm's de minimis threshold.	Active
Higher	Third party fund with a minimal holding in a cannabis related company	Overseas company producing and supplying CBD products with THC content not exceeding 1 milligram	Purchase or sale of security on the secondary market	Non-cannabis related company with a subsidiary or a significant interest in a cannabis related company. Revenue generated by cannabis related activity below firm's de minimis threshold.	Passive/ trackers
	Derivatives trading relating to cannabis related company	Overseas company cultivating and supplying medicinal cannabis		Non-cannabis related company with a minority interest in a cannabis related company. Revenue generated by cannabis related activity below de minimis threshold.	
Lower	Shares of firms admitted to the Official List UK	UK company carrying out lawful cannabis related activity under license/below THC thresholds			

### 3.6 Investment restriction support (data, lists and screening)

As part of a firm's risk-based approach consideration can be made to whether a screening solution of cannabis related securities in their client portfolios is a control that would help mitigate relevant risks. To support this process, data in the form of cannabis related issuers and securities are available from several market data and specialist vendors. These lists should ideally provide a granular view on the type of security, classification, associated reference data, listing information and the type of cannabis related activity affecting the issuer of the security.

Data on cannabis related issuers and securities is mainly used for:

- Pre-trade clearance to restrict trading of the restricted securities;
- Post-trade audit to ensure no restricted security has been traded;
- Issuer or counterparty profiling for flagging of risks such as money laundering risk.

The handling of cannabis related securities varies across the settlement and asset servicing chain; some service providers will publish their own guidance and lists which investment firms would need

to incorporate into their investment restrictions process; this is typically done within the pre-trade clearance workflow. Revisions to these restriction lists are quite common with newly identified securities frequently added to the lists. Upon restrictions becoming effective, investment firms holding the restricted securities in custody may be able to continue holding the securities, generally without a specific deadline for divestment or transfer. They will, however, not be able to have new trades in the restricted securities settled or have new trades transferred into custody.

Firms may look to maintain a continual monitoring process with several datasets potentially forming the universal view on the securities to restricted. Once established this view should be centralised so that front office functions, compliance, legal, risk and operations can have a synchronised data view. However, as firms are required to conduct their own risk-based assessment, it is possible that some securities could be excepted from restriction and therefore traded on this policy-based exemption; in these cases, firms should maintain a register with clear details on the exemption and related securities.

## Appendix 1 – Taxonomy

Cannabis belongs to a genus of flowering plants known as Cannabaceae; the exact number of species in the genus is disputed but three species are widely recognised: *Cannabis sativa*, *Cannabis indica*, and *Cannabis ruderalis*; *C. ruderalis* may be included within *C. sativa*; all three may be treated as subspecies of a single species, *C. sativa*; or *C. sativa* may be accepted as a single undivided species.

Various types of Cannabis have been described, and variously classified as species, subspecies, or varieties; dependant on the chemical properties of the strains, these can be summarised as:

- **Cannabis** (also known as **Marijuana**), which includes plants cultivated for drug production, described as high-intoxicant or drug types; these strains contain high levels of Delta-9-Tetrahydrocannabinol (THC), the psychoactive component which produces the ‘high’ that is experienced by users of Cannabis. Cannabis is mainly grown and used for medical or recreational purposes.
- **Hemp**, which includes plants cultivated for fibre and seed production, described as low-intoxicant, non-drug, or fibre types; generally associated with a low THC component (less than 0.3%) and material quantities of Cannabidiol (CBD), which is a non-psychoactive cannabis compound. Hemp is mainly grown and used for industrial purposes.
- Other forms include those that are classified as escaped, hybridised, or wild forms of either of the above types.
- The uses of Cannabis can be classified into three distinct categories: **Medical Cannabis** use is based on the plant or chemical compounds contained within Cannabis to treat a range of diseases and conditions; essentially the product is the same as for recreational use but taken for medical purposes – with the main difference being that medical cannabis has a higher CBD content than recreational cannabis.
- **Recreational Cannabis** use is based on seeking the psychoactive effects of cannabis for pleasure. Users can become dependent on or addicted to cannabis, just as someone can with alcohol and tobacco. A person is deemed to be dependent on marijuana when they have withdrawal symptoms; and is considered addicted to the drug when the drug use interferes with aspects of their and they cannot stop the use.
- **Industrial Hemp** is used to make a variety of commercial and industrial products, including rope, textiles, clothing, shoes, food, paper, bioplastics, insulation, and biofuel.

## Appendix 2– Useful links

<https://www.fca.org.uk/news/statements/listings-cannabis-related-businesses>

<https://www.gov.uk/guidance/controlled-drugs-industrial-hemp>

<https://www.fca.org.uk/publication/ukla/fca-tn-104.1.pdf>

[2021/06/28 UK Life Sciences and Healthcare Newsletter | Medicinal Cannabis in the UK: Fund Structuring, Investment and Listing Considerations \(dechert.com\)](#)

[More than puff and smoke: UK poised for cannabis boom but mind the POCA position - Lexology](#)

[Cannabis and the UK investor – two years on | Criminal Law Blog | Kingsley Napley](#)

[High return, high risk? AML risks arising from investment in the cannabis industry - Lexology](#)

[Green Signal! Proceeds with caution - 2 Bedford Row](#)

[A Green Light for Business? The Rescheduling of Cannabis-Derived Medicinal Products and the UK's Anti-Money Laundering Regime – BCL Solicitors LLP](#)

[Turning over a new leaf: Cannabis, UK investors and the Proceeds of Crime Act 2002 - Macfarlanes](#)

[Cross-Border Cannabis Investment: Managing Money Laundering Risk | White & Case LLP \(whitecase.com\)](#)

## 4. Anti- Money Laundering Transaction Monitoring

### 4.1 What is transaction monitoring?

The purpose of this section of the guide, is to provide guidance and good practice examples for TISA members in relation to financial crime related transaction monitoring, other than in respect of market abuse. Its aim is to help support such institutions in developing a framework to meet the requirements for ongoing monitoring enshrined in the FATF recommendations and Money Laundering Regulations.

Due to the scale, nature and complexity of TISA members and their different business lines it is of course inappropriate and practically impossible to describe what particular monitoring may be required in any given situation. Firms should take their own risk-based approach (RBA) using if wished this guidance as a tool to create an overall effective framework.

For the purposes of this paper, transaction monitoring (TM) is defined in line with UK legislation, namely, it is the scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, the customer's business and risk profile.

At a high level, TM involves identifying changes in behaviour (including anticipated behaviour) in respect of a client. This supports both compliance with money laundering legislation and identifying fraudulent activity. A firm may also wish to use TM to capture other events that are relevant to anti financial crime considerations – these may be internal or external events. Taking this wider approach is likely to result in a stronger monitoring framework.

TM may be wholly manual in nature (people) or “automated” with then some manual involvement typically being required.

### 4.2 Risk based approach

It is the responsibility of each individual firm to take appropriate steps to assess the money laundering and terrorist financing risks faced by their business and establish proportionate policies, procedures and controls. The business risk assessment required under the Money Laundering Regulations should form the basis of a firm's RBA to transaction monitoring.

The nature of monitoring will vary considerably across firms depending on the nature, size and complexity of their business, as well as the risks to which they are exposed. Industry guidance requires the consideration of risk factors such as customers; geographic area of operation; products or services offered; transactions; and delivery channels. When assessing the risks that are relevant to their approach to monitoring customer activity, TISA members should consider factors such as:

- The nature of relationships with clients, for example the use of introducers and the level of relationship management;
- The extent to which clients can get access to their funds and the method(s) by which that can occur; and
- The ease with which clients can transact or make changes to their portfolio.

These factors are covered further in Section [4].

Following completion of an assessment of their specific risks, firms should adjust the intensity and frequency of monitoring as required:

- In situations of elevated risk, it is probable that more frequent or intensive TM should occur;

- Conversely, in situations of low risk, more limited TM may be deemed satisfactory.

In line with regulation, higher risk client relationships require enhanced ongoing monitoring. The approach to TM for different risks should be documented.

The approach to TM should remain current and be flexible to adapt to changes in risk. Firms should consider a regular refresh based on a defined minimum periodicity or trigger changes in both the:

- External risk environment - for example obtaining intelligence on the evolution of a new criminal typology impacting investment products or an update of the UK National Risk Assessment of Money Laundering<sup>1</sup>; and
- Internal risk environment – for example introduction of a new online only product or expansion of operations to a new jurisdiction.

<sup>1</sup>[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/945411/NRA\\_2020\\_v1.2\\_FOR\\_PUBLICATION.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf)

### 4.3 Manual vs. automated monitoring

When determining a monitoring approach, firms should consider whether they will conduct TM manually, undertake automated TM or a combination of both. Where a high volume of transactional activity is expected, it is likely that an automated system will be required due to the operational challenges in appropriately reviewing large-scale client activity on a timely basis.

Regardless of which approach to monitoring is used, appropriate training should be delivered to all staff who manage clients and their transactions or perform support functions to allow them to recognise what is unusual activity and maintain awareness of what to remain vigilant for.

While this guidance does not cover the maintenance of keeping customer information up to date, it is also important to remember that any approach to monitoring is only as effective as the quality of the underlying customer information. If this information is incomplete or out of date, it may be more difficult to identify unusual or ultimately suspicious behaviour.

When considering an automated system, firms should take note of the questions included in the JMLSG guidance to aid their selection process<sup>2</sup>. In addition, as many solutions were primarily developed for banks or credit institutions which represent a differing risk profile, TISA members will need to assess whether the system typologies are relevant for their products and client transactional activity. Where an automated system is used, firms should ensure they regularly review rule effectiveness and have sufficient resources to manage alerts.

<sup>2</sup> <https://jmlsg.org.uk/guidance/current-guidance/>

### 4.4 Nature of relationship

Considering and understanding the different types of relationship can help identify potential “red flags”. Having an understanding of the expected behaviours of a client and the transactions arising and then for variances against these will help identify potentially suspicious transactions. Monitoring for transactions that are not in keeping with the life expectancy of the product is relevant to most arrangements, be it disinvestment in a short period of time or the unexpected repayment of credit product early.

#### **4.4.1 Relationship Managed**

It is recommended that those clients who are relationship managed should be monitored by the relationship manager. This is because the relationship manager should have the greatest understanding of the client and their expected behaviours. Clients who have incoming and outgoing transfers, for example, whether of cash, investments or other assets, should be reviewed by the relationship manager or their delegate prior or as soon as is reasonably practicable after the transaction, dependent on the firm's risk-based approach.

Dependent on the firm's maturity, the relationship manager could provide assurance to the firm on a regular basis, that they are conducting appropriate and effective oversight of clients and nothing suspicious has been identified, if no reports have been escalated to the financial crime team for investigation. Likewise, a positive return should also be confirmed.

#### **4.4.2 Direct clients**

For those relationships which are not relationship managed, or introduced by an entity which is not regulated, present their own challenges. Firms should consider the risk related to the extent to which the business relationship is conducted on a non face-to-face basis. The Joint Money Laundering Steering Group (JMLSG) suggests key elements of any transaction monitoring system are having up-to-date customer information, on the basis of which it will be possible to spot the unusual and asking pertinent questions to elicit the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious.

#### **4.4.3 Online Only Customers**

Online customers are unlikely to have met an employee of the firm which creates additional issues (e.g., customer impersonation/identity theft). In such cases since there is less likely to be a detailed understanding of the client's background and aspirations etc monitoring is likely to revolve around changes in behaviours and activities out of pattern for clients who use the particular product.

Transaction monitoring may therefore include the monitoring for large sums over a set threshold; whilst being a little presumptuous, firms would naturally expect clients who wish to invest large sums to be introduced by advisors or wealth managers potentially. Similarly, when a PEP has been identified, consideration should be conducted to ascertain if there are ulterior motives to take a direct to client route. These may include further investigation into the source of funds for example.

Due to the remote nature of online customer relationships, close monitoring of transactions could be conducted, requesting reasons for an increase in amounts invested. Firms could establish the rationale behind any unexpected ad hoc payments made or requested by the customer. Further information is also provided in Section [8] below.

#### **4.4.4 Telephone/email**

The ability to transact by email and telephone presents its own risks in respect of how a firm can be confident they are dealing with the client and the request is legitimate. Similar monitoring could be conducted to that of the online route, including monitoring behaviours and for example, considering sudden withdrawal requests into new bank accounts. To combat and identify possible activity of concern, a firm's monitoring programme may include the review of recent account/policy closures following an update of a policy marked 'Gone Away'. Accounts identified has high risk for fraud should be monitored. This could be in 'real time' in that any activity conducted on specific policies is escalated for approval where the client's status is for example set to 'Gone Away'/'Mail Returned.

#### 4.4.5 Advisory firms

Whilst some firms may have clients who are introduced by an advisor firm, other firms may have clients who are advisers (under the “agent as client rule”). Clients introduced by advisors should be monitored in a similar manner as to direct clients, with the difference being that the adviser could be engaged to understand the reasons for transactions on behalf of the client, on the proviso there is no tipping off risk present in the scenario. Where the adviser is the client, similar engagement could be conducted. However, it is essential that there is an understanding how the advisor will use the product and the expected scale of business. The first line business, who has the relationship with the advisor, could implement a monitoring regime based on identifying unexpected transactional behaviours. Engaging with the advisor is important and key understanding of underlying investors transactional behaviours is vital.

How to monitor customer activity is described in more detail in Section [5].

#### 4.5 Monitoring customer activity

A firm’s monitoring framework should be based upon a firm’s own assessment of client risk at the initial onboarding stage. However, firms should subsequently be considering the ongoing review of specific risk factors which represent those areas of risk which are applicable to the firm. These areas for consideration can be categorised as:

- the initial client onboarding process and assessment of the client risk type;
- transactional;
- client behavioural changes;
- identified negative media; or
- contact from external parties (e.g., regulators or government bodies)

The below sub-sections contain a summary of each of the areas of consideration. Examples of potential monitoring activities are shown in the table in section 8.

##### 4.5.1 Transactional activity

Ongoing monitoring of transactions is key to identifying unusual activity and should be performed throughout the lifecycle of the client relationship. By performing ongoing monitoring, a firm is better placed to continually know and understand who the customer is and to re-assess any risk factors that exist by maintaining the client relationship. Monitoring can include several factors, but typically will incorporate the following elements:

- source of funds;
- specific monetary thresholds;
- AML geographical risk assessment requirements;
- destination or receipt of funds;
- frequency of transactions compared to value;
- complex or unusual pattern of transactions; and
- parties to a transaction

Transactional monitoring can be conducted at an individual client level comparing possible changes over a specific period of time, or by examining a group of similar clients (peer group).

#### 4.5.2 Behavioural activity

A firm's monitoring programme should not only focus on the transactions conducted by a client, but also regularly examine other client behaviour.

Behavioural monitoring should be used to identify possible changes which could signify unusual or potentially suspicious behaviour which includes but is not limited to the following:

- amendments to static data within a short period of time;
- high risk factor static data changes;
- reactivation of dormant accounts;
- failure to complete telephone security successfully;
- second party fraud attempts - possible evidence of vulnerability;
- victim of fraud with another institution;
- requests for information from third parties and or law enforcement;
- customer's use of the chosen product and how this behaviour compares to other clients; and
- accessing of online accounts outside of a known geographical location of the client.

Behavioural monitoring should be used in conjunction with the transactional monitoring component to build a more informed picture of the client and any associated risks.

#### 4.5.3 Negative media and other sources

Alongside the transactional and behavioural elements, firms should also consider the use of additional sources such as:

- negative media;
- fraud screening (e.g., CIFAS); and
- monitoring of registers for deceased individuals.

The use of negative media and or other sources can provide a firm with an additional proactive element to an overall monitoring programme. Screening of this nature can also support a broader array of topics including fraud prevention and anti-bribery and corruption programmes managed by the firm. In all cases, a firm will need to consider the parameters that will be set to perform such searches to avoid unnecessary false alerts. As a minimum a firm may wish to consider:

- the types of clients and the particular risks that they may represent, that will be subject to screening, comparing to AML typologies applicable to the firm where these are available;
- how such screening will be performed (e.g., automated versus manual) and if a specialist vendor is required;
- which function will review the output of any screening performed; and
- determine the action to be taken when an alert is identified (e.g. suspicious activity reporting, possible exiting of a client relationship, system markers and enhanced monitoring etc.).

#### 4.5.4 Contact from external parties

Formal requests for client information can take a number of forms including:

- court orders;
- production orders; and
- bankruptcy.

Court Orders can be raised for a variety of reasons and they do not always relate to a financial crime concern. Many orders are for civil matters and can be handled accordingly.

However, any order that insinuates criminal activity, police involvement or makes specific reference to Proceeds of Crime Act, should act as an immediate prompt for specific monitoring to be conducted on the client account in question.

#### 4.6 Periodic review of TM framework.

As part of each firm's business wide risk event, the transaction monitoring framework should be subject to appropriately frequent review in order that it continues to meet your business risk profile, and should consider various factors, for example have any of the following have occurred since the last review?

- Material changes to Regulations or Industry Guidance;
- Peer firms subject to Significant adverse findings or fines for money laundering failures;
- Negative findings identified in any independent monitoring;
- Changes to internal systems or controls;
- Launches of any new products or services, or changes to your client demographic.

And, in terms of the firm's monitoring controls and processes:

- Where thresholds or alert rules apply, are they still appropriate for the current products, client types and firm risk appetite?
- When was the last time the framework was subjected to end-to-end testing to ensure it was working as expected?
- Where processes rely on human intervention, how well documented is that process and are staff adequately trained to perform them?

This is not an exhaustive list but demonstrates that there are a wide range of considerations to make the review successful.

Upon completing such a review, the outcome and any decisions must be fully documented and retained for future reference.

#### **4.7 Sources and further reading**

- JMLSG Part 1 – 5.7 Monitoring Customer Activity;
- UK National AML Risk Assessment;
- FCA Financial Crime Guide; and
- FATF Recommendations.

## 4.8 Transaction Monitoring – Practical examples

The below tables contain examples of transaction monitoring activities / actions that TISA members may wish to consider for each of the monitoring areas outlined in Section 5. Members must remain aware that these are only examples and do not on their own represent an ‘off-the-shelf’ approach or recommended framework. Monitoring should be based on a firm’s business risk assessment and aligned to members own risk-based approach using either automated or manual monitoring. Equally, thresholds should be determined based on expected client behaviours – remember that the aim of the monitoring is to pinpoint something outside the normal of typical client behaviour. Finally, monitoring activities may be tailored to the risk rating of clients, for example, a value threshold for cash withdrawal may be lower for higher risk customers.

### 4.8.1 Transactional Activity

Monitoring theme	Example monitoring activities	Automated / Manual
<b>Specific monetary thresholds</b>	<ul style="list-style-type: none"> <li>• Ad-hoc cash withdrawals above a percentage of value other than on death.</li> <li>• Ad-hoc cash withdrawals above a value threshold dependent upon a firm’s risk appetite in the early stages of a relationship</li> </ul>	<ul style="list-style-type: none"> <li>• Automated</li> <li>• Manual</li> </ul>
<b>AML geographical risk assessment requirements</b>	<ul style="list-style-type: none"> <li>• Ad-hoc cash withdrawals above percentage or value thresholds to high or very high-risk countries.</li> <li>• Occasional transactions involving jurisdictions on high risk third country list, if during CDD the client was not identified as established in the country.</li> <li>• Additional investments are made a long distance from where the account was originally opened and/or the address registered on the account.</li> </ul>	<ul style="list-style-type: none"> <li>• Automated</li> </ul>
<b>Destination or receipt of funds</b>	<ul style="list-style-type: none"> <li>• Payment attempts to accounts other than nominated account or where bank account is not verified.</li> <li>• Overseas payments - in or out - from non-UK sort codes or other non-standard payment types.</li> <li>• Conflict of interest checks on lending investment.</li> </ul>	<ul style="list-style-type: none"> <li>• Automated</li> <li>• Manual</li> </ul>
<b>Frequency of transactions compared to value</b>	<ul style="list-style-type: none"> <li>• Series of connected transactions that appear to be structured to avoid hitting</li> </ul>	<ul style="list-style-type: none"> <li>• Automated</li> <li>• Manual</li> </ul>



	<p>value thresholds.</p> <ul style="list-style-type: none"> <li>• Cumulative thresholds on investment.</li> </ul>	
<b>Complex or unusual pattern of transactions</b>	<ul style="list-style-type: none"> <li>• Money paid in and then immediately taken out if not appropriate for the product.</li> <li>• Cash receipts and payments out of equal amounts (within 5% variance) in a 3 month period.</li> <li>• Transfers in received and then transferred out of equal holding in a 3 month period.</li> <li>• Routing a payment in a convoluted direction rather than direct to nominated bank account.</li> <li>• Unexpectedly taking money out of a product early, particularly a fixed term product.</li> </ul>	<ul style="list-style-type: none"> <li>• Automated</li> <li>• Manual</li> </ul>
<b>Parties to a transaction</b>	<ul style="list-style-type: none"> <li>• Third party payments in or out of high value or volume.</li> <li>• Large number of payments from different investor accounts into single bank accounts.</li> <li>• Unexplained payments from a third party.</li> <li>• Payments to employee bank accounts.</li> <li>• Payments from unconnected client accounts to the same bank sort code / account number.</li> </ul>	<ul style="list-style-type: none"> <li>• Automated</li> <li>• Manual</li> </ul>
<b>Unexpected transactions</b>	<ul style="list-style-type: none"> <li>• Ad-hoc withdrawals made within 6 months of an investment.</li> <li>• Rapid exit of investment product.</li> <li>• Full surrenders/ account/ service closures within 2 years of commencement other than on death.</li> </ul>	<ul style="list-style-type: none"> <li>• Automated</li> <li>• Manual</li> </ul>
<b>Unexpected account activity</b>	<ul style="list-style-type: none"> <li>• Further investment or withdrawals at values inconsistent with customer's prior</li> </ul>	<ul style="list-style-type: none"> <li>• Automated</li> <li>• Manual through</li> </ul>



	<p>account activity.</p> <ul style="list-style-type: none"> <li>• Payments lodged into an existing product above that indicated at account opening or out of line with evidenced source of funds.</li> </ul>	<p>training to report unexpected transactions</p>
--	--	---

#### 4.8.2 Behavioural Activity

Monitoring theme	Example monitoring activities	Automated / Manual
<b>Amendments to static data within a short period of time</b>	<ul style="list-style-type: none"> <li>• Postal or e-address mail change with subsequent new regular or ad-hoc withdrawals within 3 months.</li> <li>• Changes to one or more of the following within 30 days: i) address; ii) online access; iii) new device connected to existing online access; iv) new phone number; v) new email address; or vi) new bank mandate.</li> </ul>	<ul style="list-style-type: none"> <li>• Automated</li> <li>• Manual</li> </ul>
<b>High risk factor static data changes</b>	<ul style="list-style-type: none"> <li>• Change to bank mandate, particularly where follows a static data change that may result in redirection of confirmation or approval.</li> <li>• Address changes involving a move to a high risk or previously unconnected country.</li> <li>• Address change to a potentially higher risk scenario such as a prison address or a PO Box.</li> </ul>	<ul style="list-style-type: none"> <li>• Automated</li> <li>• Manual</li> </ul>
<b>Reactivation of dormant accounts</b>	<ul style="list-style-type: none"> <li>• Dormant accounts suddenly transacting in high volumes over a short period of time.</li> <li>• Changes to one or more of the following within 30 days prior to reactivation: i) address; ii) online access; iii) new device connected to existing online access; iv) new phone number; v) new email address; or vi) new bank mandate.</li> </ul>	<ul style="list-style-type: none"> <li>• Automated</li> <li>• Manual</li> </ul>
<b>Failure to complete security</b>	<ul style="list-style-type: none"> <li>• Multiple failures to authenticate online</li> </ul>	<ul style="list-style-type: none"> <li>• Manual</li> </ul>

<b>checks successfully</b>	<p>leading to the addition of a marker or a block on access until reaccreditation.</p> <ul style="list-style-type: none"> <li>Failed phone authentication resulting in the issue of a security concern letter to a trusted address - where possible place marker against account to track any further failed telephone security checks.</li> </ul>	<ul style="list-style-type: none"> <li>Automated (online)</li> </ul>
<b>Second party fraud attempts</b>	<ul style="list-style-type: none"> <li>Known individual attempting to pass themselves off as the account holder – may be an indicator of vulnerability.</li> </ul>	<ul style="list-style-type: none"> <li>Manual</li> </ul>
<b>Victim of fraud with another institution</b>	<ul style="list-style-type: none"> <li>Bank account compromised - informed by customer or banking provider.</li> <li>Changes to static data.</li> </ul>	<ul style="list-style-type: none"> <li>Automated</li> <li>Manual</li> </ul>
<b>Requests for information from third parties and or law enforcement</b>	<ul style="list-style-type: none"> <li>Court orders or freezing orders.</li> <li>Subject access / witness statement request from HMRC Investigation Officer Organised Crime Operations</li> </ul>	<ul style="list-style-type: none"> <li>Manual</li> </ul>
<b>Accessing of online accounts outside of a known geographical location of the client</b>	<ul style="list-style-type: none"> <li>Monitoring of accounts for which the IP address accessing online services differs geographically from the registered address for correspondence.</li> <li>Device ID or geo-location on mobile access differs from known device or location of the customer.</li> </ul>	<ul style="list-style-type: none"> <li>Automated</li> </ul>
<b>Identification of negative media</b>	<ul style="list-style-type: none"> <li>Review activity of the client to determine if behaviour sits outside the firm's risk appetite</li> <li>Identification of source of funds to determine if proceeds of crime could be held</li> </ul>	<ul style="list-style-type: none"> <li>Automated</li> <li>Manual</li> </ul>

- FATF Typology reports <https://eurasiangroup.org/en/fatf-typology-reports>



## 5 Anti Bribery & Corruption (ABC) Guide

### 5.1 Introduction

Bribery and corruption are among the most common risks facing global organisations in all sectors, and penalties for failure are increasing. The UK Bribery Act has been in force since 2010 and global anti-bribery legislation continues to be strengthened, requiring improved internal controls to ensure compliance.

The majority of financial services organisations have well established procedures for preventing money laundering, terrorist financing and fraud. This guide will facilitate organisations' implementation of sound anti-bribery and corruption systems and controls. Financial crime in all forms remains a continuous area of vulnerability for organisations and much of the work required for an effective control system is common to all areas.

Companies will design their anti-bribery programme according to their circumstances (internal and external environment) and risk appetite. This guide offers a template for TISA members to ensure their policies and procedures follow best practice and provides a basis for comparison. Companies may wish to incorporate the template/assessment into their broader risk assurance activities.

### 5.2 ABC Framework

#### 5.2.1 Governance and Management Information

The objective is to establish and maintain an ABC programme that sets the standards for appropriate behaviour and ethical business practices.

#### 5.2.2 Culture / tone from the top

Commitment by the board and senior management to a policy of prohibition of ABC is the bedrock for countering ABC. The board and senior management should make a public commitment (website) to prohibiting bribery and corruption in the company's operations.

The board should commit to supporting the implementation of an ABC programme, by:

1. Providing oversight; and
2. Assigning a senior manager to implement the programme.

In doing so, the board should inform themselves of the risks and appropriate policies and procedures required; a record of this should be documented within the board minutes.

#### 5.2.3 Senior Management sponsorship

Senior Management (and the SMF responsible) should give substance to its zero-tolerance policy by supporting the implementation of an ABC programme by:

- A commitment to support the implementation of the programme is made formally with written approval by the board;



- Management designing, reviewing and improving policies and procedures based on regular risk assessments; and
- The board providing oversight to the ABC programme and assigning senior manager clear responsibility for its implementation via their statement of responsibilities.

In a small company the distinction between governance and management roles may need to be modified, with owners or executive directors taking a more hands-on role in the company's anti-bribery activities.

#### **5.2.4 Roles & responsibilities**

##### **Chief Executive Officer:**

Responsibility for ensuring the corporate integrity culture and implementation of the anti-bribery programme should be with the CEO.

The CEO should be accountable to the board and should ensure that responsibilities are assigned across the company for implementing the programme.

The CEO should provide tone from the top and it should be the aim of the CEO and senior management to embed the programme in the company such that every manager and employee accepts a personal commitment to the programme and its effective implementation.

##### **Compliance Officer:**

The CO is responsible for the day-to-day operation of compliance. In large companies, functional responsibility for the programme is commonly assigned to a CO but can often be placed in legal and occasionally in internal audit or risk management. The CO must consider how best to build a team structure to launch, implement and monitor ABC.

In a large company, the CO will be responsible for a network of compliance officers, located throughout the business. In small companies the compliance function may be only part of the job of a human resource professional, a legal officer or finance manager.

The CO should have responsibility for leading the design and implementation of all aspects of the ABC programme.

The CO must be a person of integrity and command the respect of employees.

The CO's responsibilities may include the design and provision of ABC communications and training.

The compliance function should provide reports to management and the board on:

- the implementation of the programme;
- results of risk assessments;
- emerging practices, issues and concerns; and
- recommendations for improvements or additional resources.

The reporting line for the CO is a significant decision for the board. Best practice is for the CO to report directly into the board or a board committee such as an integrity, audit, risk or compliance committee.

Examples of good practice	Examples of poor practice	
<ul style="list-style-type: none"> <li>• Clear, documented responsibility for anti-bribery and corruption apportioned to either a single senior manager or a committee with appropriate terms of reference and senior management membership, reporting ultimately to the Board.</li> </ul>	<ul style="list-style-type: none"> <li>• Failing to establish an effective governance framework to address bribery and corruption risk.</li> </ul>	<p>d this could be</p>
<ul style="list-style-type: none"> <li>• Regular and substantive MI to the Board and other relevant senior management forums, including: an overview of the bribery and corruption risks faced by the business; systems and controls to mitigate those risks; information about the effectiveness of those systems and controls; and legal and regulatory developments.</li> </ul>	<ul style="list-style-type: none"> <li>• Failing to allocate responsibility for anti-bribery and corruption to a single senior manager or an appropriately formed committee.</li> </ul>	<p>d on the legal tion should be nt laws in the . It should also nce.</p> <p>; role will be to ethical culture to training on and counsellor</p>
<ul style="list-style-type: none"> <li>• Where relevant, MI includes information about third parties, including (but not limited to) new third-party accounts, their risk classification, higher risk third-party payments for the preceding period, changes to third-party bank account details and unusually high commission paid to third parties.</li> </ul>	<ul style="list-style-type: none"> <li>• Little or no MI sent to the Board about bribery and corruption issues, including legislative or regulatory developments, emerging risks and higher risk third-party relationships or payments.</li> </ul>	<p>re anti-bribery</p> <p>re anti-bribery ) channel.</p>
<ul style="list-style-type: none"> <li>• Considering the risk posed by former PEPs and 'domestic PEPs' on a case-by-case basis.</li> </ul>		<p>omitee such as hieved by the s have formed</p>
<ul style="list-style-type: none"> <li>• Actions taken or proposed in response to issues highlighted by MI are minuted and acted on appropriately.</li> </ul>		<p>s being carried oversight. The draw its own</p>

### 5.3 Assessing bribery and corruption risk (risk-based approach)

The ABC programme should be informed by periodic risk assessments to ensure that the programme is proportionate to the organisations:

- Location;
- Size;
- Industry; and



- Products and services.

In order to determine the scope of the assessment at the appropriate level, an initial pre-assessment exercise may identify the high-level topics which will then be used to assess each business area. For example:

- UK vs EMEA vs Global assessments. Global assessments are likely to have more geographical risk variables;
- The types of service a firm may offer e.g. traditional asset manager vs. a more diverse business;
- Legacy business areas that need to be taken into account which, may have a different risk profile.

A single set of questions and scope should be used for each for each business area assessed to ensure consistency of outcomes.

### **5.3.1 Assessment methodology**

A prescribed list of questions under topic headings such as Nature of Operations, Geographical factors etc., emailed to stakeholders for completion may be an effective use of time but may not be particularly robust unless stakeholders are highly engaged and understand what the objective of the exercise. A series of interview style sessions, although potentially time consuming and resource intensive, can provide for more robust outcomes.

Key considerations in performing the risk assessments of each business area are:

- Legal and regulatory landscape and its implementation/enforcement within different jurisdictions i.e. FCPA;
- Jurisdictional risk which includes:
  - the organisation's footprint in that country, including size, product and customer type/industry.
  - the country's risk, based on perceived levels of corruption highlighted by country reports and corruption league tables published by reputable organisations ie Transparency International;
- Third party relationships and due diligence (incl. intermediaries);
- Regulated vs unregulated 3<sup>rd</sup> parties;
- Subsidiaries;
- Acquisitions, joint ventures and mergers;
- Physical assets business e.g., Real Estate;
- Gifts and Hospitality, political contributions, sponsorships, charitable donations and the applicability of the associated policies to the business area;
- Risk of customer/client facilitation and / or a customer or client laundering the proceeds of bribery & corruption; and



- How the assessment designed to articulate whether the risk is inherent or residual.

The risk assessment may identify any gaps or area(s) for improvement, some examples of which are:

- Inconsistent implementation of 'global' policies;
- Lack of awareness among staff;
- Previously acquired businesses that are not fully integrated; and
- Additional controls that are required to lower residual risks to bring within the firms' risk appetite.

The risk assessment process should have appropriate governance with an appropriate Committee or other governance group reviewing and challenging the process and outcomes.

Any actions identified to improve the control environment and lower the residual risk should be tracked to completion with regular reporting of process to the governance body appointed with oversight of the process.

## **5.4 Policies and Procedures**

### **5.4.1 Documented, risk based, policies and procedures**

Effective, embedded policies and procedures are an essential element in Anti Bribery and Corruption compliance. The Act provides a defence where the organisation can prove it had in place adequate policies and procedures to prevent bribery occurring on its behalf.

An organisation's procedures to prevent bribery, by persons associated with it, should be proportionate to the bribery risks it faces and to the nature, scale and complexity of the organisation's activities. Such policies and procedures may be stand-alone or integrated with other related policies and procedures.

The Ministry of Justice has produced guidance on adequate procedures and has developed six 'principles' to enable firms to develop their policies and procedures considering:

1. -Proportionality
2. -Top Level Commitment
3. -Risk Assessment
4. -Due Diligence
5. -Communication
6. -Monitoring and Review

Demonstrating policies to staff, supported by effective and robust policies and procedures, enables staff to understand the issues involved, what it means to them and what they can do to prevent bribery and corruption within their area of responsibility.



Good practice includes senior management leading by example by complying with the firm's anti bribery and corruption policies and procedures.

Policies should include:

- The firm's approach to reducing and controlling the risks of bribery;
- Rules about accepting gifts, hospitality, or donations;
- Guidance on how to conduct business, e.g., negotiating contracts;
- Rules on avoiding or stopping conflicts of interest; and
- Recruitment and staff: staff working in areas of the business or positions identified as a higher risk should be subject to enhanced vetting process in comparison to staff in positions identified as a lower risk of a bribery and corruption perspective. There should also be a process/policy detailing the firm's approach to managing conflicts where staff are recommended by a client. If employment agencies are used, processes should be in place to ensure that they adhere to the appropriate vetting standards.

Staff responsible for implementing and monitoring anti-bribery and corruption policies and procedures should have adequate levels of anti-corruption expertise.

#### **5.4.2 Remuneration structures**

Policies should take into account good compliance behaviours, and not exclusively reward for revenue generation. Policies should be constructed and reviewed regularly to ensure they do not encourage unacceptable risk taking.

#### **5.4.3 Code of ethics**

Setting out the expected behaviours of those representing the organisation is an important aspect of ABC compliance. Ensuring the organisation embeds the appropriate culture is important and this should be driven by senior management demonstrating the expected behaviours to set the example to staff.

It is recommended third parties representing the organisation should be made aware, and if possible, agree to follow these Code of ethics.

#### **5.4.4 Third parties / intermediaries**

It is good practice for the firm to clearly set out behaviour expected of those acting on its behalf.

As noted previously, the firm can be prosecuted should a third party acting on its behalf attempt a bribe. The policy and procedures should include that the third party agrees to follow the firm's code of ethics. Prior to the business relationship commencing, the third party's due diligence should include assurance on their own ABC policy and how they enforce their requirements, including a review of the third party's own anti-bribery and corruption controls. Any negative responses to these points should act as a red flag to future dealings with the third party.

#### **5.4.5 Whistleblowing, investigation, dismissal**

Procedures for whistleblowing and reporting suspicions, including the use of hotlines, should be clear and communicated to all staff. If hotlines are not provided, firms should consider measures to allow staff to



raise concerns in confidence or, where possible, anonymously, with adequate levels of protection which staff should be made aware of.

As good practice, if firms do not provide staff with access to whistleblowing hotlines, it is recommended that they have processes in place to allow staff to raise concerns in confidence or, where possible, anonymously, with adequate levels of protection.

#### **5.4.6 Gifts & Hospitality**

The Gifts and Hospitality (G&H) policies and procedures should clearly define the approval process and the applicable thresholds. Processes in place should identify unusual or unauthorised G&H, and deviations from approval limits for G&H. Staff should be trained on G & H policies, relevant to their role, and should be regularly reminded to disclose G & H in line with the policy.

As good practice it is recommended that, where appropriate, the firm refers to existing sources of information, such as expense registers, policy queries and whistleblowing and complaints hotlines, to monitor the effectiveness of its anti- bribery and corruption policies and procedures.

#### **5.4.7 Facilitation payments**

Facilitation payments, which are payments to induce officials to perform routine functions they are otherwise obligated to perform, are bribes and a firm's policies and procedures should reflect this. Procedures should include the oversight and approval before a payment is made to a third party, following appropriate due diligence on the entity and/ or individual.

#### **5.4.8 Political and charitable contributions and public officials' definition**

The policies and procedures should describe how political and charitable donations are approved at an appropriate level, with input from the appropriate control function, such as compliance, and subject to appropriate due diligence. Processes should also consider whether there are conflicts present with the action of the giving and whether the action, although meeting the policy could have subsequent reputational risk at a later stage. Public officials' definition should be included to help ensure circumstance are identified and appropriate procedures followed.

#### **5.4.9 Books and record keeping**

Policies and procedures should ensure evidence of events is captured, alongside monitoring and regular testing of procedures to demonstrate adequacy.

#### **5.4.10 Training and Awareness**

Training and awareness of policies and procedures created to support ABC efforts is key to the successful delivery of an effective framework.

As noted in the earlier section, multiple policies are likely to be in place to support ABC. The nature and depth of training required on each area should reflect the area being trained (e.g., complexity, rate of change, level of risk) and the target audience (scope of responsibilities, knowledge and experience).

In addition, the scale and complexity of an organisation and its subsidiaries (where captured by the compliance framework) is also likely to have a bearing on the type(s) of training to be provided. Regardless



of the scale and complexity it is important that training is delivered to all the right people in an effective manner, at appropriate frequencies and with adequate recordkeeping of the training undertaken.

There are multiple methods to provide training and awareness, broadly, these fall into one of the following:

- Day to day interaction with subject matter experts e.g., compliance;
- Policy and other reading – supported by regular attestations;
- Computer based training and testing; and/or
- Face to face structured training including webinars for remote or home-based staff.

Tailored training and communications reflecting the nature of the business and risks arising will be of most value to the organisation and its employees. For example, policy reading together with attentions does have benefits although, where risks are elevated or individuals are likely to encounter an area as part of their role, this will often not be sufficient to provide adequate awareness. In such situations, tailored training should be provided. The reasoning for each type of training should be recorded.

When identifying the staff that should receive training and awareness, this should include directors and officers as well as all employees. In certain cases, particularly where the risks are elevated, agents and business partners may need to be included (or adequate assurance provided that they are subject to their own ABC requirements which, are adequate for the risks posed to the business). It is important that those subject to policies and procedures have access to these and know where to refer for additional guidance.

Examples of focussed training include:

- Practical advice or case studies to address real-life scenarios;
- How to obtain ethics advice on a case-by-case basis as needs arise;
- Examples of prior incidents at the firm and the lessons learned;
- Bespoke training to areas where misconduct has occurred; and
- Training on ‘red flags’ that are most likely to be applicable to the firm.

It is also important that the “gatekeepers” to ABC control processes receive adequate guidance and training so that it can be shown they have sufficient understanding of the processes that must be followed, the nature of risks to be alert to and when and how to escalate concerns.

As in most areas of compliance, the “tone from the top” greatly assists in any training programme. Messaging in respect of the expectations from staff should be clear, with failure to engage reported, actioned appropriately, and where necessary fed into performance and other reviews e.g., annual fitness and Fitness and Propriety certifications.

## **5.5 Monitoring for compliance**

Monitoring and auditing of a firm’s ABC framework is recommended to review compliance with applicable policies and procedures. The nature, frequency and depth of monitoring and auditing should be based on



the level of bribery and corruption risk, the results from past reviews and the nature, scale and complexity of the organisation.

Such monitoring should include reviewing individual policy areas that form part of the overall ABC framework e.g., gifts and hospitality, whistleblowing, third party procedures but also the framework itself i.e., the ABC policy, the ABC risk assessment and governance. Remediation of any findings should be undertaken in a timely manner.

Whilst not strictly “monitoring”, an effective ABC framework includes appropriate investigation of potential misconduct and is included in this section for ease. Hallmarks of an appropriate investigation include:

- Being undertaken in a timely and thorough way by independent qualified personnel;
- Appropriate documentation – both the assessment and the firm’s responses to findings;
- Analysis of the issue e.g., the root cause of the misconduct (control failings, lack of policies/procedures, poor training etc) and whether the issues are systemic issues in nature; and
- Appropriate escalation to senior management and the undertaking of disciplinary and remedial actions where necessary.

## **5.6 Anti-Bribery and Corruption for Financial Services Organisations**

Summary of considerations for ABC Compliance by Financial Services Organisations:

- Most anti bribery and corruption threat will come from third parties such as suppliers, service providers, introducers and agents. Third parties of this type are often the focus of investigation by law enforcement (SFO) and prosecution is brought under the UK Bribery Act 2010. Firms should conduct a risk assessment of all third parties and ensure that they have adequate procedures in place to handle the risk of misconduct by these third parties as well as their own employees.
- Anti-bribery and corruption risk and compliance must also be viewed from an international perspective. For businesses in any sector, bribery and corruption are a focus for enforcement agencies across the globe. An understanding of geo-political risk is helpful; many firms use the Corruption Perception Index produced by Transparency International and updated annually.
- Additionally, the focus on controls, systems and procedures to prevent bribery and corruption is key. As mentioned, this is underpinned by a robust and tailored risk assessment, to understand the threats posed and put in place adequate procedures designed to meet business and jurisdictional risk. Monitoring and adjusting procedures on a regular basis is critical to providing up-to-date and effective protection against bribery and corruption.

## **5.7 Links to useful resources:**

### **Financial Conduct Authority**

Thematic Review



Anti-Money Laundering and Anti-Bribery and Corruption Systems and Controls

<https://www.fca.org.uk/publication/thematic-reviews/tr13-09.pdf>

Bribery & Corruption note for FS organisations

<https://www.fca.org.uk/firms/financial-crime/bribery-corruption>

Financial Crime Guide

<https://www.handbook.fca.org.uk/handbook/FCG/1/?view=chapter>

### **Serious Fraud Office**

Bribery Act Guidance

<https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/bribery-act-guidance/>

### **Ministry of Justice**

UK Bribery Act

<https://www.legislation.gov.uk/ukpga/2010/23/contents>

UK Bribery Act Guidance

<https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf>

### **Transparency International**

Corruption Perception Index and useful publications

<https://www.transparency.org/en/cpi/2019/index/nzl#>

<https://www.transparency.org.uk/publications>

### **UK Government**

Anti-Corruption Plan 2017-2022 ( latest update)

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/902020/6.6451\\_Anti-Corruption\\_Strategy\\_Year\\_2\\_Update.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902020/6.6451_Anti-Corruption_Strategy_Year_2_Update.pdf)



## 5.8 TISA Anti Bribery and Corruption High Level Risk Assessment Template

### 5.8.1. Purpose of the template

This bribery and corruption self-assessment template takes the user through key questions all organisations ought to consider in order to:

- better understand and articulate the threat;
- establish the risks faced; and
- assess the organisations capacity to manage and mitigate those risks.

We have set out a series of points to consider for each question to help users identify areas to assist with their risk assessment approach to counter bribery and corruption activity. We also recommend summarising the current activity within the organisation for each question and documenting next steps.

Those responsible for bribery and corruption within the organisation will be responsible for co-ordinating the completion of the form, but we recommend that it is approved by top level management.

### 5.8.2 Key Definitions

In this document several definitions are used. It is important to relate the following to your organisation:

<b>Bribery</b>	Bribery is defined as – offering, promising, agreeing to receive or giving of a financial or other advantage to induce or reward improper functions or activities and/or the request or receipt of such an advantage.
<b>Corruption</b>	Corruption is defined as - the abuse of power by an official (or any employee entrusted to carry out the functions of government, including contractors) for personal gain.
<b>Risk Assessment</b>	A bribery and corruption risk assessment builds a comprehensive picture of the risks that an organisation faces, evaluates controls and assesses the likelihood and impact of these risks on the organisation.
<b>Top Level Management</b>	Board of directors (or any other equivalent body or person)



**5.8.3 TISA Anti Bribery and Corruption High Level Risk Assessment Template**

Having completed the assessment sheet, please provide an overview of where your organisation currently is in terms of the following areas:

**Governance and MI**

Red     Amber     Green

Overview

**Assessing bribery and corruption risk (risk-based approach)**

Red     Amber     Green

Overview

**Policies and procedures**

Red     Amber     Green

Overview



**Training and awareness**

Red

Amber

Green

Overview

**Monitoring for Compliance**

Red

Amber

Green

Overview

**Reporting and investigation**

Red

Amber

Green

Overview

**Supplier Management/Third Party Relationships**

Red

Amber

Green



Overview

**Governance and MI**

Does your organisation establish and maintain an ABC programme that sets the standards for appropriate behaviour and ethical business practices?

Points to consider:

Element	Yes	Developing	No	Don't know
Culture / tone from the top				
Senior Management sponsorship of the programme				
Roles & responsibilities				
Resource / skill sets				
Internal reporting framework (event driven and regular MI)				
Independent review of programme				

In the space below, please provide a brief overview of current activity and future plans:

**Assessing bribery and corruption risk (risk-based approach)**

Does your organisation have an ABC programme which is informed by periodic risk assessments to ensure the programme is proportionate to your organisations:

- Location
- Size



- Industry
- Products and Services

**Points to consider:**

Element	Yes	Developing	No	Don't know
Legal and regulatory landscape and it's implementation and enforcement within different jurisdictions i.e. FCPA				
Third party relationships and due diligence (incl. intermediaries)				
Subsidiaries				
Jurisdictional Risk eg footprints in high risk countries based on perceived levels of corruption highlighted by country reports and corruption league tables published by reputable organisations ie Transparency International				
Acquisitions / joint ventures / mergers				
Gifts & Hospitality, political contributions / sponsorships / charitable donations				
Customer / client risk: risk of facilitation and / or laundering the proceeds of bribery & corruption (link with AML framework)				
Products/services offered				



In the space below, please provide a brief overview of current activity and future plans:

**Policies and Procedures**

Does your organisation have documented and risk-based policies and procedures in place to combat the risks associated with Bribery and Corruption?

Points to consider:

Element	Yes	Developing	No	Don't know
Staff recruitment and vetting, including procedures for work experience e.g. referrals by customers				
Remuneration structures				
Code of ethics				
Third parties / intermediaries				
Whistleblowing, investigation, dismissal				
Charitable giving				
Gifts & Hospitality including a G&H register				
Facilitation payments				
Political contributions				
Marketing sponsorship				
Books and record keeping				
Public officials' definition				



In the space below, please provide a brief overview of current activity and future plans:

**Training and Awareness**

Does your organisation have a training programme in place to help staff with the prevention and detection of the risks associated with Bribery and Corruption, and is it effectively communicated and applicable to all persons at all levels?

Points to consider:

Element	Yes	Developing	No	Don't know
Risk based training for all staff (incl. Board training)				
Subsidiaries / third parties				
Maintenance of training completion records				
Bespoke training for higher risk areas/roles eg Supplier Management, Commercial/Sales				

In the space below, please provide a brief overview of current activity and future plans:

Do you communicate/raise awareness of bribery and corruption within your organisation and the channels available to report suspicions?

Yes	Developing	No	Don't know



In the space below, please provide a brief overview of current activity and future plans:

**Monitoring for Compliance**

Does your organisation have a monitoring programme in place (including control testing) to review compliance with applicable policies and procedures relating to Bribery and Corruption?

Points to consider:

Element	Yes	Developing	No	Don't know
Annual monitoring programme				
Remediation programme				
Document retention				
Annual policy, process and procedure reviews				

In the space below, please provide a brief overview of current activity and future plans:

**Reporting and Investigation**

Do you have systems and processes for i) recording and capturing all incidents, ii) investigating allegations and iii) dedicated resource for either investigating internally or for arrangements with external investigators associated with bribery and corruption?

Points to consider:

Element	Yes	Developing	No	Don't know
System for recording incidents of bribery and corruption				



Element	Yes	Developing	No	Don't know
System for recording breaches of the counter bribery and corruption control system				
Process for reporting incidents and breaches to top level management				
Process to report allegations of bribery and corruption internally				
Process to report allegations of bribery and corruption to external agency				
Case acceptance criteria for bribery and corruption				
Trained internal capability to respond to incidents of bribery and corruption				
Case management system to log allegations				
An arrangement with external investigators				
Plan to continually develop skills and capability of investigators				
Sanctions and Redress policy for investigators to refer to				

**In the space below, please provide a brief overview of current activity and future plans:**

**Supplier Management/Third Party relationships**

**Does your organisation review the counter bribery and corruption procedures of outsourced service providers and promote awareness of bribery and corruption with outsourced partners / supply chain??**

**Points to consider:**

Element	Yes	Developing	No	Don't know
Procedures of outsourced service providers/suppliers reviewed				



Element	Yes	Developing	No	Don't know
Counter bribery and corruption requirements are built into contracts				
How to report incidents of bribery and corruption is promoted with outsourced partners				
Audit clauses built into third party contracts				

**In the space below, please provide a brief overview of current activity and future plans:**



## 6. Application of the 'Three Lines' model

### 6.1. Purpose of this review

The TISA Financial Crime Working Group has explored how the three lines model is currently operating, what is best practice, and moving forwards the ideal target operating model for AML /CTF. In this context, the roles, and responsibilities in each of the three lines of defence are further explained and this paper serves to outline how the MLRO's team should be developed once first line activities are fully passed to first line ownership.

### 6.2. Introduction to the three lines of defence (3LOD) model

In the financial sector, an established internal control and risk management approach that helps firms strengthen, clarify, and coordinate their essential governance, internal control and risk management roles and responsibilities is the 3LOD model- now known as the Three Lines Model (3LM).

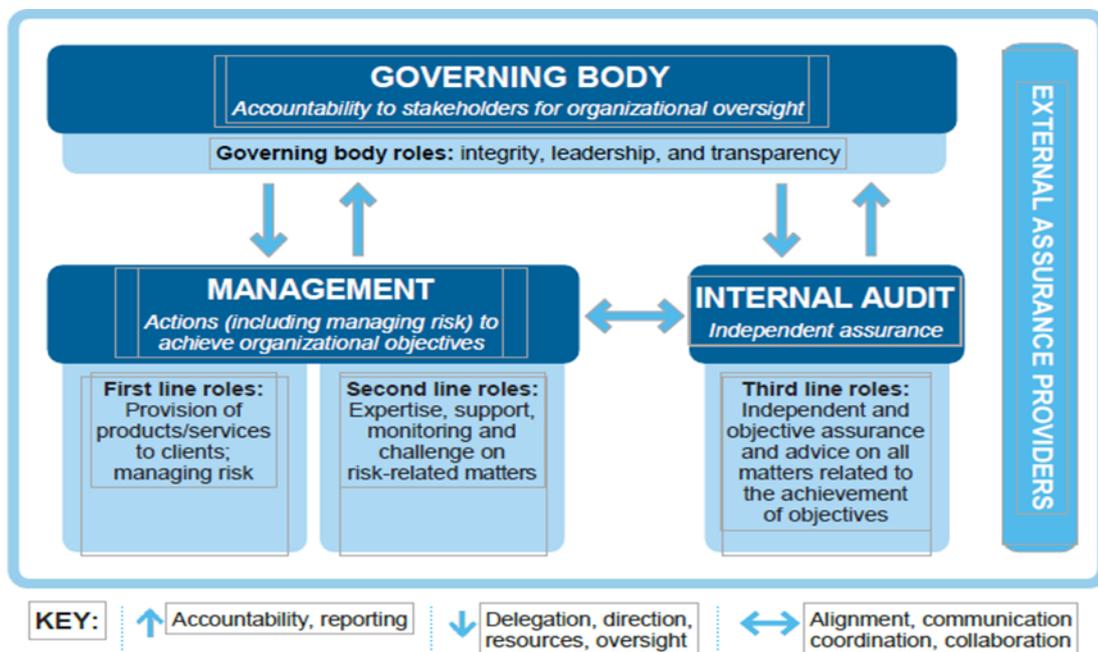
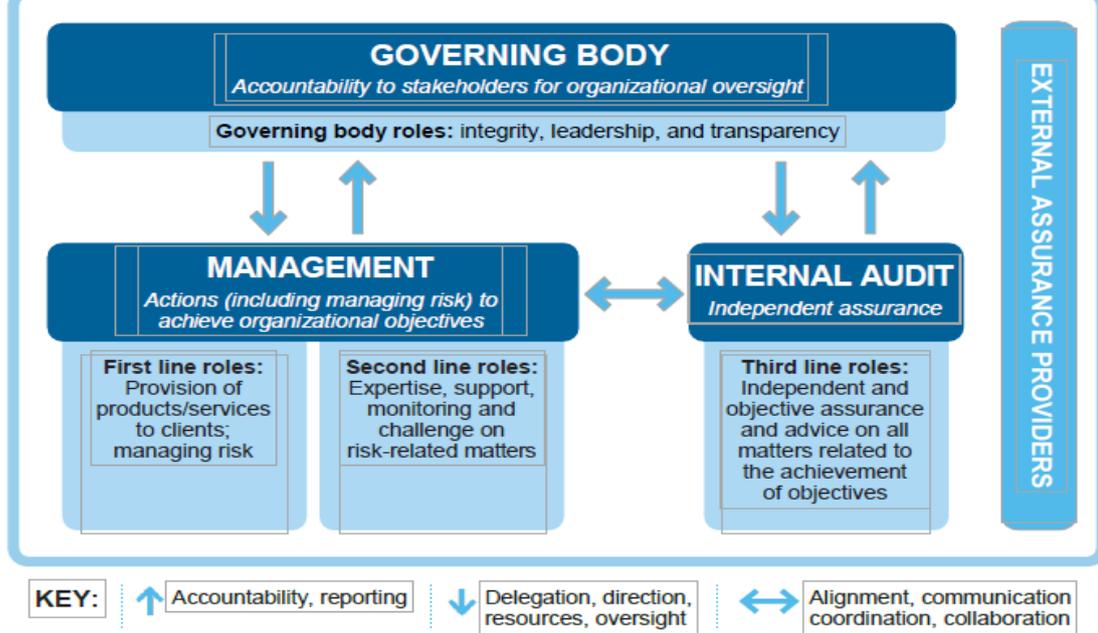
The first reference to the 3LOD in the FSA's publicly available documents dates from 2003 where it would appear that firms had adopted the 3LOD model without the FSA requiring them to, though it is not clear what the driver for this adoption was. In July 2020 an updated version of the 3LM model was published by the Institute of Internal Audit. This version sets out three key areas of responsibility and six principles.

Even with its evolution, the framework of the 3LM has predominantly stayed the same. The 3LM model distinguishes three groups (or lines) with the Board sitting above the model performing a 'model oversight' role through the activities of:

- Set 'Tone at the Top'
- Perform strategic risk assessments
- Establish risk appetite, strategy, targets
- Safeguard mission and values as cornerstone of the firm's culture
- Approve internal control system, risk and compliance framework, methodologies, overall policies and roles and responsibilities
- Approve adequate system for internal controls over financial reporting
- Leverage risk and compliance information into decision making process and evaluate business operations activities on a risk-adjusted basis

The model has the lines divided by:

- 1st line is business operations who have risk ownership



Implementing the 3LM model increases the ability of a firm to achieve its strategic objectives by:

- a. Identify and mitigating negative risks (those that threaten strategy); and
- b. Identifying opportunities and placing the business in a position to take the same'

### 6.3. Application of the three lines model to AML /CTF and the role of the MLRO

The 3LOD model, now known as the Three Lines Model (3LM) is how most firms in the financial sector now approach risk management as it helps firms identify structures and processes that best assist the achievement of objectives.

The role of Compliance in the 2L is: advising; educating; monitoring and testing; identifying, measuring, and assessing compliance risk associated with the firm's activities; reporting and



escalating concerns to senior management; and liaising with regulators. However, the MLRO function is different, albeit in the 2L, as the MLRO role defined in regulatory requirements is to:

1. Monitoring and testing of the day-to-day operation of firm's AML and CTF policy which has clear roles and responsibilities;
2. Conducting a risk assessment to identify where the firm's business is vulnerable to ML and TF (within MLR);
3. Maintaining policy to reflect the result in the AML/CTF risk assessment;
4. Producing a compliance report for senior management at least annually;
5. Receiving and investigating internal suspicious activity reports, with required record keeping, to determine whether externally reportable;
6. Making external reports to the UK Financial Intelligence Unit, the NCA, and to HM Treasury under financial sanctions legislation;
7. Responding promptly to any reasonable request for information made by the Regulator and law enforcement;
8. Keeping abreast of industry trends alongside national and international findings concerning countries of concern; and
9. Producing training and awareness materials.

#### **6.4. FCA expectations of firms**

The FCA expects firms to have adequate organisational structures in place to mitigate the furtherance of financial crime and has specific regulatory requirements detailed in their Handbook (SYSC 6.3). Specifically, in November 2017 the FCA stated that: "Structurally, firms are seeking to clarify the shifting boundaries of the first and second lines of defence to help define the responsibilities of the compliance function, with regard, for instance, to financial crime. Such organisational change is likely to continue in the coming years." The TISA FCWG recognise that there is still a diverse range of MLRO mandates which typically include the core elements of acting with full independence to provide effect governance and oversight, and be both a partner and a challenger, to ensure regulatory requirements, both the letter, and the spirit of the law, and regulations, are effectively applied. It is critical that the MLRO's mandate and desired outcomes are absolutely clear, understood by internal and external stakeholders, and maintained to support business strategy, growth, and innovation.

In May 2021 the FCA issued a Dear CEO letter to retail banks with details of the AML /CTF common control failings it has found and needed to be addressed. This included the following on the 3LOD:

- Poor understanding of the 3L in practice
- Inappropriate allocation of responsibilities resulting in blurring of 1L and 2L
- Lack of technical knowledge in the 1L



- 1L not fully understanding the financial crime risk faced by the firm, impacting the ability to identify and tackle potentially suspicious activity
- 2L undertaking 1L roles which restricts the 2L ability to independently monitor and test the control framework, which can lead to gaps in the understanding of risk exposure.

## 6.5. Conclusion

For realising the benefits and robust embedding of the 3LM, the roles, responsibilities, activities, policies, and procedures within the responsibility of each line of defence should be clear and transparent to everyone in the firm. The 3LM is most effective when there is collaboration and communication across both the 1L and 2L roles of management and internal audit to ensure there is no unnecessary duplication, overlap, or gaps. Once the mandate is clarified it should be possible to translate this into key priorities, key activities, and the skills, competencies and resources required for the lines, including the MLRO, to be capable of discharging its mandate effectively in support of SMCR. The right balance needs to be found between the independence of the MLRO function and its close collaboration with the business. The 3L need to work together to ensure that a firm has a coherent risk structure, and it appears that for AML /CTF the target operating model is mainly consistent. In the FCA experience, firms where those in business roles fully understand the relevant risks and know that part of their role and responsibilities is to help mitigate those risks, are significantly better at mitigating risks than their peers so the direction needs increased momentum.

The appendix below (Appendix 3) details the current position found in the industry (across surveyed TISA member firms) for AML /CTF and the target operating model. Red indicates that a low number of firms gave a positive response to the particular Line, with Amber being a smaller number of positive response and Green being the highest number of firms performing a task in a particular Line. For example, in Task 4 it appears the majority of firms surveyed have Sars emanating from the 1L, with some firms having SARS emanating from the MLRO, and the majority of firms plan to move the responsibility of the task to the 1L, 2L and MLRO.

It appears that the results of this review have identified differing levels of maturity in relation to the reorganisation of the operating model, with some movement of activities that were previously in the 2L to the 1L. Some firms have moved towards a more empowered 1L with a clear understanding of its role in delivering risk management. But this has not been entirely one-way traffic – there have also been examples of insufficient clarity of the different types of testing objectives performed across the 3L. Such organisational change is likely to continue in the coming years. There are some tasks where the direction is for both 1L and 2L to complete, but from their own responsibility perspective. The current trend on the positioning of the MLRO, is to move to reporting to the CRO (or CEO), away from Compliance as defined in the FCA Handbook, and for good reasons such as to recognise the importance of countering financial crime, not least to provide the over-arching view of risks and risk management that is required of a CRO.

### Appendix 3

	Task	Who completes task					Who do you aim to complete task?			
		1LOD	1B	2LOD	MLRO team		1LOD	1B	2LOD	MLRO team
1	Processing alerts generated from electronic verification and screening to determine if a true match	Yellow	Red	Red	Red		Green	Red	Red	Red
2	Processing updates received from OFSI relating to financial sanctions to determine if a match on the client database	Red	Red	Red	Yellow		Green	Red	Red	Red
3	Contact with OFSI for obtaining a financial sanctions licence	Red	Red	Red	Green		Red	Red	Red	Green
4	Reporting an internal SAR for further investigation to determine if reportable to the NCA as a reasonable suspicion	Green	Red	Red	Yellow		Green	Red	Green	Green
5	Processing internal SARs received, reporting as appropriate to NCA, and associated record keeping	Red	Red	Red	Green		Red	Red	Red	Green
6	Generating business case for application rejection /business relationship termination due to Proceeds of Crime risk	Yellow	Red	Red	Green		Green	Red	Red	Green
7	Approval/decline of application rejection /business relationship termination due to Proceeds of Crime risk	Red	Red	Yellow	Green		Green	Red	Red	Green
8	DAML submission to NCA, and associated record keeping	Red	Red	Red	Green		Red	Red	Red	Green
9	Generating business case for approval of business relationship with PEP /local PEP	Yellow	Red	Red	Green		Green	Red	Red	Yellow
10	Approval /decline of business relationship with PEP /local PEP	Red	Red	Yellow	Green		Red	Red	Yellow	Green
11	Processing 3rd party contact requesting information e.g. from DWP, restraint orders, confiscation orders, court orders	Red	Red	Red	Green		Green	Red	Red	Green
12	Providing statements to authorities in relation to Proceeds of Crime investigations	Red	Red	Red	Green		Red	Red	Red	Green
13	Generating materials for guidance to clients on preventing financial crime e.g. scam awareness	Red	Red	Red	Green		Green	Red	Red	Green
14	Generating AML /CTF training materials to colleagues	Red	Red	Red	Green		Red	Red	Red	Green
15	Key control testing including quality assurance	Green	Red	Red	Yellow		Green	Red	Red	Green
16	Generating general AML /CTF MI for management committees	Red	Red	Red	Green		Yellow	Red	Red	Green
17	Generating general AML /CTF MI for Board reporting	Red	Red	Red	Green		Yellow	Red	Red	Green
18	Formal MLRO report to Board, and periodic updates	Red	Red	Red	Green		Red	Red	Red	Green
19	Generating AML /CTF MI for third party contracts e.g. providing details on processing volumes to partners	Yellow	Red	Red	Yellow		Green	Red	Red	Red
20	Producing assurance documents for third parties (comfort letters, attestations, Wolfsberg questionnaires, etc)	Yellow	Red	Red	Green		Yellow	Red	Red	Green
21	Approval /signature for assurance documents for third parties (comfort letters, attestations, Wolfsberg questionnaires)	Red	Red	Red	Green		Red	Red	Red	Green
22	AML /CTF risk assessment - core and when generated from other triggers such as change in the target	Red	Red	Yellow	Green		Yellow	Red	Red	Green



	market for products /services	Red	Red	Yellow	Green		Yellow	Red	Red	Green
23	Approval of AML /CTF risk assessment - core and when generated from other changes	Red	Red	Yellow	Green		Red	Red	Red	Green
24	Ownership of AML /CTF Policy	Red	Red	Red	Green		Red	Red	Red	Green
25	Ownership of AML /CTF procedures /processes	Green	Red	Red	Green		Green	Red	Red	Yellow
26	Monitoring the effectiveness of AML /CTF systems and controls, the fulfilment of AML /CTF duties by the firm	Red	Red	Yellow	Green		Red	Red	Yellow	Green
27	Monitoring to identify potential reasonable suspicions	Green	Red	Red	Green		Green	Red	Red	Green
28	Generating core data for FCA REP CRIM	Yellow	Red	Red	Yellow		Green	Red	Red	Yellow
29	Collating and submitting the FCA REP CRIM	Red	Red	Red	Green		Red	Red	Red	Green
30	Maintenance of record and cascade when changes relating to AML /CTF high risk jurisdictions	Red	Red	Red	Green		Red	Red	Red	Green
31	Project consultation to ensure AML /CTF risks are identified and managed to within appetite	Green	Red	Yellow	Green		Green	Red	Yellow	Green
32	Thematic AML /CTF risk reviews	Red	Red	Green	Green		Red	Red	Green	Green
33	Horizon scanning and industry threats and trends – identification and cascade, including thoughts on preventions /solution	Red	Red	Yellow	Green		Red	Red	Yellow	Green
34	Maintain a robust AML /CTF prevention framework and ensure appropriate controls are in place to mitigate firm's exposure	Red	Red	Red	Green		Yellow	Red	Red	Green
35	Oversight /challenge to the 1LOD on the firm’s approach to combating the AML /CTF threat with aim to improve processes /reduce risk	Red	Red	Green	Green		Red	Red	Yellow	Green
36	Define and communicate an AML /CTF strategy, aligned with the firms risk appetite and strategic direction	Red	Red	Red	Green		Red	Red	Red	Green
37	Management /Board Committee Representation	Red	Red	Green	Green		Red	Red	Yellow	Green