IDEAS | PEOPLE | TRUST

BDO Economic Crime Advisory

How to build a robust SAR framework

How to build a robust SAR framework

Financial crime ruins lives.

It funds terrorism, facilitates dictators, and every year an estimated £100bn[1] is laundered through the UK.

Our guide to building a robust SAR framework helps firms play their part in reducing the devastating effect financial crime has on us all.

Contents **page**

The regulations	3
Where and how to file SARs	4
The building blocks of a robust framework	5
Customer due diligence	6
Transaction and/or customer monitoring	7
Training and awareness	8
Escalation and evaluation	9
SAR filing	10
Know your SARs	11
Post SAR activity	12
Record keeping and management information	13
Assurance	14
Helping you succeed	15

[1] Economic Crime Plan 2, HM Government, 2023

The regulations

As part of the fight against financial crime, all UK firms are legally required to report suspicious activity.

Firms in scope of
The Money Laundering, Terrorist Financing & Transfer of Funds (Information on the Payer) Regulations 2017
('The UK Money Laundering Regulations' or 'UK MLRs')

Credit and financial institutions | Auditors, insolvency practitioners, external accountants and tax advisers | Independent legal professionals | Trust or company service providers | Estate and lettings agents | High value dealers | Casinos | Art market participants | Cryptoasset exchange providers and custodian wallet providers

Known as:
The Regulated Sector

Are:
Legally obliged to appoint a Nominated Officer (NO) to investigate internal escalations and report SARs to the NCA

And under:
The Proceeds of Crime Act 2002 (PoCA)

Must file SARs upon knowing, suspecting or having reasonable grounds for knowing or suspecting money laundering

And under:
The Terrorism Act 2000 (TACT)

Must file SARs upon knowing, suspecting or having reasonable grounds for knowing or suspecting terrorist financing

All other sectors

Known as:
The Non-Regulated Sector

Are:
Encouraged to appoint a similar dedicated role as a matter of best practice

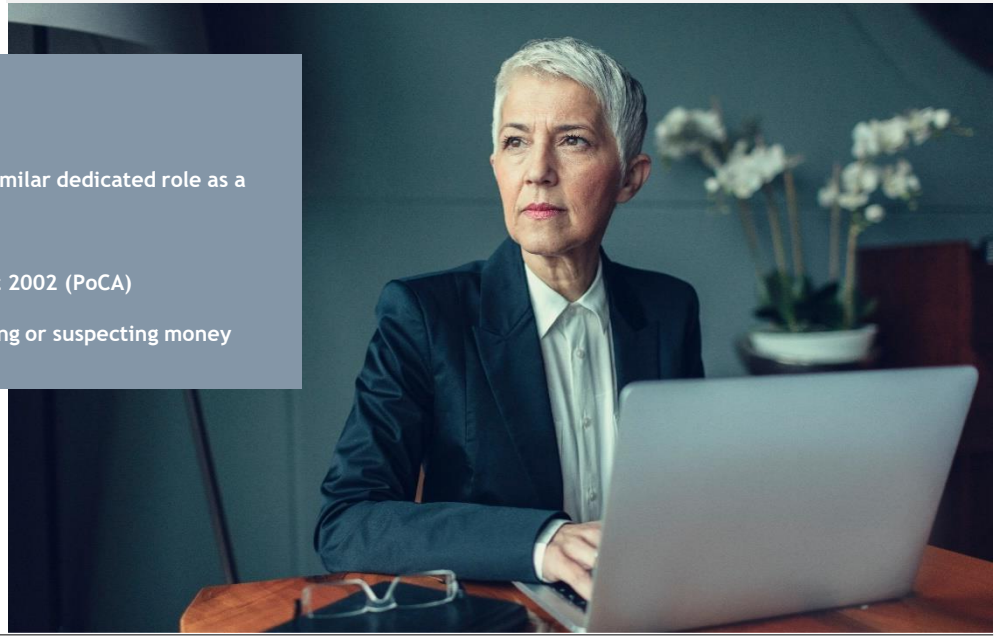
And under:
The Proceeds of Crime Act 2002 (PoCA)

Must file SARs upon knowing or suspecting money laundering

Money Laundering
Concealing of criminal property (disguising, converting, transferring, removing). Arrangements whereby the acquisition, retention, use or control of criminal property is known or suspected. Acquiring, using or possessing criminal property – [PoCA 2002, Part 7, clauses 327, 328 and 329]

Terrorism
Fundraising (receiving, offering or facilitating the receipt/offer of funds/property intended to be used for terrorism). Use and possession (possessing funds/property intended to be used for terrorism or using funds/property for terrorism) – [The Terrorism Act 200, clause 16 and 17]

Having reasonable grounds for knowing or suspecting money laundering or terrorist financing applies only to 'The Regulated Sector'. These firms are expected to have processes to investigate and determine facts, "a vague feeling of unease" does not constitute 'having reasonable grounds'(R v. Da Silva, 2006).



Where and how to file SARs

SARs must be filed electronically via the NCA SAR Portal here.

As of 4 March 2024, the previous SAR fling system (SARs Online) was decommissioned, and access has now been permanently revoked for all reporters. The NCA SAR Portal is the single and only platform to be used.

The NCA SAR Portal is exclusively for reporting suspicions of Money Laundering or Terrorist Financing only. The NCA is not a crime reporting agency.

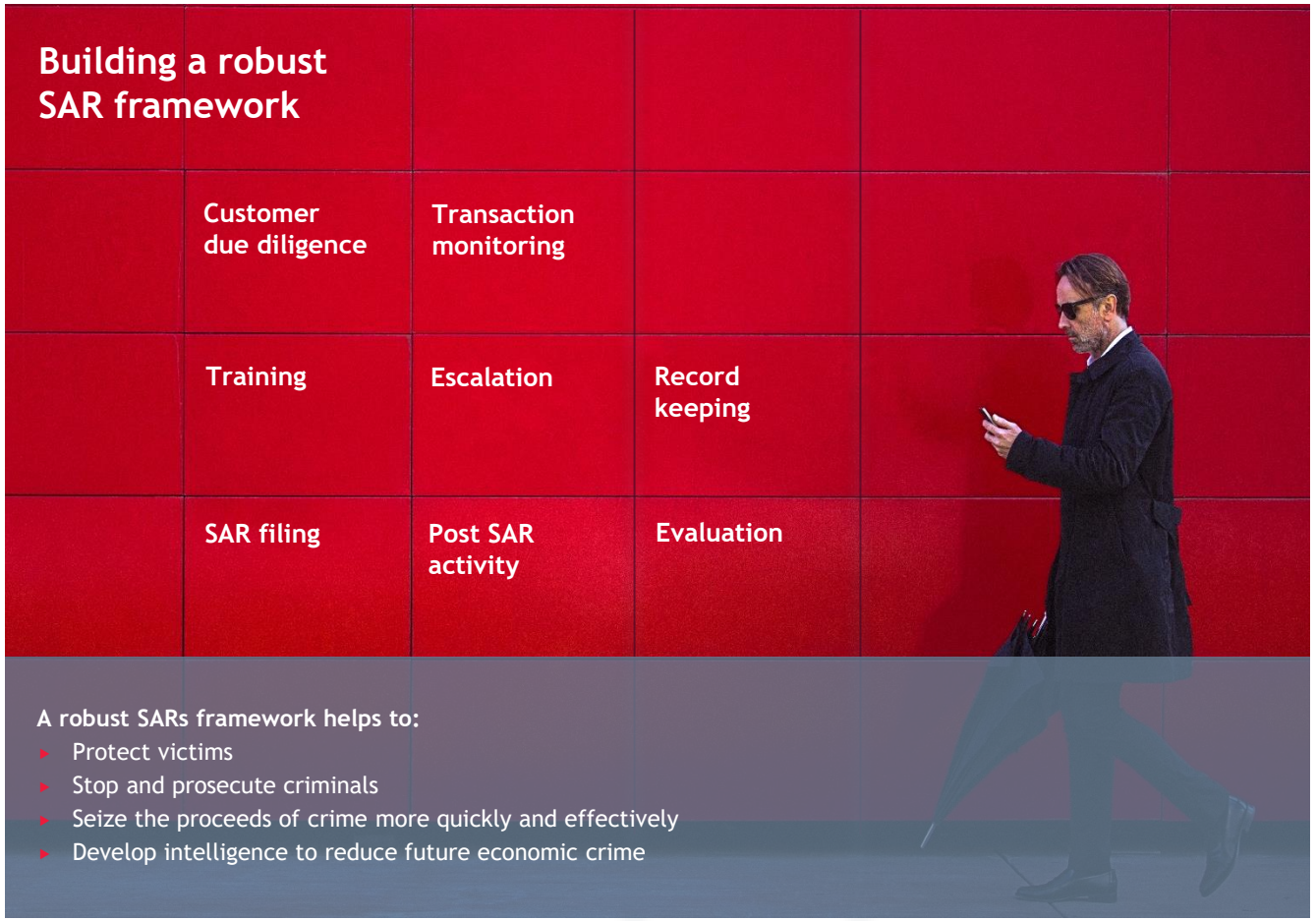
If your concern relates to Fraud, you should report via Action Fraud (website or call 0300 123 2040). If you have concerns about funds which are not yet the proceeds of crime, then this is attempted fraud (not money laundering) and therefore should be reported via the Action Fraud pathway not the SAR pathway.

The building blocks of a robust framework

Suspicious activity reports (SARs) provide law enforcement agencies with the information they need to investigate and take action. The better quality the information provided, the more effective the SAR is in the fight against financial crime.

Filing high quality SARs relies on laying the right foundations. By building a robust SARs framework you are complying with the regulations and helping to protect victims and prosecute criminals.

The illustration right shows the building blocks of an effective SARs framework. Each item is covered in depth throughout this guide.



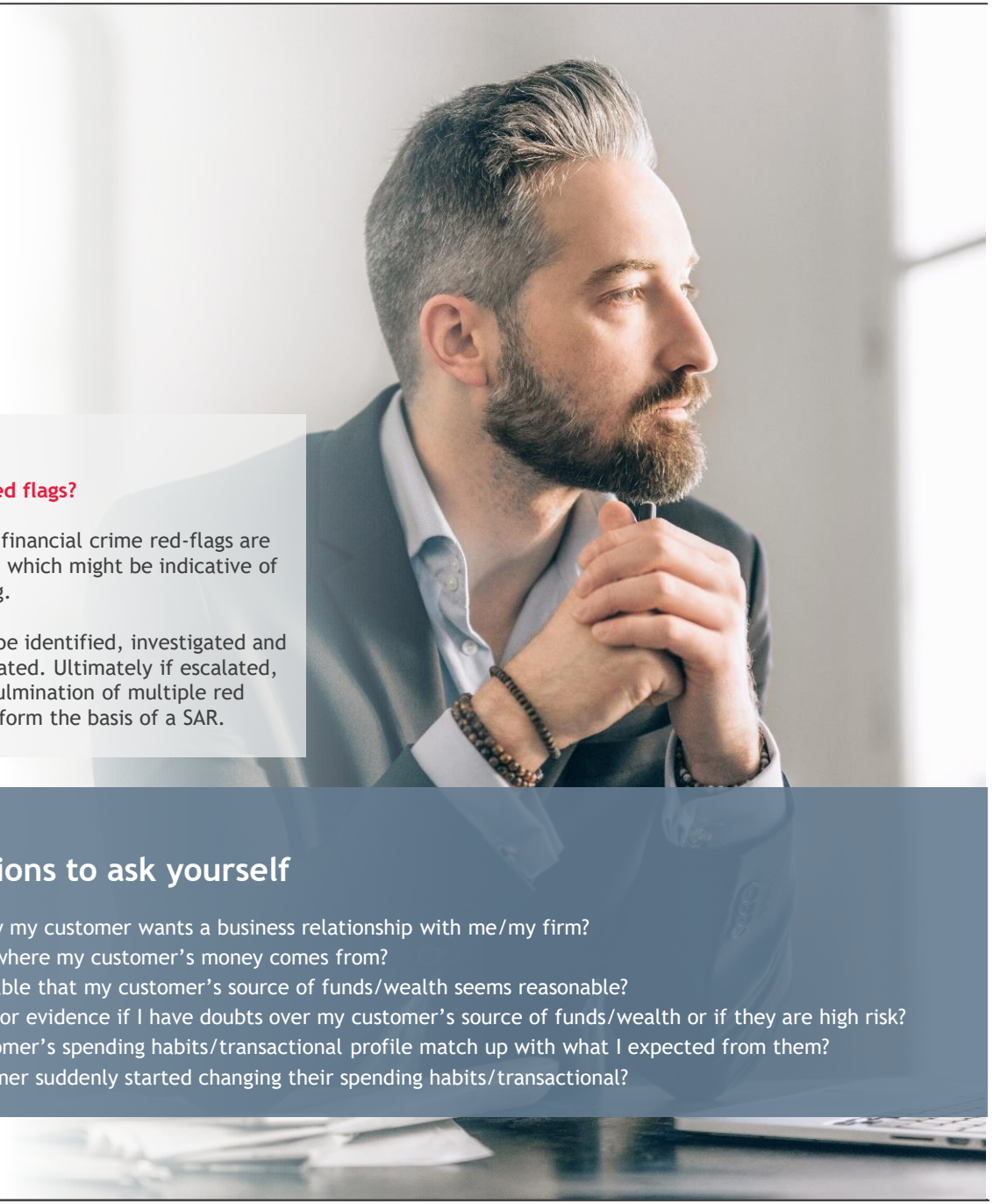
Customer due diligence

Regulated firms are required to carry out customer due diligence (CDD). This means understanding the customer's purpose for the intended business relationship with you, profiling how they will 'normally' transact and knowing their sources of their wealth. This process is also referred to as know your customer (KYC).

By 'knowing your customer' you can notice when their behaviour is in some way unusual, which may be an indicator (or red flag) of suspicious activity.

Depending on the size and scale of the firm, the way KYC information is captured may vary. Larger firms typically use a customer relationship management (CRM) tool to record all KYC information and documentation. Smaller firms may rely on paper-based records; however, this is becoming less common in the digital age. Instead, a secure shared drive/SharePoint is typically used to retain KYC information for each client.

It is important to note that what is 'normal' in one situation may be suspicious in another. For example, a one-off £600k transaction is common-place when buying a new home but not so when placing a bet on the outcome of a football fixture. CDD/KYC must be kept up to date so any changes in customer circumstances are captured.



What are red flags?

In the context of financial crime red-flags are customer activity which might be indicative of money laundering.

Red flags should be identified, investigated and discounted/escalated. Ultimately if escalated, a red flag (or a culmination of multiple red flags) is likely to form the basis of a SAR.

Questions to ask yourself

- Do I know why my customer wants a business relationship with me/my firm?
- Have I asked where my customer's money comes from?
- Am I comfortable that my customer's source of funds/wealth seems reasonable?
- Have I asked for evidence if I have doubts over my customer's source of funds/wealth or if they are high risk?
- Does my customer's spending habits/transactional profile match up with what I expected from them?
- Has my customer suddenly started changing their spending habits/transactional?

Transaction and/or customer monitoring

Regulated firms are required to continually monitor customer transactions to ensure they are consistent with what would be expected from CDD/KYC profiling.

The ability to monitor transactional behaviour and spot peculiarities will vary across different firms. For example, retail banks, e-money firms, casinos and lettings agents may be able to develop detailed transactional profiles of customers, whereas art dealers, real-estate agents and lawyers may only engage with customers for a one-off transaction.

Automated transaction monitoring tools are available to help firms handle higher volumes of data and gain insight on their customers. Typically, automated controls (augmented with modern techniques such as machine learning) are used to identify and discount straight forward 'false positives' with human intervention to carry out more discrete judgements. Where firms choose more manual methods they should consider if they are adequate for the size and nature of their customer activity.

Firms should also be alive to other changes in customer relationships. A customer who becomes less responsive or otherwise changes the way they usually engage could be a red flag.

False positives

False-positives refers to activity which was originally flagged as potentially unusual/suspicious (either by an automated or manual transaction/customer monitoring) but later confirmed not to be.

For example, in retail banking, an individual suddenly starts making payments to a foreign bank account it appear suspicious but then confirmed as a genuine donation to an aid programme. Equally, in property lettings, an individual suddenly requesting that rental payments are made by a third party might at first be considered unusual/suspicious but later confirmed to be from a parent.

Questions to ask yourself

- Does my CDD/KYC approach enable me to identify what "normal" behaviour/activity looks like for my customers?
- Have I checked whether my supervisor published red flags relevant to my sector which I can incorporate into my transaction and/or customer monitoring approach?
- Have I conducted a transactional risk assessment to understand what activity is considered "normal" for my organisation, operational footprint and customer base so I can define what might be unusual or suspicious?
- Have I tested (and calibrated) my transaction and/or customer monitoring approach to validate that it works as intended and is optimised to the extent possible?

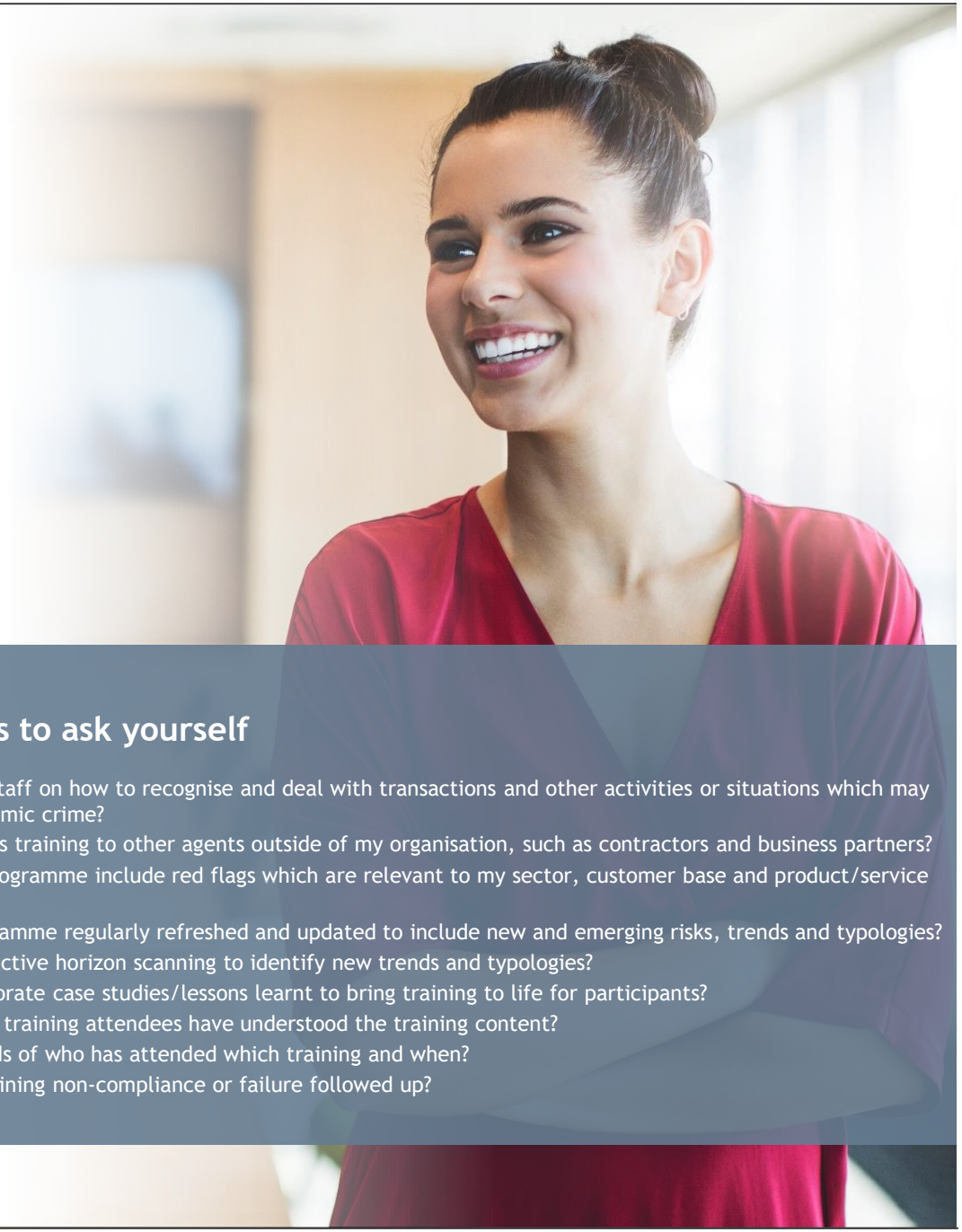
Training and awareness

The MLRs put a legal obligation on regulated firms to train all staff, contractors and agents. This is so they can recognise and deal with 'red flags', i.e. activities which may be related to economic crime. Employees who fail to report suspicious activity can rely on defence under PoCA if the employer has failed to provide adequate training.

It is important to note that 'red flags' will vary from sector to sector. For example, in the art market it is typically more common for a buyer based in another country to use an agent, whereas a typical retail banking customer would be unlikely to request to conduct business with their bank via an intermediary.

Firms should be scanning for emerging trends in money laundering and terrorist financing, particularly in relation to their sector, and updating their training accordingly.

Training tends to be most effective when it is: interactive, uses real life scenarios, and is assessed to test correct understanding.



Questions to ask yourself

- Have I trained my staff on how to recognise and deal with transactions and other activities or situations which may be related to economic crime?
- Have I extended this training to other agents outside of my organisation, such as contractors and business partners?
- Does my training programme include red flags which are relevant to my sector, customer base and product/service offering?
- Is my training programme regularly refreshed and updated to include new and emerging risks, trends and typologies?
- Do I undertake proactive horizon scanning to identify new trends and typologies?
- Am I able to incorporate case studies/lessons learnt to bring training to life for participants?
- Do I assess whether training attendees have understood the training content?
- Am I keeping records of who has attended which training and when?
- Are instances of training non-compliance or failure followed up?

Escalation and evaluation

Whether identified by technology or people, firms should have written policy and procedure manuals for escalation channels. These will clearly define how to escalate 'red flags' and how potentially suspicious activity will be evaluated.

Firms must ensure adequate governance in relation to the evaluation of suspicious activity. Decision-making must be made by people with the right experience, technical knowledge and sufficient authority. Roles and responsibilities should be clearly documented, communicated and understood.

Depending on the size and complexity of a firm, more than one 'Nominated Officer' maybe designated for the evaluation of red flags.

When an internal escalation reaches the Nominated Officer or responsible team, an internal investigation should be undertaken to determine whether a SAR should be filed to the NCA.

Firms should also ensure that they formally document the evaluation of any internal escalations, whether these have given rise to a SAR or not.

Nominated Officer vs. MLRO

While used interchangeably these terms are distinct:

- The UK MLRs Regulation 21(3) requires all regulated firms to appoint a Nominated Officer (NO), whereas;
- Appointment of a Money Laundering Reporting Officer (MLRO) is requirement for firms who are also supervised by the Financial Conduct Authority (FCA).

The NO and the MLRO may be the same person, and this is often the case. In larger institutions with more escalations, more than one individual may be appointed as MLRO, NO or both.

Questions to ask yourself

- Have I written down how suspicious activity/behaviour should be escalated, considering all channels which it may stem from?
- Have I made staff aware of red flags of behaviour/activity which they may come across in their roles, and what they need to do if they identify it?
- Are timelines and roles and responsibilities specified in my escalation channels?
- Have I appointed a Nominated Officer, or equivalent, as well as delegate(s) to fulfil this duty in the appointed individual's absence?
- Are appropriate individuals from senior management involved in escalations, both in drawing suspicious behaviour/activity to their attention and its evaluation?

SAR filing

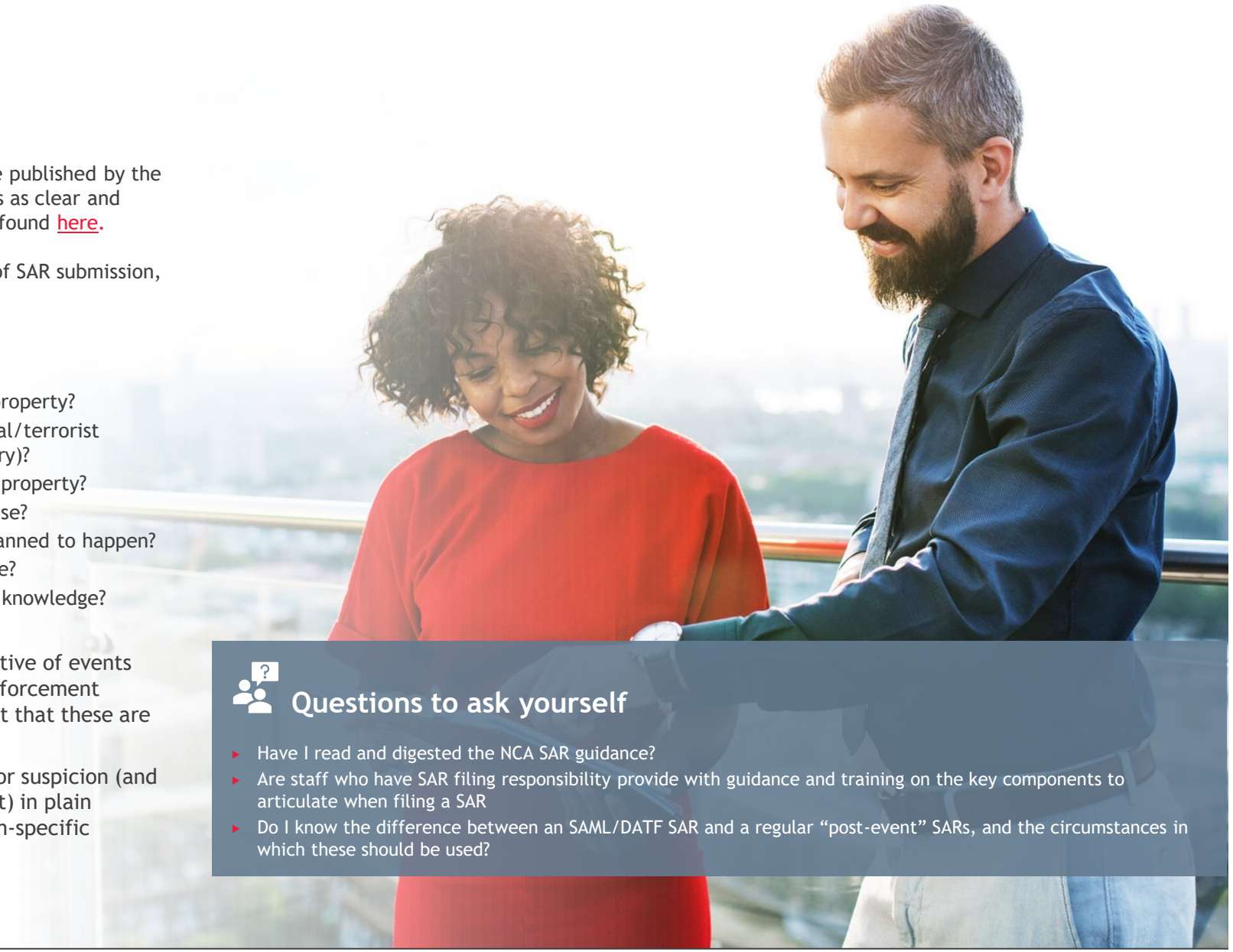
Firms should make use of guidance published by the NCA to make their SAR submissions as clear and complete as possible. This can be found here.

In the free text summary portion of SAR submission, firms should articulate:

- Who is involved?
- How are they involved?
- What is the criminal/terrorist property?
- What is the value of the criminal/terrorist property (estimated as necessary)?
- Where is the criminal/terrorist property?
- When did the circumstances arise?
- When are the circumstances planned to happen?
- How did the circumstances arise?
- Why you are suspicious or have knowledge?

SARs should set out a clear narrative of events and include details which law enforcement authorities can use, to the extent that these are available.

A good SAR sets out the reason for suspicion (and any relevant background/context) in plain English, avoiding uncommon/firm-specific acronyms and jargon.



Questions to ask yourself

- Have I read and digested the NCA SAR guidance?
- Are staff who have SAR filing responsibility provide with guidance and training on the key components to articulate when filing a SAR
- Do I know the difference between an SAML/DATF SAR and a regular “post-event” SARs, and the circumstances in which these should be used?

Know your SARs

SARs are formal reports which are filed by entities or private individuals to alert law enforcement to potential money laundering or terrorist financing. It is mandatory for a SAR to be filed in any case where there is suspicion or knowledge of money laundering or terrorist financing. In the UK, SARs are filed to the UK Financial Intelligence Unit (UKFIU), which is part of the National Crime Agency (NCA). When a SAR is filed, the UKFIU conducts further investigation into the known or suspected illicit activity.

The primary legislation in the UK which covers money laundering is the Proceeds of Crime Act (PoCA) 2002, and for terrorist financing the Terrorist Act (TACT) 2000. Both PoCA and TACT require all firms (regulated or not) to report an appropriate SAR to the UKFIU. See page 3 for this distinction.

Firms may also wish to also appoint a 'Nominated Officer' whose role it is to evaluate cases and determine whether there is sufficient suspicion to file a SAR:

- For regulated firms having a Nominated Officer is a mandatory requirement.
- For other firms it is considered best practice.

Failing to fulfil SAR obligations can result in a prosecution of 'failure to disclose'. Depending on the situation, the individual prosecuted may be the Nominated Officer or another employee:

- If the Nominated Officer failed to report suspicion which was escalated to them, it would likely be the Nominated Officer facing prosecution
- However, if an employee of a firm in the regulated sector failed to escalate internally to the Nominated Officer, the employee would be the most likely to be subject to prosecution (rather than the Nominated Officer).

Sentencing for 'failure to disclose' (for all persons in all sectors) can be an unlimited fine and/or up to 5 years in prison.

In most cases a firm will file a SAR 'post event', after activity or behaviour deemed to be suspicious has already happened or after a transaction has taken place. However, sometimes a firm will suspect money laundering or terrorist financing in advance of a transaction. Where this is the case, they should submit a DAML (Defence Against Money Laundering) SAR or DATF (Defence Against Terrorist Financing) SAR. If a DAML or DATF SAR is filed, the subject activity must be withheld for seven working days from the filing date (known as the Notice Period).

- If the firm does not hear from the NCA within the Notice Period, they may proceed with the customer transaction.
- If the transaction/activity which is the subject of a DAML/DATF is rejected by the NCA within the Notice Period, law enforcement has 31 calendar days to take action (this is known as the Moratorium Period). The Moratorium Period can be extended up to a maximum of 186 days(beyond the initial 31-day period) through application to the Crown Court. During the Moratorium Period the firm must continue to withhold the subject activity.

Post-SAR activity

Once a SAR is filed the firm should maintain open communication with the NCA, responding promptly to any law enforcement requests and production orders. For regulated firms there may be need for voluntary information sharing and filing of a 'Super SAR', which is where multiple firms compile the information/evidence that they are privy to file a joint and more comprehensive SAR.

Information relating to the filing of a SAR must be kept strictly confidential. Staff must be careful not to disclose information alerting the customer that they are under suspicion. 'Tipping off' is an offence under PoCA.

Further transactions of customers subject to a DAML or DATF SAR must be escalated to the Nominated Officer.

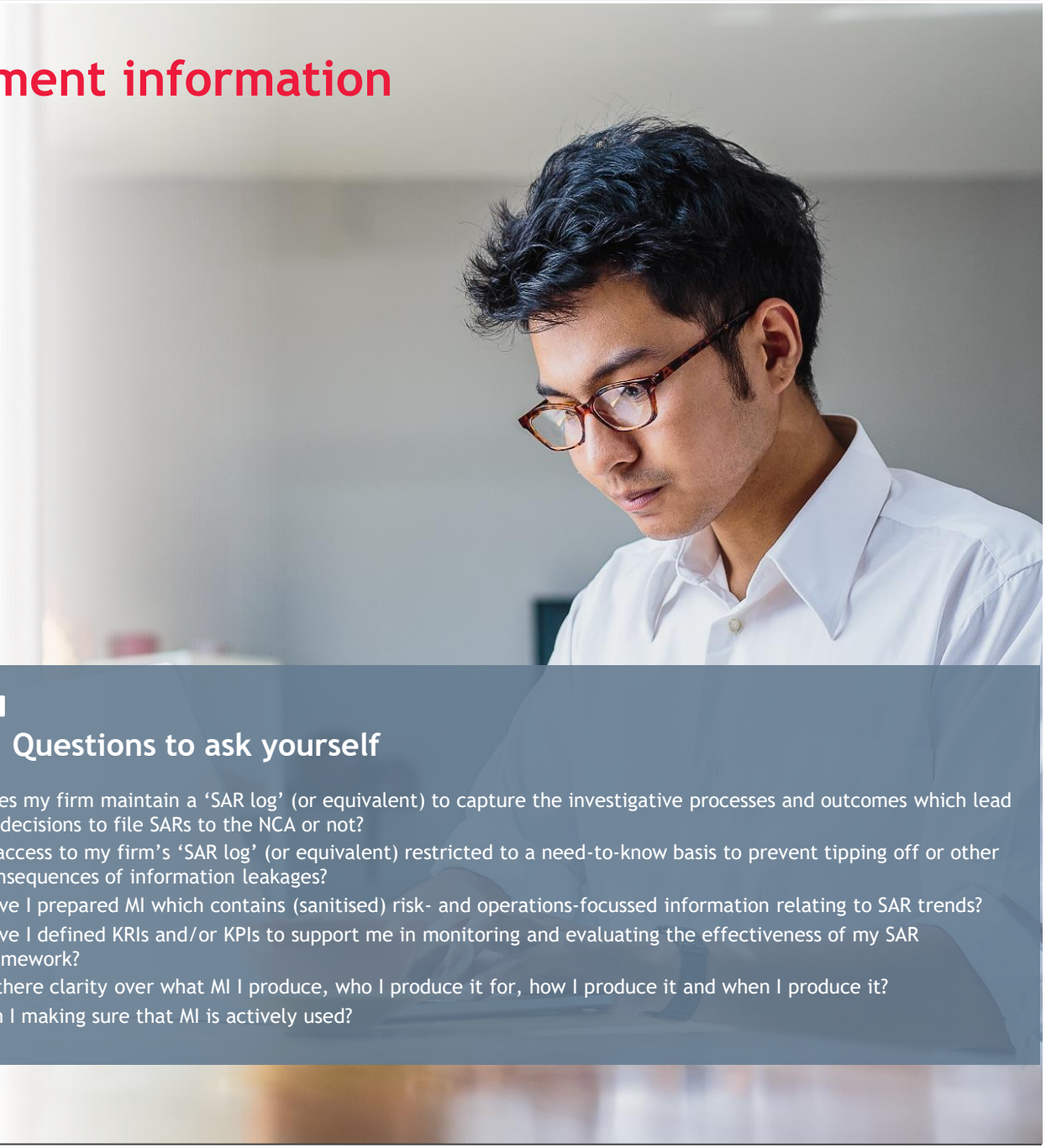
For transactions of £1,000* or more, a further DAML or DATF SAR must be submitted, and another seven working day Notice Period commences.

*On 5 January 2022, the threshold amount specified in section 339A of POCA was increased from £250 to £1,000. This amendment only affects a deposit taking body' as defined by the FCA as a bank, building society, credit union, or electronic money institution.

Questions to ask yourself

- Do my procedures guide staff on how to interact with customers following a SAR without "tipping off"?
- Do my procedures cover what steps should be taken and by whom if law enforcement requests and/or production orders are received?
- Have I clearly instructed staff about what to do (and not to do) during the Notice Period and Moratorium Period?
- Do my procedures explain what DAML/DATF SARs are, when these should be reported, and what actions must be taken once these have been reported?
- Have I updated my processes and documentation to account for the change in 'threshold amount' (if applicable)?
- Am I aware of my voluntary information sharing channels for submissions of 'SuperSARs' (if applicable)

Record keeping and management information



Firms should ensure that records maintained relating to SARs, including internal escalations which did not result in external submissions, are robust, sufficiently detailed and confidential.

Evidence should be maintained to set out:

- The steps taken at each level of investigation, and when these steps were taken
- The evidence reviewed to justify/underpin the decision taken to file a SAR or not
- The conclusion of the investigation
- The individuals involved in the investigation and decision-making process

MI about SARs should be generated and effectively used to:

- Manage operational performance, such as time taken for internal investigation
- Gain insights about customer demographics, products and services, and other factors that might inform strategic decision making
- Manage risk.

Therefore, it's important that SAR MI is shared with both operational teams as well as Senior Management.

Questions to ask yourself

- Does my firm maintain a 'SAR log' (or equivalent) to capture the investigative processes and outcomes which lead to decisions to file SARs to the NCA or not?
- Is access to my firm's 'SAR log' (or equivalent) restricted to a need-to-know basis to prevent tipping off or other consequences of information leakages?
- Have I prepared MI which contains (sanitised) risk- and operations-focussed information relating to SAR trends?
- Have I defined KRIs and/or KPIs to support me in monitoring and evaluating the effectiveness of my SAR framework?
- Is there clarity over what MI I produce, who I produce it for, how I produce it and when I produce it?
- Am I making sure that MI is actively used?

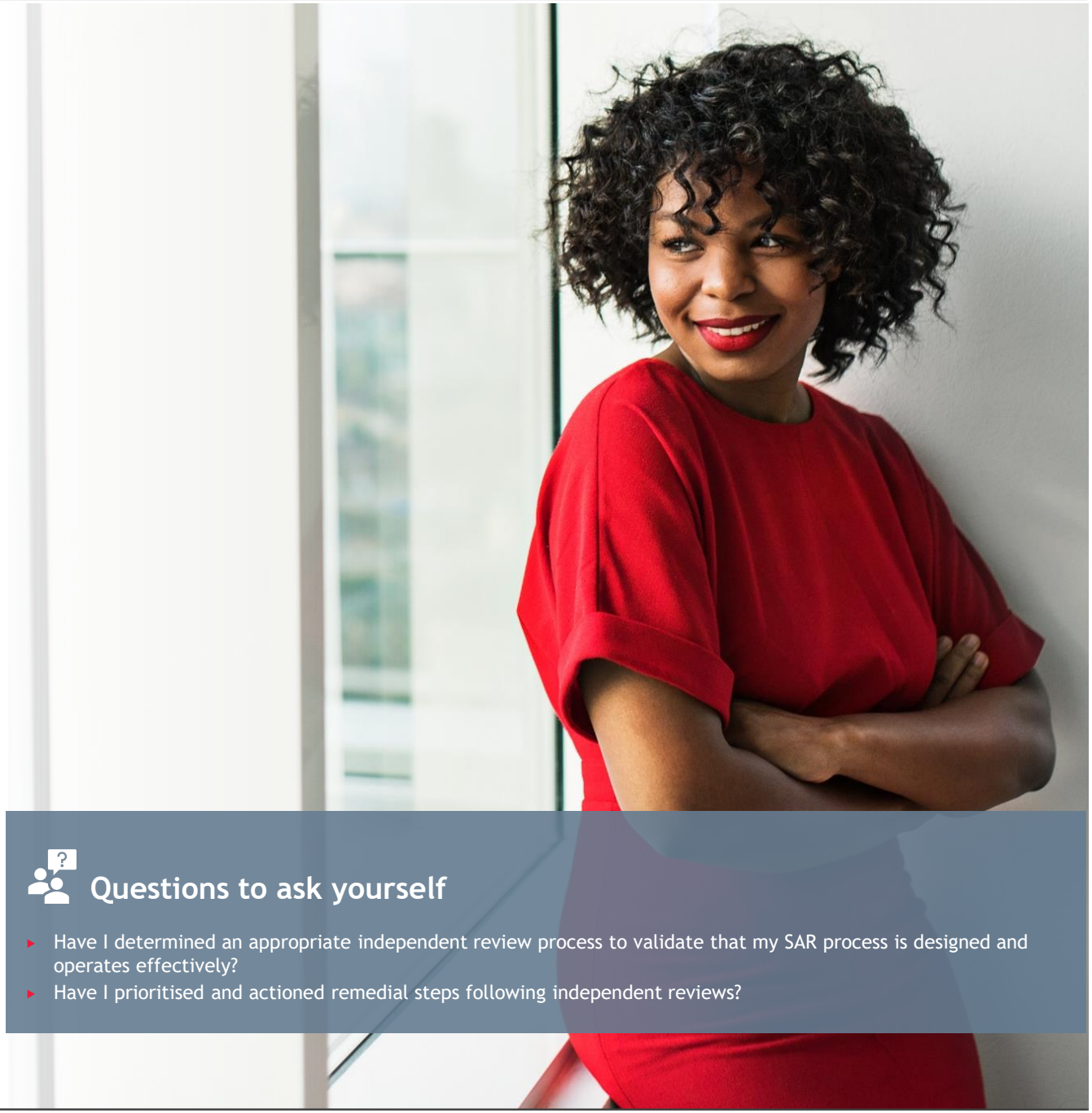
Assurance

The economic crime landscape changes rapidly and so do ‘red flags’ as criminals become increasingly sophisticated with their attempts to circumvent controls.

Firms need to make sure that their SAR framework, is well designed and up-to-date with regulation and industry best practice. It’s also crucial that wider controls feeding into the SAR framework are optimised.

The critical nature of SARs also means that firms should be assuring that their framework is operating effectively. Depending on their size and scale, firms typically benefit from:

- ‘First line’ operations teams' quality control testing to spot check and identify issues more proactively
- ‘Second line’ of defence compliance monitoring to ensure that the firm’s SAR framework is holistically operating as it should
- ‘Third line’ of defence auditing to ensure that the firms SAR policies and procedures are up to date and effective
- Assurance from a third-party expert to offer regulatory and industry best practice, and an independent view.



Questions to ask yourself

- Have I determined an appropriate independent review process to validate that my SAR process is designed and operates effectively?
- Have I prioritised and actioned remedial steps following independent reviews?

Helping you succeed

Whether you need practical advice to ensure your financial crime frameworks meet expectations, or support in dealing with regulatory actions, we can help you succeed.

Our Economic Crime Advisory team is comprised of experienced professionals with backgrounds in consultancy, industry, regulators and the NCA. We work across financial services, legal, betting & gaming, the art market, crypto and real estate, supporting firms to enhance their SAR frameworks. We provide a wide range of support and services, including SAR framework design, SAR framework independent evaluation and SAR training. These are in addition to our wider proactive or reactive economic crime compliance capabilities.

Get in touch today to find out how we can help.

Clarinda Woodford
Director
BDO Economic Crime Advisory
clarinda.woodford@bdo.co.uk

Examples of how we can help you succeed:

- SAR process design, including escalation channels and roles and responsibilities
- SAR MI design support
- SAR procedure drafting/enhancement
- SAR framework independent evaluation (design and/or operating effectiveness)
- SAR training design and delivery
- Tips relating to navigating the NCA SAR portal

BDO UK

18 OFFICES | **8,000** PEOPLE

92% OF OUR CLIENTS SAY IT'S EASY TO WORK WITH US[1]

2023/2024 RESULTS:
REVENUES[2] UP **8.6%** TO **£1.02bn**

1. BDO Tax & Advisory Client Experience Survey - Spring 2024
2. Gross Revenues for BDO LLP

IDEAS | PEOPLE | TRUST

FOR MORE INFORMATION:

Clarinda Woodford
Director
BDO Economic Crime Advisory

clarinda.woodford@bdo.co.uk

BDO