Occasional Paper

The Cartography of Compliance
On Banks, Anti-Money Laundering and Achieving Effectiveness in the UK

Inês Sofia de Oliveira, David Artingstall and Florence Keen, with Matt Russell and Ben Luddington
The Cartography of Compliance
On Banks, Anti-money Laundering and
Achieving Effectiveness in the UK

Inês Sofia de Oliveira, David Artingstall and Florence Keen,
with Matt Russell and Ben Luddington

RUSI Occasional Paper, January 2017
# Contents

- Executive Summary v
- Introduction 1
- I. Effectiveness: Working Towards Improving Compliance 5
- II. Anti-Money Laundering in the UK 9
- III. Towards a More Effective Anti-Money Laundering Regime 21
- IV. Steps Forward 35
- V. Conclusion: The Road to Effectiveness 39
- Appendix A: Survey and Interview Methodology 41
- Appendix B – Survey Questions 43
- About the Authors 51
Executive Summary

‘The UK’s anti-money laundering and counter financing of terrorism regime has a clear aim: to ensure that the UK financial system is a hostile environment for illicit finances, while minimising the burden on legitimate businesses and reducing the overall burden of regulation’.¹

Harriet Baldwin MP, former Economic Secretary to the Treasury, May 2016

The UK possesses one of the most advanced anti-money laundering (AML) legal and regulatory frameworks in the world. However, with a staggering number of suspicious activity reports received by the National Crime Agency every year and London’s infamous (although perhaps not entirely justified) reputation as the money laundering capital of the world, there is an urgent need to address any remaining inefficiencies in AML provisions in order to keep critics, as well as criminals, at bay.²

Our Approach

This paper is a collection of perceptions expressed by the private sector – in particular banks – on the field of AML and the implementation of AML provisions in the UK. Through their views, and the authors’ desk research, this report identifies the specific obstacles to effective AML provisions in the UK (not including the Crown dependencies), as well as innovative best practices that could help overcome them. Given the growing nature of the ‘compliance industry’ as a result of regulatory requirements at national and international level, this report emphasises the main challenges around the implementation and interpretation of laws as seen by practitioners and corroborated by relevant policymakers. The research has been developed with the aim of increasing knowledge about the context in which UK AML actors operate, their strategies and resources, and expectations and outcomes. In particular it set out to investigate – through a survey, interviews and a literature review – the functioning AML management structures at financial institutions (FIs), Know Your Customer procedures, investment levels and targets, the use of utilities (and third parties), as well as these institutions’ relationship with regulators and supervisors.³ This paper’s objective was to investigate and elaborate on the work being developed by the banking sector on compliance and the challenges of its implementation. Views were collected from a survey sent out to more than 60 UK-based FIs. Data were complemented with and corroborated through semi-structured interviews with the major banks drawn from the survey pool, as well as relevant government bodies and experts.

3. The Treasury is responsible for appointing anti-money laundering and counter-terrorist financing supervisors; Her Majesty’s Revenue and Customers (HMRC) is an example of a supervisor.
Our Findings

In 2015, Standard Chartered announced that there had been a fivefold increase in its financial crime staff levels in the past three years; in the same year, it was reported that HSBC was spending up to £525 million annually on its compliance and risk programme, and employs a tenth of its workforce on this function.⁴

Despite a staggering level of recent investment by banks in compliance, and attempts by the government to improve existing regulatory instruments, significant challenges to AML effectiveness persist in the UK. Among the challenges more commonly identified by interviewees were: lack of clarity over laws; fear of penalties; misguided investments and lack of resources; conflict between business priorities and regulatory obligations to implement AML systems and controls; and poor implementation of a culture of compliance. Unwillingness to comply or disagreeing with the law were not mentioned as issues.

Participants in this study suggested that challenges in interpreting requirements led to excessive defensive action – influencing both the reporting of suspicious activity reports and broader standard implementation – as well as a sub-optimal management of resources, including underinvestment in the development of internal skills. This assumption was corroborated by interviews with government officials as well as the authors’ literature and desk-based reviews. It is proposed that an effective AML framework will need to be based on clearer guidelines. Currently, the international and UK AML context has generated compliance structures that fail to reconcile the competing aims of different regulators and supervisors, so that these structures are ineffective in preventing crime. There continues to be a substantive mismatch of expectations between those who make, implement, and supervise the laws, generate guidance and advise on best practices.

Participants in this study noted that, in terms of the effectiveness of the AML regime, an organisation’s internal financial intelligence unit (FIU) has the potential to contribute to continuous improvement in their AML systems and controls. An internal FIU enables these organisations to better identify their exposure to money-laundering risk, and is perceived as necessary given their size and complexity. An organisation’s FIU is also likely to be a key participant in the UK government’s attempts to improve information sharing through the Joint Money Laundering Intelligence Taskforce (JMLIT) – although JMLIT is open to financial institutions broadly, not just those with FIUs.

Another driver of change has been the introduction of the UK Senior Managers Regime by the UK government, which is forcing banks and other financial organisations to focus on management of AML risk and the operation of AML compliance frameworks.

Analysis

This report’s objective is to suggest ways through which banks’ core business may be made more compatible with the regulatory requirements imposed on them. The research and analysis suggest that the main barriers to a more effective AML system, as identified by practitioners, relate to three main elements: people; resource management; and clarity of mission.

First, AML staff, managers and policymakers are essential to the successful implementation of requirements and best practices. At a higher level, possessing the right degree of leadership to push forward the right measures and guide staff in the most appropriate direction is considered essential to properly implementing standards. Knowledge of – and expertise in – the area are key for the effective detection of new trends and hidden threats. A broader understanding of the objectives of the AML framework was highlighted as another important aspect of the role of personnel in implementing the standards more effectively. Awareness of business objectives and the ability to promote a culture of compliance within the FIs themselves, and in a way tailored to specific institutions, also emerged as essential to future measures in improving effectiveness.

Second, correspondents stressed the need for more targeted resources and investment management, and more investment in public sector actors. The report shows that investment must be focused on the priorities and objectives defined in law in order to achieve results. However, it should also take into account internal needs and the amount of spending in relation to business objectives.

Third, this paper identifies continued uncertainty about what AML regulation hopes to achieve. Whether the objective of financial crime prevention initiatives is to disrupt crime or protect FIs remains unclear. This has led to unclear implementation of requirements and the perception of a ‘box-ticking’ mentality. An effective and compliant regime should focus more on monitoring and cooperation with law enforcement rather than on avoiding penalties. It should be guided by the risk-based approach, free of fear or misinterpretation. It should above all be clear, straightforward and facilitate easy implementation.

Recommendations

This paper finds that, although challenges to a more effective AML framework continue to be significant, a few simple adjustments and an overall increased commitment to AML could lead to radical improvements in levels of effectiveness. To summarise, in order to overcome the identified barriers and move towards a more effective AML framework, this paper makes the following recommendations:

People

- Leadership (supported by highest-level management) is crucial to the setting up and management of effective AML practices. Strong leadership would encourage the proper implementation of the risk-based approach. FIs should have a leadership that is able to
balance business priorities with compliance requirements. This in part is being addressed by the introduction of the Senior Managers Regime.

- Companies should encourage investment in knowledgeable, expert and motivated compliance professionals. Expertise should be supported through training and innovation. Hiring, training and retaining efficient compliance staff is key to building the ‘culture of compliance’ and greater effectiveness.
- Companies should nurture business awareness at all staff levels in order to implement well-rounded operations that consider the business context, specific risks and impact, along with legal imperatives.
- Companies should try to reduce the high turnover levels of staff experienced as a result of the high demand for specialised and expert compliance officers. Staff satisfaction should be improved in order to retain the right expertise and ensure that it is kept in-house. Companies should maximise levels of investment in training.
- Companies must promote a culture of compliance. Desired behaviours should be set and role modelled from the top, then ‘cascaded’ through all tiers of management. This allows employees to understand what is expected of them and why. This needs to be underpinned with support and guidance on emerging good practices, how these practices apply to specific institutions and the ways in which it is important to manage risk as a core part of business dealings.

**Resources**

- The UK government, regulators and law enforcement agencies should upgrade mechanisms and practices to respond appropriately to the efforts of FIs. Investment in AML generated by the private sector should be mirrored by equivalent capabilities within law enforcement investigation units and competent authorities. FIs need responsiveness, greater guidance, feedback and interaction to be able to comply with standards in a way that leads to real and effective results.
- Companies should build internal risk and opportunities awareness through targeted investment. The burden of compliance can be mitigated if FIs focus investment on understanding their own individual risk matrix and on the right expertise, tools and resources to manage it. These efforts should be supported by clearer guidance from regulators and law enforcement. The introduction of FIUs by organisations is a positive step in targeting investment.

**Mission**

- Regulators need to achieve greater clarity for monitoring, evaluation and enforcement regimes. Regulation – in particular the risk-based approach – is difficult to comply with due to the perception that there are moving goalposts in terms of what regulators are ‘happy with’ and penalties can be enforced ad hoc. Overall, regulatory and supervisory authorities should become more sympathetic to the ‘results-driven’ rather than formulaic nature of AML.
• Improve coordination and collaboration between actors. Platforms similar to JMLIT should be encouraged, supported and refined. It is important to foster these relationships from planning and strategic to operational and investigative levels in order to have an inclusive stakeholder approach.

• Implement AML standards with a view to maintaining the integrity of the financial system and simultaneously contributing to the disruption of crime. To increase the overall effectiveness of AML, the financial services industry must be able to operate within an independent and expert-based environment, free from political, resource or perception-related constraints.
Introduction

‘Effectiveness, Effectiveness, Effectiveness!’

Paul Simkins, Chair of the Anti-Money Laundering Supervisors Forum, May 2016

This twelve-month research project was inspired by the recognition that the current anti-money-laundering (AML) requirements, as implemented in the UK, make up a system that is not fit for purpose. We set out to investigate – through a survey, interviews and review of expert analysis – the practitioners’ perceptions of the functioning of AML management structures, Know Your Customer procedures, investment and reliance on third parties, and the relationship between companies’ AML efforts and the relevant regulators and supervisors.

‘Dirty money’ threatens the integrity of the financial system. The perceived presence of illegal capital in the regulated economy leads to a lack of market confidence, which will ultimately lead to fewer investment and trade opportunities, suspicion of corruption and potential political instability.

The introduction of illegal funds into the financial services industry and legal economies creates a distortion in public and private financial structures, and can influence credit ratings and threaten economic stability. Financial institutions (FIs) may incur reputational and financial costs, and as a result banks now find themselves on the front line in the battle against financial crime.

FIs are playing an increasingly active role in the fight against organised crime and terrorism. Figures suggest that investment in compliance is on the rise. That banks have been investing more in compliance, including AML, is not surprising given the historic fines imposed upon them in recent years for breaching AML requirements. In 2012, HSBC was fined $1.9 billion by the US for processing at least $881 million for the infamous Sinaloa cartel, perhaps the most brutal cartel in Mexico. Standard Chartered were similarly fined $300 million by the New York State

Department of Financial Services for failure to comply with the US sanctions regime against Iran. In November 2015, the Financial Conduct Authority (FCA) fined Barclays £72 million for failing to properly carry out anti-money laundering and corruption checks on a £1.88 billion transaction carried out on behalf of several politically powerful figures.

Debates on the efficacy of international regulatory standards and compliance regimes with regard to AML have long been prominent in the UK at both public and private sector levels. The repeated refrain during these debates has been the desire to create and implement a more effective system that will allow the economy to grow and the financial services industry to thrive without being shadowed by illicit financial flows.

In 2016, a report by Lexis Nexis and the British Bankers’ Association summarised the likely risks from future financial crimes:

- Increased burden of AML compliance.
- Increased personal liabilities and the subsequent impact on ‘compliance’ as an appealing career.
- The barriers to more cooperation between and within banks, regulators and law enforcement.
- Advances in technology paired with criminal methodologies innovation.

Although the UK government has made efforts to curb the ‘burden of compliance’, by reviewing and sometimes eliminating any confusing legislation or guidance, there is broad consensus among banks and expert consultants that the financial crime compliance regime implemented by the FCA fails to reflect the preferred risk-based approach. FIs fear that ongoing policy changes are insufficient to reduce the burden of compliance and ease the ever-increasing spend on complying with AML requirements.

The threat of money laundering means that FIs must strike a balance between minimising the facilitation of illicit funds and remaining competitive. As Michael Levi has argued, the trick

---

10. A risk-based approach means that countries, competent authorities and banks identify, assess and understand the money-laundering and terrorist-financing risk to which they are exposed, and take the appropriate mitigation measures in accordance with the level of risk. See Financial Action Task Force (FATF), ‘Guidance for a Risk-Based Approach: The Banking Sector’, October 2014.
of an effective regulatory regime is to minimise illegitimate exploitation, without wrecking economic dynamism.\textsuperscript{11}

This paper offers a thorough review of the perceived obstacles faced by FIs in trying to implement AML requirements and stay competitive. It analyses the strategy, resources, outputs and expectations behind implementation by taking into account the objectives set out by regulators and policymakers and identifying ways the system might be improved.

The research for this pilot project focused on FIs, their interpretation and implementation of AML and whether or not they achieve legal effectiveness (compliance with the law) and economic effectiveness (crime disruption). The analysis and recommendations are based on existing literature, industry papers, white papers and government guidance, as well as on the results of a survey carried out by PwC and RUSI\textsuperscript{12} and semi-structured interviews with private sector stakeholders, regulators, supervisors and law enforcement organisations.

The interviews were carried out with five banks which were selected from the wider survey participant lists on the basis of their size, role, impact and presence in the UK. The questions were asked in an informal setting and adapted to suit the interviewee's background and function. Interview questions for policymakers, regulators and supervisors were tweaked to fall under the same topic, but reflect the position and function of respondents.


\textsuperscript{12} The methodology for the survey and interviews is set out in Appendix A.
I. Effectiveness: Working Towards Improving Compliance

REGULATORY REQUIREMENTS WILL continue to exist and possibly increase as a result of old and emerging threats. Regulators and regulated alike persistently struggle with the implementation of AML provisions, the plethora or lack of existing guidance, and the competing priorities of their business or organisation. Efforts to transform AML actions into meaningful practices should therefore be supported, consolidated and well defined. Understanding what is meant by ‘effectiveness’ in AML is a helpful start.

The Financial Action Task Force (FATF) has recently formalised ‘effectiveness’ as an evaluative tool by adding it to the list of requirements on its mutual evaluation methodology paper,\(^1\) which until recently focused only on technical compliance.

The assessment of effectiveness has become ‘a driving force in the analysis of international relations’\(^2\) and therefore its evaluation within the implementation of AML standards will be key to actors’ performance reviews and the future development of standards. Through this focus on effectiveness, the FATF’s fourth round of mutual evaluations should produce in 2023 a revision of practices and new guidance for improved methods to identify, record, share and investigate illicit financial flows.

In theory, the principle of effectiveness is connected to that of good governance, whereby ‘citizens’ rights are respected and ... policy objectives of the ... administration are attained at the same time’.\(^3\) The core principles of good governance were recently defined by the European Commission as participation, accountability, effectiveness and coherence. These four terms are considered the pillars of good policymaking.\(^4\) Complying with these principles should therefore be standard practice in the public policymaking process, as well as in the regulator’s guidance to the private sector on implementation and its subsequent monitoring and evaluation.

From an international policymaking perspective – from where many of the AML standards emerge – the principle of effectiveness, as part of good governance, has no other objective but to ensure that measures are made applicable to national contexts as corroborated within legal

---

literature closely connected to the principle of national procedural autonomy – or the ability of states to operate in accordance with national laws.⁵

It is outside this paper’s remit to cover all principles of good governance; however, given the growing debate over effectiveness within AML realms, it does take a closer look at this particular principle and its current state of practice.

Effectiveness is defined in the literature in either legal or economic terms, depending on the expected outcomes of implementation.⁶ Legal effectiveness is defined as ‘when the norms are applied and obeyed’ and ‘when there are no legal hindrances that make reaching the goal more difficult, nor are there other factors with legal consequences that negatively influence the application of the law’.⁷ Legal effectiveness is what the majority of FIs strive towards by making sure that internal procedures follow principles established in law as well as available guidance and examples of best practice.

Economic effectiveness, on the other hand, is defined as the achievement of results related to the reduction of money laundering, terrorist financing and crime in general through the implementation of compliance requirements. Economic effectiveness is particularly difficult to measure as crime disruption relies on the action of law enforcement and prosecutors as much as on the collection and transfer of relevant financial intelligence on criminal activity. The impact that one individual institution has on the reduction of criminal activity is relative to all factors that contribute to the investigation or prosecution.

Determining whether a policy and associated practices are ‘effective’ is often difficult because it depends on the agreed definition of effectiveness, the capacity to measure a given outcome and the ability to identify the impact of individual actions within ‘the crowd’. For the majority of FIs, achieving a robust and ‘effective’ compliance system means managing risks and being able to demonstrate that sufficient action is being taken against the identified risks. Smaller organisations often use third parties to do this work, and larger organisations have had to significantly increase numbers of staff and create new financial crime compliance-specific functions.

Broadly all institutions aim to keep their business crime- and penalty-free. However, as achieving economic effectiveness becomes aspirational, is achieving full compliance with the official requirements sufficient to be deemed effective by regulators and supervisors? Or must FIs change organisational culture in addition to implementing compliance?

**Challenges to Effectiveness**

This paper identifies the principal obstacles to AML effectiveness in the UK: poor clarity of laws; fear of penalties and enforcement; sub-optimal investment and lack of resources; conflict

---

5. van den Broek, *Preventing Money Laundering*, p. 32.
between business priorities and AML; and a poor implementation of the culture of compliance and staff best practices. Without these barriers it is, arguably, possible that economic effectiveness could be achieved.

Among the most commonly mentioned challenges is the difficulty in truly understanding the mission and objectives of AML compliance as related to specific business, its reach and nature. In interviews, the leading obstacle to effectively implementing AML compliance standards was identified as the misinterpretation of requirements, guidance, typologies (methods and trends), and, especially, what to do in case those typologies do not apply. The real or perceived conflict between compliance objectives and profit motivations was the second-most mentioned obstacle.¹

The enforcement actions surrounding AML, and particularly the significant fines applied in the past, are the source of the ‘compliance by fear’ approach that was mentioned during the majority of interviews. Fines are interpreted by FIs as punitive to the institution without having any real impact on financial crime and its reduction, although they often lead to investment in compliance teams or activities. The extent to which penalties constitute a sufficient deterrent to FIs’ negligent behaviour is questionable; fines for AML breaches in the UK continue to be mostly diminutive – with the exception of Barclays – compared with those imposed on banks in the US.² Furthermore, it appears that in the UK these fines do more to harm competition – given the negative reputational effects – than they do in fighting financial crime, as pointed out by a recent report by the Treasury Select Committee, which called for the FCA to be stripped of some of its enforcement powers.³

In fact, despite an increase in regulatory fines, major compliance issues remain unresolved. In 2014, the FCA outlined the continued areas of AML weaknesses across a number of businesses, including: inadequate governance and oversight of money-laundering risk; inadequate risk assessment to identify high-risk customers; poor management of politically exposed persons (PEPs, or people in prominent public positions), particularly when establishing their source of wealth; inadequate due diligence on correspondent banks; weaknesses in handling alerts relating to sanctions and/or transaction monitoring; and poor or questionable decision-making when taking on money-laundering risk.⁴ The latter was reaffirmed in the 2015 report, as was the issue of risk management generally, and the ability to coincide business and AML requirements.⁵

---


Arguably, the lack of clarity in legislation and the fear of penalties for poor implementation are the direct causes of a poor culture of compliance and misguided investment. Without clarity and the appropriate guidance it is difficult to establish best practices and support staff with the appropriate tools. Consequently, the wider implementation of AML provisions suffers from this cascading effect, contributing to a broadly ineffective system.

The data gathered for this study suggest that these obstacles will need to be overcome if the UK wants to achieve true effectiveness in operation and implementation of AML requirements. However, ahead of learning more about the alternatives being proposed to overcome them, this paper offers an overview of the system is perceived and how obstacles have been created.
II. Anti-Money Laundering in the UK

TRILLIONS OF POUNDS of transactions are made each year through UK banks and their subsidiaries. The UK is a global financial centre due to its stability, advanced professional services sector and widely used language. As of 2016, there were more than 250 foreign banks operating in the UK and £1.55 trillion worth of assets managed in the UK for foreign clients.¹ This amounts to a figure that is almost as large as the UK’s GDP, currently estimated at approximately $2.85 trillion.²

However, it is these very characteristics that were cited by the UK National Risk Assessment of Money Laundering and Terrorist Financing as those that make the UK an attractive place to launder the proceeds of crime.³ The main threats and vulnerabilities that were identified in the assessment with regards to the banking sector included: criminals moving and storing the proceeds of crime; funnelling the proceeds of corruption; and systemic failings in AML control frameworks that allegedly facilitate money laundering and terrorist financing.⁴ Despite this, the UK government appears to be committed to the fight against money laundering and former Prime Minister David Cameron stated publicly that ‘London is not a place to stash your dodgy cash’.⁵

The Current Regime

Following the FATF Recommendations⁶ and the obligations set out by the four EU Anti-Money Laundering Directives, the UK adopted primary legislation, in the form of the Terrorism Act 2000⁷ and the Proceeds of Crime Act (POCA) 2002,⁸ providing for the criminalisation of money laundering and terrorist financing.

---

4. The UK underwent its first national risk assessment in October 2015; conducting a national risk assessment is an obligation under the FATF Recommendations. Its objective was to better understand the UK’s money-laundering and terrorist-financing risks in order to efficiently allocate resources and mitigate risks. See ibid., p. 4.
6. The FATFs ‘preventive measures’ are the best known as they can be implemented directly by FIs.
Secondary legislation, in the form of the Money Laundering Regulations 2007 (MLRs), sets out which businesses and professional activities are included in the regulated sector and gives details as to the regulatory requirements for AML that must be followed, and the supervisory powers available when regulations are not followed.¹⁰

Some of the compliance regulations fall under POCA – for example, the requirement for firms to submit suspicious activity reports (SARs) of money laundering or terrorist financing to the UK financial intelligence unit (UK FIU), which falls under the Economic Crime Command of the National Crime Agency (NCA). There is an officer responsible for submitting SARs, the money-laundering reporting officer (MLRO) or ‘nominated officer’, and failure to report suspicious activity constitutes a regulatory, and potentially criminal, offence.

**Box 1: The EU Anti-Money Laundering Directive**

Since the FATF’s inception, supranational and national bodies have created their own legal instruments in order to enact the anti-money laundering/counter-terrorist financing regime. Within the EU, the 1991 Directive on prevention of the use of the financial system for the purpose of money laundering was the first legislative measure adopted by the Council of the European Communities, which aimed to give effect to the FATF Recommendations.

The Directive fully embraced the preventive approach to money laundering, which involves protecting the proper functioning of the financial system from interference by laundering schemes. It was primarily addressed to credit and financial institutions and imposed obligations on them that were designed to ensure that money laundering was detected before the stage of criminal investigation was reached.

Its most recent manifestation, the EU’s Fourth AML Directive, agreed in June 2015, remains the keystone of the EU system. This instrument is legally binding for member states of the EU, who have implemented legislation accordingly. It is expected that all member states will have implemented the Directive’s recommendations by June 2017.

In 2015, the NCA reported that more than 380,000 SARs had been filed, around 90% of which came from the financial sector.¹⁰ Although the financial sector has been commended by organisations such as Transparency International for having the highest reporting level out of all sectors, a key concern is that as the SARs regime expands, the capacity of law enforcement is not increasing to the level required to investigate reports.

---

SARs are then disseminated to the relevant law enforcement agencies for further investigation. With regard to terrorism finance, the National Terrorist Financial Investigation Unit (NTFIU), based within Special Branch of the Metropolitan Police (SO15), has responsibility for investigating the relevant SARs, which are normally very different from the total number of SARs.

The FCA is the designated AML supervisor for FIs. It imposes its own rules, in addition to supervising compliance with the requirements of POCA and the MLRs. The FCA is at the centre of the confusion surrounding the diverse expectations that arise from AML requirements and therefore more detail about its functions and purpose is needed ahead of our analysis of the challenges faced by the private sector, especially with regard to clarifying regulatory objectives.

The Risk-based Approach

‘A truly risk-based approach to supervision will ensure that threats and vulnerabilities are effectively and efficiently mitigated, while avoiding placing unnecessary burdens on business’.\(^\text{12}\)

HM Treasury, May 2016

The FCA advocates a risk-based approach to AML, focusing on outputs. This is guided by FATF Recommendation 1:

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.\(^\text{13}\)

Firms must therefore have in place policies and procedures to assess their risks. Firms will vary in the policies they implement, depending on the different types of risks they face. The type of risk a firm is likely to face is often determined by its size. For example, larger banks operating in international markets face a greater number of risks than those operating in single jurisdictions. Whilst all are vulnerable to criminal activity, and must therefore be aware of their own risk-profile, the more cross-border the operations, the more likely it is that criminals will attempt to use the institutions for laundering the proceeds of crime. The FCA notes that firms applying a risk-based approach must be proactive in seeking information regarding threats, collating

---

information from external sources such as law enforcement agencies, as well as relying on their own judgement and experiences.\textsuperscript{14}

The risk-based approach was developed with the intention of addressing some of the criticisms that had previously been directed at AML standards – crucially, the perception that they operated with a ‘tick-box’ mentality. The approach’s core objective was to allow FIs to move beyond strict guidelines and reflect risk assessments instead.

**Consistency in Implementation?**

The International Standards Organisation defines risk as the effect of uncertainty on objectives. However, in discussions around AML/counter-terrorist financing (CTF) there is seldom an explicit or agreed definition of the risk being addressed – an increasing consensus, drawn from the security world, is to focus on threat and vulnerabilities and measure risk as a function of the two. In common language usage risks are regarded as bad things that may happen (and should be avoided where possible).

In the context of this paper, supervisors and those they supervise may have different objectives and these may not align with the stated or (more often) unstated policy objectives of the international community and national authorities. The current FATF mandate is clear about what its objectives are:

> The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. Starting with its own members, the FATF monitors countries’ progress in implementing the FATF Recommendations; reviews money laundering and terrorist financing techniques and counter-measures; and, promotes the adoption and implementation of the FATF Recommendations globally.\textsuperscript{15}

However, the broader rationale for, and approach to, AML/CTF measures is not only that they protect the integrity of the financial system, but that they also (a) reduce the amount of money laundering and terrorist financing, (b) reduce the amount of predicate crime and terrorism, or (c) do both (probably preferable from a policymaker’s point of view).

The preamble to the EU’s Fourth AML Directive also begins by referring to the integrity, stability and reputation of the financial sector. However, in the next paragraph ambitions become grander:


the objectives of protecting society from crime and protecting the stability and integrity of the Union’s financial system should be balanced against the need to create a regulatory environment that allows companies to grow their businesses without incurring disproportionate compliance costs.\textsuperscript{16}

A statement of the UK government position can be found in the AML/CTF Action Plan, which draws on the 2013 Serious and Organised Crime Strategy’s aims to substantially reduce the level of serious and organised crime affecting the UK and its interests. Money laundering is presumed to contribute to this threat by acting ‘as a critical enabler of serious and organised crime, grand corruption, and terrorism’.\textsuperscript{17} The Ministerial foreword states that:

we will not stand for money laundering or the funding of terrorism through UK institutions. We are determined to protect the security and prosperity of our citizens, and the integrity of our world-leading financial system, and will vigorously pursue those who abuse it for illicit means.\textsuperscript{18}

The Action Plan’s section on supervision is more explicit, echoing the EU’s view above:

The government’s aim for the Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) regime is to make the UK financial system a hostile environment for illicit finances, while minimising the burden on legitimate businesses and reducing the overall burden of regulation.\textsuperscript{19}

There is little detail on how these two very different objectives – ‘creating a hostile environment for illicit finances’ and ‘minimising the burden on legitimate businesses’ – are to be balanced, nor how FIs are expected to approach and measure the very different risks.

Ultimately, despite the importance of social responsibility for firms, FIs are profit-making enterprises, accountable to their shareholders. While the integrity, stability and reputation of the financial system as a whole are undoubtedly important to them – given that this is the field in which they operate and generate their profits – they are more directly concerned with the integrity, stability and reputation of their own institution. The mere existence of the AML regulatory regime implies that this self-interest has not been sufficient to incentivise them to keep criminal money out of the system. The accusation sometimes levelled at banks is that they would be happy to do whatever activity generated profits.

The wider mindset in banks may have changed to accept a degree of responsibility when it comes to dealing with crime, be it through a growing concern about the reputational damage

\begin{itemize}
\item \textsuperscript{17} Home Office and HM Treasury, \textit{Action Plan for Anti-Money Laundering and Counter-Terrorist Finance}, p. 7.
\item \textsuperscript{18} \textit{Ibid.}, p. 3.
\item \textsuperscript{19} \textit{Ibid.}, p. 44.
\end{itemize}
of association with crime or terrorism; an enhanced sense of corporate social responsibility; or an ‘entryism effect’ of recruiting large numbers of former law enforcement and intelligence operatives to their financial crime teams. However, their regulatory objective remains compliance with the law, regulations and FCA rules. This results in a mix of objectives within FIs, with some very compliance-focused (systems and controls, record keeping, monitoring) and others objective-focused (keeping criminal money out of their system, or even having some beneficial effect on levels of crime and terrorism).

The ongoing debate over ‘de-risking’ is a good example of this clash of objectives. Rightly or wrongly, FIs identify certain types of clients as too high risk for their mitigations departments to manage. Moreover, some institutions may de-risk because they simply want a ‘safer’ or different business model that does not require an intensive risk assessment, and would be more profitable. In refusing to do business with these clients they may believe that they are:

- Protecting the integrity of the financial system.
- Keeping potential criminal activity out of their bank.
- Identifying and dealing with risk in accordance with their compliance obligations.
- Choosing to change business model.

FIs are then surprised and confused to find themselves condemned by regulators, from FATF down to national level, for not doing the right thing (although there may be grudging acknowledgment that they are acting rationally), partly on the basis that their actions may drive criminal money underground where it cannot be monitored. In other words, whereas on the one hand FIs are being told to address risk, once they do it – perhaps too diligently – they receive criticism that their actions are leading to de-risking and making it harder to monitor illicit transactions. This attitude implicitly suggests that banks should prioritise the broader objective of helping to fight crime, even if that means causing potential damage to the integrity of the financial system and their own institution by accepting a high risk of introducing criminal money into it.

Policymakers thus far have been reticent to explicitly state this objective in law or regulation, preferring to rely on a fuzzily defined notion of a risk-based approach, and leaving banks to identify for themselves what those risks may be.

**The Regulators and their Regulations**

The FCA regulates but it is not the sole regulator in this field. Although it sets out certain AML rules, these are generally drawn from other requirements, such as the MLRs and the POCA, which ultimately represent the UK’s interpretation and implementation of international obligations, such as the FATF Recommendations, and are directly applicable to firms. Indeed, the FCA’s predecessor, the Financial Services Authority, withdrew its detailed Sourcebook containing rules on AML/CTF in 2006 precisely because it simply mirrored other legal requirements.

According to Regulation 24 of the MLRs, a supervisory authority must effectively monitor those persons that fall under its purview, and take necessary measures for the purpose of
securing compliance by such persons with the requirements of these Regulations. The FCA’s responsibilities extend to the financial sector, including those institutions over which the Bank of England’s Prudential Regulation Authority has regulation responsibility.

**FCA Requirements, Expectations and Guidance**

Requirements for firms are set out in the FCA Handbook, which contains various principles and rules that businesses must follow.\(^\text{20}\) The FCA has rules relating to financial crime, which require firms to establish and maintain effective systems and controls to prevent the risk that they might be used to further financial crime; there are also more detailed rules concerning money laundering specifically.

Several of the FCA’s overarching principles are considered to be especially pertinent to financial crime and money laundering. These are Principles 1 (integrity), 2 (skill, care and diligence), 3 (management and control), and 11 (relations with regulators).\(^\text{21}\) Failure to comply either with specific rules or the Principles are regulatory or compliance failings that can be dealt with either through supervisory mitigation and engagement or, in more egregious cases, through enforcement action.

**Box 2: HM Treasury on the Future of the Guidance Regime**

‘The future of the guidance regime will be considered in the AML/CTF Action Plan’s review of supervision. Concerns have been raised that the volume of Treasury-approved guidance leads to confusion for businesses, some of whom feel that they need to familiarise themselves with multiple sets of guidance, some of which is lengthy and is written in technical language. This could lead to businesses being unsure of the correct approach to take, and has the potential to contribute to disproportionate compliance and a less effective regime.’


The FCA itself characterises its approach to financial crime as requiring ‘all authorised firms to have systems and controls in place to mitigate the risk that they might be used to commit financial crime,’ which is a compliance-focused statement.\(^\text{22}\) But it goes on to say, ‘Effective systems and controls can help firms to detect, prevent and deter financial crime,’\(^\text{23}\) perhaps implying that banks have a wider responsibility to society as a whole.


The FCA also seeks to apply a risk-based approach to its supervision of banks and other FIs, and in terms of AML/CTF supervision its stated aim is to target resources at firms that represent the highest money-laundering risk, irrespective of their size, although inevitably size and systemic importance are significant factors in this risk assessment.

The FCA’s ‘Financial Crime: A Guide for Firms’ gives specific guidance on AML/CTF, including examples of good and poor practice. The status of the Guide is described as ‘general guidance’ under the Financial Services and Markets Act 2000 and it is therefore not binding (and does not contain rules). If a firm does not follow the guidance given in the Guide it will not necessarily have breached the FCA’s rules, nor will there be a presumption that it has.

The MLRs allow the Treasury to approve ‘relevant guidance’, which provides a weak form of ‘safe harbour’ – a decision-making body such as a court or tribunal has to take account of whether a person has followed relevant guidance when deciding if they have committed an offence under the Regulations. A court or tribunal may take account of other guidance, such as the FCA Guide, but has no obligation to do so.

Relevant guidance for the financial sector is found in Treasury-approved guidance issued by the Joint Money Laundering Steering Group (JMLSG), a collection of trade bodies with a secretariat hosted by the British Bankers’ Association. The JMLSG provides extremely detailed guidance on compliance with the MLRs, and is used by compliance officers to design and assess their systems and controls.

The FCA Guide therefore occupies a slightly odd position, especially as some perceive it as being – at the very least – inconsistent with the JMLSG guidance. It has no formal statutory role in either compliance with the FCA’s own rules or the Regulations; yet, according to the Guide, it is supposed to enhance understanding of FCA expectations and help firms to assess the adequacy of their financial crime systems and controls. On the other hand, the FCA is obliged to consider whether a firm has taken account of the JMLSG guidance, even if it were contrary to the FCA Guide.

According to the Guide, the FCA’s focus when supervising firms is on whether they are complying with FCA rules and their other legal obligations. This formulation may in part contribute to the view expressed in submissions to the Cutting Red Tape review that the FCA’s supervision can ‘focus on procedural requirements which are thought not be [sic] the most effective way of detecting and preventing money laundering and terrorist financing’. Of course, under the Regulations banks are obliged to carry out various procedures, such as customer due diligence and transaction monitoring. Part of any supervision of AML/CTF controls must therefore have elements of procedural checking.

The Guide does contain examples of poor practice in complying with the various obligations. Banks find these useful – along with notices of enforcement actions or new thematic reviews that contain more examples of poor practice – as they, in effect, set a minimum standard, or at least establish a canon of behaviours that banks must ensure they are not replicating. The Guide states that ‘some poor practices may be poor enough to breach applicable requirements’, which at least provides any sensible and diligent compliance officer with a ‘rule of thumb’.

More problematic, it seems, are the examples of good practice. Although the Guide itself is very clear that these are not to be seen, by either firms or supervisors, as a checklist that will ensure compliance with requirements, it is easy to understand that they could be taken as such and therefore regarded as almost equivalent to rules. In trying to be helpful, the FCA may inadvertently be stifling innovation and firms’ attempts to implement a more risk-based approach. This will very likely be the case if FCA supervisors are seen to refer too much to the good practice examples in their Guide when assessing firms, rather than focusing on desired outcomes. This leads to FIs focusing on their regulatory risk, rather than their underlying financial crime risks.

In a hypothetical world based on FATF standards, regulatory and financial crime risks would be one and the same. However, that is far from reality. This paper’s analysis of the UK AML compliance structures and the obstacles faced by them as a result of the regulatory and supervisory system illustrates the existing difficulties and suggests new ways to solve them. Ultimately, the aggregate effect of these elements of compliance – rules, laws and regulations – leaves little room for FIs to be innovative; in fact, they are incentivised not to be, which limits their ability to combat new forms of financial crime or use ‘out of the box’ thinking to tackle the current ones.

The Main Obstacles to Effectiveness and the Rise of Financial Intelligence Units

The more effective FIs are those that position the compliance function as an integrated and strategic element of their business. Compliance means to adequately implement the law. It is the process through which the protection of the integrity of the financial system is enforced by supervisory authorities on all relevant entities, including FIs, through the application of civil and/or administrative sanctions.

There is variation in how compliance within banks is enacted, with some organisations and groups publishing their own advice on best practice (for example, the Wolfsberg Group and the Basel Committee). The compliance function must be independent: while the implementation and organisation of the compliance department differs between FIs, the crucial element of its independence from other departments within the same organisation is universal.

Many FIs have interpreted the UK’s risk-based approach to AML as empowering the business (known as the first line of defence) to be responsible for the money-laundering risk associated

with their customers. Under this interpretation, the business relies on the framework for managing money-laundering risk established by the compliance function (and any risk function) which is the FI’s second line of defence, through policies, procedures and ad hoc advisory support. The compliance department is also responsible for monitoring the business for evidence of compliance with the framework as reflected in the organisation’s policies and procedures.

**Box 3: The Three Lines of Defence Model**

The first line of defence typically refers to the revenue generating part of an organisation and therefore includes the organisation’s frontline staff. An organisation’s first line of defence is referred to as ‘the business’ and is ultimately accountable for all risk and controls in the business’s processes.

The second line of defence provides oversight of the first line of defence (or ‘business’) and is made up of compliance and risk-management functions. These functions set and police policies, and oversee the business with regard to risk and compliance.

The third line of defence is responsible for ensuring independent and objective assurance on the effectiveness of risk management, internal controls and governance processes. As such, it reviews both the activities of the first and second lines of defence to ensure they are carrying out their tasks to the required level of competency. The third line of defence includes an organisation’s internal audit function.

The FCA’s Senior Managers Regime has reinforced the respective roles of business and compliance in managing an institution’s money-laundering risk. While a senior person must be held accountable for the design of the AML systems and controls (and the MLRO responsible for the bank’s compliance with its policies, procedures and relevant laws and regulations), there is an expectation that responsibility for financial crime, including money laundering, is embedded within the roles and responsibilities of senior business and other front office management. As such, how money-laundering risk is managed across the first and second lines of defence should be documented in the relevant senior manager’s responsibility statements. During the research for this paper it was found that the focus on individual accountability has been one of the biggest contributors to improving effective AML frameworks, as discussed in the following chapter.

Internal auditing is part of the third line of defence and plays a critical role in independently evaluating the risk management of the bank, and in conducting periodic evaluations of the effectiveness of compliance with AML/CTF standards. Entities should establish policies for conducting assessments of the effectiveness of their staff in implementing the bank’s policies and procedures and addressing risks; the effectiveness of compliance oversight and quality control; and the effectiveness of the bank’s training of relevant personnel.

One area of organisational change where some FIs have focused considerable effort in recent years is the internal financial intelligence unit (FIU). While the size, shape and scope of these
functions vary across those institutions that have introduced them, the common theme is that the FIU is becoming increasingly important in how an organisation manages its financial crime risk on a more proactive basis. An FIU’s methods might include: interrogating the customer base to identify related parties and transactions following enquiries from external parties; managing higher-risk customers that bank with multiple parts of the institution more centrally; assessing the institution’s vulnerability to the latest financial crime typology; and developing strategies to mitigate the risk.

The form and function of internal FIUs are typically shaped by the originating business unit, in line with the development of national FIUs. For example, those FIUs that manage higher-risk customers often have their foundations in the compliance functions that were previously responsible for enhanced due diligence as part of the customer ‘onboarding’ process. Similarly, the FIUs that are focusing on the analysis of typologies and the interrogation of customer and transaction data to identify relevant patterns and actionable events are typically located within the FI’s investigations department (often where they were already using data-mining techniques). As a result, where these functions are in operation, the team composition, skills and capabilities of the FIU, as well as the tools available, can vary considerably across the financial services industry.

Although there is no regulatory requirement for an FI to operate an internal FIU, a key external factor behind their emergence has been the regulatory focus on FIs building a complete picture or ‘single view’ of their customer. A number of FIs are using their internal FIUs to bridge the gaps between unconnected systems, to identify a customer’s touch points across the institution and determine whether this more complete picture affects their original assessment of the financial crime risk posed by the customer or any related third parties. The internal FIU enables these institutions to better identify their exposure to money-laundering risk given their size and complexity.

**Box 4: Responses to Survey (see Appendices A and B)**

Where FIUs were in place, 67% of respondents considered that the output of the FIU positively impacted the control environment relating to AML/CTF.

The US Office of the Comptroller of the Currency, for example, has censured a number of banks in recent years for their failure to take this holistic approach. In relation to the management of money laundering risk, banks were censured for failing to take into account ‘Information regarding the client’s relationships with the Bank, all lines of business within the Bank, and all Bank subsidiaries. This includes accounts within other lines of business, regions, and countries

---

While there may be a regulatory belief that banks and other FIs have a complete view of their customers, those larger institutions with a global footprint often are the product of growth through acquisition and as a consequence are struggling to satisfy these expectations. These FIs are – in practice – an amalgamation of multiple (and often incompatible) underlying legacy IT systems that are unable to link customer and transactional data in a way to realise this ambition easily, or in ‘real time’. Under these circumstances, an internal FIU is the closest proxy an institution has for a complete overview of its customers.

In terms of the effectiveness of the AML regime, the internal FIU has the potential to contribute to continuous improvement of an organisation’s AML systems and controls. First, an institution’s internal FIU is likely to be a key player in the UK government’s attempts to improve information sharing through the Joint Money Laundering Intelligence Taskforce (JMLIT). One of the objectives of JMLIT is to better understand the money-laundering risks associated with four operational priorities: bribery and corruption; trade-based money laundering; human trafficking; and terrorist financing. The internal FIUs will gather information from JMLIT, using this information to better understand their organisation’s own vulnerability to these risks, calibrating their controls accordingly. Second, in addition to consuming this external intelligence, the internal FIU should also be in a position to analyse internal sources of information, whether based on activities relating to due diligence or ongoing monitoring (manual or automated). The outcome of this analysis is relevant intelligence that can be used to further calibrate AML systems and controls, including updating the enterprise-wide risk assessment, due diligence requirements and monitoring scenarios and thresholds, where applicable.

Finally, the UK Criminal Finances Bill 2016–17 provides important additional powers that help create a financial crime-fighting architecture that matches the scale of the threat. The Bill contains several important legislative initiatives that will allow both public and private sector actors involved in efforts to disrupt money laundering, corruption and terrorist financing to operate more effectively. The Bill will transform the information sharing and disclosure relationship between public and private sectors and significantly improve the capability to recover the proceeds of crime, including international corruption.

---

III. Towards a More Effective Anti-Money Laundering Regime

The purpose of the Economic Crime Command at the NCA, in its fight against financial crime, is to ‘reduce the impact of economic crime … on UK society and the UK economy’. The purpose of this paper is to contribute to the reduction of economic crime in the economy by suggesting new ways through which FIs may be made more efficient. The definition of effectiveness used here relates to evidence of increased robustness by FIs – the absence of criminal interference in the financial services industry and their transactions – that can be derived from the full and transparent implementation of AML rules and regulations.

This paper’s interviews and the literature confirm that ‘fear of negative exposure [is] the top driver for compliance’, because it might pose an existential threat to FIs.

The evidence presented here suggests that in addition to understanding effectiveness and the real objectives of AML, it is important to ensure coherent approaches are reflected in policymaking, implementation strategies and investment decisions. Regulatory and supervisory authorities should become more sympathetic to the ‘results driven’ rather than formulaic nature of AML. In order to emphasise the focus on ‘results driven’, do we need to be more explicit about standard-setting (by government), implementation by financial institutions and supervision?

The role of people, the clarity of regulations and the proper management of resources are thought to be the three essential elements required to achieve overall effectiveness – both legal and economic. In fact, in line with the goal of maintaining the integrity of the financial system, legal effectiveness is the basis for all other actions attempting to disrupt crime.

People

Compliance teams have grown substantially, with some describing the present situation within FIs as ‘the age of the compliance officer’. But has this growth been reflected in knowledge, resources and the construction of an appropriate culture? Interviewees stressed the importance of strong recruitment policies and staff maintenance as a way to build up team expertise and contribute to more effective systems.

Determining the ideal number of compliance staff per firm or department is difficult and perhaps a fruitless task given that numbers are ultimately determined by the needs of each team, the

type of organisational structure and institution. The quality and skills of staff, however, can be shaped by the standard’s requirements and the general perception that in order to implement the risk-based approach, compliance teams must have some degree of specialisation, knowledge of business objectives and practices, as well as a belief that AML ‘makes a difference’.

The majority of interviewees agreed that ‘hiring needs to be based on personal skills and what the team needs’ and not on fulfilling standard requirements or what are typical AML functions. It may be that the key to greater effectiveness lies outside the ‘normal’ job description or expectations.

Gathered data suggest that most compliance officers continue to lack knowledge of financial crime as well as awareness of business priorities. A recent study noted, ‘banks tend to focus on specialist groups: 85 percent of banks look for staff among cybersecurity professionals; 84 percent seek staff from software companies; 61 percent from universities; 50 percent from the government intelligence community’. The data indicate that staff background continues to be limited and rarely includes those with a finance background or knowledge of the banking sector.

Business awareness was, nevertheless, emphasised by interviewees as key to building effective compliance teams. ‘More people with the right knowledge of the business’ was an oft-cited suggestion for what would make the biggest difference to compliance teams. One interviewee suggested ‘we should promote training and events, exchanges and others [sic] among teams. That would be a good way to make everyone understand what a bank is for’.?

Still, movement within FIs appears to be somewhat restricted. The reason varies depending on interviewee, but is broadly related to individual professional ambitions and the reward systems in place, as well as training and management issues.

As shown in Figure 1 (below), staffing issues are among the main challenges for FIs when it comes to complying with AML/CTF requirements, and taken as a whole represent the greatest perceived barrier to implementation.

The people behind compliance are a key part of the structure, but they are responsible for setting appropriate risk-based standards, with the business (the first line of defence) responsible for the application and implementation of those standards. Therefore, as FIs should be applying a risk-based approach, they cannot be expected to prevent and detect all instances of potential money laundering. The UK Treasury has echoed this statement, affirming that while there is a ‘clear expectation that businesses should take commensurate measures in order to

mitigate risks[,] this does not imply a “zero failure” approach. In other words, as long as risk is appropriately managed, regulators and supervisors should be ready to accept that criminal activity will still take place.

**Figure 1:** Most Significant Challenges to Compliance With AML/CTF Requirements.

A reformed AML regime would therefore reflect the difficulties identified and promote a hiring and cooperative framework focused on ‘enlisting the support of all stakeholders’ in order to ‘comply with regulatory obligations effectively and lessen the risk of potential money laundering violations and corresponding reputational risk’. This research’s interviews and survey further suggest that ‘training is essential’ and that the ‘increased feedback and interaction [promoted between public and private sector actors in the UK] is proving useful’.

---

10. Axelrod and Ross, ‘Effective AML Compliance’, p. 73.  
Currently, because there are no explicitly defined rules on how to implement compliance within a bank (merely that it must exist, and that it must be an independent function), there is huge variance in hiring and expertise-building between compliance structures across FIs.

The thinking behind compliance teams and their staffing should, in particular, be better understood so policymakers and businesses are able to determine ‘what good looks like’, if resources are to be allocated more efficiently and if a common basis for a ‘functioning’ compliance model is to be put in place. As one participant stated, ‘you can have all the rules, but it will not work unless people’s minds are in the right place’.

Interviewees suggested that promoting effectiveness through changing the current AML regime and the operation of SARs was a product of the right leadership as much as the regulatory space.

Leadership – defined as the ability to shape and influence the implementation of standards in a manner that is original, reflecting prior assessment of needs, and pertaining to a specific institution – is crucial to the revision and advancement of standards and practices. Participants interviewed for this study agreed that compliance teams that were led by dynamic and engaged managers – for instance heads of compliance and senior management – would be more likely to be deemed effective because the push, know-how and incentive to act and review practices is greater (albeit theoretically). Leadership is furthermore crucial to the degree of effectiveness that can be achieved through regulation: a good leader will go beyond ‘box-ticking’ and ensure efforts are focused on economic effectiveness rather than simply pleasing the regulator.

The majority of interviewed experts agreed that the leadership behind the implementation and management of AML efforts is crucial to its effectiveness.

Representatives from key FIs suggested that leadership alone might not be able to dramatically change what are fairly common global procedures. However, leadership can push for action in the right places or help junior staff to establish priorities, work towards the firm’s specific goals and, more importantly, build a culture of compliance from within the institution and with clear support from managing levels. This should be further supported by the fact that fines and the enforcement system are moving closer to the penalties focused on individuals through, for example, the Senior Managers Regime (see Box 5), therefore placing extra weight on individual responsibility.

Participants in this study further suggested that without leadership, FIs have little opportunity to innovate compliance beyond basic broadly acknowledged practices. The role of leaders is also to ensure that compliance teams are knowledgeable enough to justify their actions and act both preventively and effectively.

As international efforts against financial crime move forward, the importance of leadership increases. The added regulatory weight will theoretically be an incentive for good performance, implementation of good practices and more robust AML systems.

Box 5: The UK Senior Managers Regime

The UK Senior Managers Regime is forcing banks and other FIs to focus on their management of AML risk and the operation of AML compliance frameworks.

One of the key regulatory changes forcing banks to consider their approach to AML was the introduction of the Senior Managers Regime on 7 March 2016. The new regulatory regime for individuals makes it easier for regulators to hold senior executives of banks and other FIs to account over regulatory breaches.

The Senior Managers Regime focuses on individuals who hold key roles and responsibilities in relevant firms. It requires banks to clearly allocate and map out individual responsibilities. Central to this is the requirement to prepare a Statement of Responsibilities for individuals carrying out Senior Management Functions.

Individuals who fall within the Senior Managers Regime will continue to be pre-approved by regulators. Banks will also be legally required to ensure that they have procedures in place to assess their fitness and propriety before applying for approval, and they will have to reconfirm this annually.

In addition to the Senior Managers Regime, the Certification Regime applies to other staff who could pose a risk of significant harm to a bank or any of its customers (for example, staff who give investment advice or submit to benchmarks).

In terms of achieving greater clarity of mission for banks in respect of monitoring, evaluation and enforcement regimes, the Senior Managers Regime represents a significant advance. The requirement for individuals to clearly map out and be held accountable for their own responsibilities has had two complementary outcomes.

First, individuals within banks, and particularly those in senior management, have been required to recognise their personal responsibilities in respect to AML. The tighter focus on individual responsibilities has, in the opinions of those we talked to, significantly improved FIs’ understanding of their role in the effectiveness of their organisation’s AML compliance framework.

Second, there has been an improvement in the challenge and scrutiny provided by the regulator. The increased clarity around individual roles has enabled regulators (and to a lesser degree FIs themselves) to challenge the capabilities of senior management and their ability to discharge their AML responsibilities.

Overall, the introduction of the Senior Managers Regime, although still in its infancy, is being credited with having had a significant positive effect on the clarity of bank’s AML programmes and also the supervision of those programmes by regulators.
Mapping compliance is about looking to the future and planning a more effective and resource-efficient system for both private and public sectors. People are key to its achievement, through leadership, better awareness of policy needs and operational competence. As one interviewee put it, ‘what we should have more of are thought leaders’ who understand the financial crime processes and their varied stages and needs.14

In sum, efforts to create a culture of compliance have begun to bear fruit, but much more still needs to change.

Creating a Culture of Compliance

As well as questions over results and investment, there is the normative question of whether or not compliance is implemented as part of an ethical commitment, or if it is simply a way to avoid supervisory penalties. Who is responsible for the setting up of internal cultures of compliance? Do FIs move beyond what is required towards ‘creating a culture where compliance is hard-wired to values – and to the overarching strategy of the organisation’?15 As Mark Steward, Director of Enforcement and Market Oversight at the FCA, said:

Culture is in danger of becoming a buzz term, an integrated ideal of good governance, regulatory compliance and fair process. Intangible, theoretical, in danger of becoming merely regulatory, and yet another catchphrase, it cannot be bought, nor sold.16

According to the Basel Committee, compliance starts at the top, and for there to be an effective corporate culture that practises standards of honesty and integrity, it must be led by the board of directors and senior management. However, compliance is not just the responsibility of specialist compliance staff, but should be integrated into the culture of the organisation.17 A PwC report confirmed that to drive new behaviour and build trust, an ethical culture must be embedded at all levels, led by explicit behaviour and constant reinforcement from the top of the organisation. This demands much more than simply publishing a code of conduct and running online training programmes in the hope of inculcating the desired behaviours. If everyday behaviours are really to change, all the relevant elements that encourage and/or motivate people to act in certain ways must be aligned and coordinated, including incentives, training, communications, disciplinary processes and performance evaluation.18

Lori Richards, the then Director of the Office of Compliance Inspections and Examinations of the US Securities and Exchange Commission, summarised this coordinated approach as follows:

Simply put, it means instilling in every employee an obligation to do what’s right [...] when employees make decisions, large and small, and regardless of who’s in the room when they make them, and whether or not lawyers, regulators, clients, or anyone else is looking, they are guided by a culture that reinforces doing what’s right. Importantly, a firm’s Culture of Compliance exists outside the compliance department — it exists throughout the firm.19

In October 2010, Hector Sants (chief executive of the Financial Services Authority until 2012) said, ‘we want the firm to have a culture which encourages individuals to make the appropriate judgements and deliver the outcomes we are seeking. At all times we want an institution to act with integrity’.20 While the principles certainly exist, the reality of a true culture of compliance is hard to measure, and will differ between institutions.

Evidence gathered by the authors suggests that whereas some FIs show attempts at building these practices, it is still a privilege of the largest firms that have the funds, staff numbers and pressure to act. Others, which may be a little more reliant on guidance to pursue this route, still find it difficult to understand how to promote a ‘better culture’, given that the FCA guidance on the matter continues to be a little vague.21 For example, in the 2015 FCA’s ‘Financial crime: a guide for firms Part 2: Financial crime thematic reviews’ there is only one text box dedicated to examples of what constitutes good practices and ‘adequate culture’.22

Furthermore, while the practice is far from being widespread, it appears increasingly difficult to promote the belief in AML compliance given the misunderstanding of what the objective is and what kind of results matter. For example, whereas in other sections of banks the profit-making element is a clear indicator of success, with financial crime teams it is harder to measure accomplishment.

Effectiveness requires a certain degree of commitment to the practices in place and the belief that pursuing and improving these measures will lead to positive results. The degree to which practices can be analysed and compared between companies, however, has been called into question by the FCA itself. A representative recently suggested that ‘each company is unique and cannot be easily compared, according to people familiar with the situation’.23 This conclusion was not supported by all, with Labour MP John Mann saying, ‘As far as we know, the culture

22. This was furthermore confirmed by an author interview with a senior supervisor, May–June 2016.
hasn’t changed yet — that’s very clear to people. Cultural problems were fundamental to the financial crisis and remain fundamental now. Lessons haven’t been learnt’.24

Ultimately, the existence of a culture of compliance is essential for effectiveness because it influences actors’ commitment to the goal of effectiveness and their understanding of what it entails, inside and outside FIs. This culture determines which priorities are chosen and therefore what supervisors monitor, assess and evaluate.

**Resources Management**

FIs are obliged to develop, maintain and expand their compliance teams as determined by risk and legal assessments – often due to external pressure, for example the threat of fines. Existing regulation does not provide much leeway, especially for activities such as transaction monitoring, which have to follow the advice of these legal and risk assessments, resulting in the amount of investment currently ploughed into AML being much greater than for some other bank functions.

The tension between profit and compliance is more strongly felt when discussing investment priorities as a business, due to the increasing cost of compliance. However, compliance procedures are clearly important for achieving effectiveness in AML policies and therefore cannot be ignored. Interviewees suggested that compliance should be seen as part of best practice, rather than simply a way to fulfil a mandatory obligation. This approach needs to be considered in the making, implementing and revising of compliance teams and policies within banks.

**Box 6: Senior Compliance Officer on Compliance Procedures**

‘The system we have in place is very straightforward and targeted at results and protecting the bank. We want to have good results as regards disrupting crime, but our main concern is to maintain the institution at the best reputational level possible. We are here to make business and our actions reflect that’.

*Source: Author interview with senior compliance officer, May–June 2016.*

The resources dedicated to regulation and compliance within FIs are on the rise and show no sign of abating; global spending on AML compliance is set to grow to more than $8 billion by 2017 (a compounded growth rate of almost 9%).25 As financial crime continues to be a government priority, the regulators continue to support investment in these areas, frowning upon any suggested cutbacks.26

26. Author interviews with MLROs in London and New York, 2015. These interviews were conducted in the context of RUSI’s work on public–private partnerships in fighting financial crime.
In 2015, Standard Chartered announced that there had been a fivefold increase in its financial crime staff levels in the past three years;27 in the same year it was reported that HSBC were spending up to £525 million annually on its compliance and risk programme, and employs a tenth of its workforce in this function.28 Indeed, the BBA has found that their members are collectively spending at least £5 billion annually on core financial crime compliance, including enhanced systems and controls, and recruitment of staff (not including direct costs from fines for breaching AML/CTF standards).29

The picture from professionals working in the sector is illuminating: Patrick Lemmens, senior portfolio manager at Robeco, has pointed out that there is a risk of banks actually overspending, and stated that it is ‘very difficult to grasp what makes up banks’ regulatory and compliance spending’.30 Another study, carried out by Thomson Reuters, reports that:

Cost pressures are mounting with 10% of financial institutions spending approximately $100m or more on KYC [Know Your Customer]/CDD (client due diligence) and client onboarding and at the top end some financial institutions are spending in excess of $500million a year on these activities. To add to the pain, our research also shows that client onboarding costs rose by 19% last year and are expected to rise another 16% this year.31

While investment in compliance shows no sign of slowing, there are few tangible outputs through which to measure its economic effectiveness, leading many to question the state of the current system. For example, there is little evidence that money laundering has diminished as a result of greater investment in compliance by banks, more SARs being reported and/or better monitoring. Rob Gruppetta, Head of Financial Crime at the FCA, reflected this mood in a recent speech, arguing that the steps that the financial services industry takes to tackle money laundering and comply with financial sanctions are not without cost, questioning whether the correct balance had been struck between compliance costs and societal benefit.32

When questioned, the majority of participants in this study confirmed that, whereas compliance teams and structures are mostly independent, the investment and the board decisions around it are dependent on the level of risk identified and are often weighed against business priorities.33

Compliance managers interviewed claim that, as with all businesses, there is too great an expectation about what can be achieved by individuals and instead there should be more of a focus on improving the policy structure. It must be ensured that ‘the benefits we obtain outweigh [...] costs’ of poorly led compliance.\(^\text{34}\)

Investment direction varies between FIs, but a major trend appears to be reliance on third parties and investment in technology.\(^\text{35}\) A recent study found ‘implementing advanced technologies and data storage platforms will underpin [...] success in proactively combating financial crime’.\(^\text{36}\) Reliance on technology in this field has become the ‘go-to’ solution for the majority of FIs attempting to reduce costs and have better results through automation. The widely held belief is that ‘the right technology can certainly lessen [...] impact of compliance on banks’.\(^\text{37}\) Properly implemented automation can help, but it is not a panacea.

Investing in compliance – including revised strategies, new staff and new technology – is a significant part of doing business for elite FIs and an unavoidable element of managing any successful and robust institution.

However, improving effectiveness in compliance ‘is very difficult to deal with because of its highly politicised agenda’.\(^\text{38}\)

The many interests, priorities and expectations that surround compliance, particularly as it is led by regulators and supervisors, are highlighted by the growing investment in this area and the proliferation of technologies created to fix remaining gaps. Crucially, investment must be better informed, expert based and targeted, or risk falling into disrepute as just another ‘box-ticking’ exercise.

**Nearing Parity in Investment**

The great majority of those from the private sector contacted for the purpose of this study added that as far as resources are concerned, the lack of investment in law enforcement tools and instruments to deal with AML generally must be reversed. The lack of capacity to analyse SARs, to provide feedback and guide action through keeping ahead of criminal trends is proving to be another obstacle to the efforts of private actors who are left to interpret, report and act on suspicious transactions without clear assistance, responsiveness or guidance.

In an attempt to create an environment in which the financial services industry and law enforcement agencies can share and analyse SARs intelligence – as requested by the above-


\(^{35}\) According to the RUSI/PwC survey in 2016, 83% of respondents claimed an increase in reliance on third parties for AML compliance purposes.


\(^{38}\) Author interview with senior supervisor, May–June 2016.
mentioned legal instruments – the JMLIT was established in February 2015. This collaboration is seen as an essential step in protecting the UK from the security threats posed by terrorist financing and money laundering.\(^{39}\)

It is unlikely that this effort will suffice. Evidence shows that 83% of specialists believe compliance has become more complex in the last two years.\(^{40}\) FIs have responded to the growing threats identified in financial crime by increasing expenditure and overall costs in AML. The public sector must catch up, or at least demonstrate it is able to respond adequately to private sector efforts.

**Clarity of Mission**

Interviews carried out for this paper’s research found that ‘knowing what the mission’s goals are’ continues to be a challenge. Further clarification is necessary, especially to keep the legal departments at ease. Existing guidance is often open for interpretation and the fear of not doing it correctly leads to over-reliance on service providers, a tendency to over-report, and too much unstructured investment.

The UK government is currently carrying out a review of financial ‘red tape’ to which businesses are encouraged to submit evidence of any ‘over-complicated and ineffective requirements’.\(^{41}\) With regard to AML, there is a widespread assumption that while plenty of guidance is available, many FIs continue to be unsure about what exactly is required of them and, especially, what the penalties are for particular deviations from traditional guidance and practice by individuals and institutions.

In fact, at this stage it can be said that the problem is not a regulatory one, but one linked to the interpretation of requirements and their implementation in a reasonable, risk-based manner that reflects national and institution-specific money laundering and terrorist financing risk assessments.

Participants interviewed for this paper suggested that the most pressing issue is lack of clarity between the regulators’ requests and the supervisors’ demands. It is one thing to implement requirements according to the law and its interpretation, but when the supervisor’s criteria and their consequences are unclear it becomes difficult to build a coherent compliance structure. Actions are often motivated by fear of penalties and defensive action rather than on ‘expertise’ and belief in the measures being implemented.

\(^{39}\) HM Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing*. A similar initiative is the Payments Strategy Forum, which hosts a working group focused on ‘Financial Crime, Data and Security’, corroborating the importance of cooperation and exchanges in these areas.

\(^{40}\) Risk Advisory, ‘Compliance Horizon Survey 2015’.

The UK’s SARs regime is one example of how regulation is being implemented without real direction and led by fear, which creates a number of unintended consequences – not one of which is the disruption or reduction of crime.

**The SARs Regime**

The increasing pressure by regulators to report suspicious activity has become core to the implementation of standards and the assessment that is made of FIs’ effectiveness.

The regulatory pressure that is felt by FIs is especially noticeable in the implementation of the SARs regime and the reward system, culture and resource allocation that surrounds it. A recent study reported that ‘some industry commentators believe that increased regulatory scrutiny and action are redefining what a bank’s role should be’.  

However, experts emphasise that many SARs are of no use to law enforcement and yet the number of SARs submitted continues to rise. With an overload of SARs reports to process, the public sector is unable to offer an effective response to all reports. Simultaneously, as it appears to be key in demonstrating FIs’ commitment to standard implementation, the private sector continues to invest in and multiply efforts to produce SARs and make sure that nothing is left unreported.

Interviewees mentioned that results from SARs are limited and while JMLIT is a good initiative and offers some insight about what should be prioritised, not all regulated entities are covered and therefore there are still many gaps in reporting.

Interviewees also complained that reporting officers do not receive sufficient support or training to be able to contribute towards effectiveness or a proper implementation of the risk-based approach. This situation is contrary to what should be expected from the SARs regime as ‘a good SAR is a piece of information that is relevant and that we can safely say we found first. It cannot be reactive. It needs to be proactive’.

The inefficiency of the SARs regime generates difficulties at both ends of the reporting process and it has so far made no known contribution to effectiveness. The situation has been made worse by the fact that significant cuts have been made to the public sector – including the UK FIU – and ‘shifted responsibility to the private sector’ without proper consideration for whether that is the best approach or whether the right structures are in place in the private sector.

A few of the participants suggested that a ‘drastic’ change in the SARs regime structure would be desirable. ‘What if there was a system that allowed us to monitor criminal transactions

---

43. Author interview with officer from UK financial intelligence unit, May–June 2016.
44. Author interview with senior compliance officer, May–June 2016.
45. Author interview with senior compliance officer, May–June 2016.
without reporting or tipping off?” The bulk of suggestions revealed a strong scepticism that the information collected and shared would actually be able to achieve any successes or advance existing knowledge on financial crime.

The survey carried out by PwC and RUSI for the purpose of this study suggests that it is the operation of the SARs regime, rather than the idea itself (of monitoring and reporting), which is currently dysfunctional. Interviewees made suggestions for changing how the SARs regime functions, including further developing monitoring practices while focusing on different sharing, investigative and record-keeping processes overall.

Overall, the views collected in relation to the SARs regimes, as an example of excessive regulatory burden and non-effectiveness in AML, continue to support the view that ‘civil rights are trampled under foot, a fortune is spent, and no significant success is achieved or on the basis of the approach adopted, achievable’. Participants in the survey did demonstrate appreciation for transaction monitoring – the process that leads to SARs – but opinions varied about the use of SARs.

Within the current system, banks may conclude that over-reporting will protect them. ‘Defensive’ reporting ultimately does not satisfy a bank’s obligation to contribute to a sound and effective AML/CTF regime, and the quality of information should be much more important than the quantity. As one senior figure in the police has said, ‘We know the SARs regime is not fit for purpose. It is simply a defensive process adopted by banks to meet regulatory or legal requirements’.

In sum, an effective and compliant regime should focus more on monitoring and cooperation with law enforcement than on avoiding penalties. It should be guided by the risk-based approach, free of fear or misinterpretation. It should above all be clear, straightforward and able to facilitate easy implementation.

---

46. Author interview with senior compliance officer, May–June 2016.
IV. Steps Forward

In addition to the above, some changes to the internal compliance structures at FIs and UK public laws might be needed to promote alternative means of reporting poor compliance. For example, with ‘more effective whistleblowing practices and protection laws, money laundering and other financial crimes could be more effectively curbed because workers or employees with front-seat views of wrongdoings occurring in their workplace [...] are encouraged to disclose’.¹

Interviewees and the literature confirm that lower-level members of staff are often unable to ‘speak up’ against senior managers that may be involved in facilitating or ignoring money-laundering operations.² Therefore, civil society advocates believe that in addition to having ‘effective’ compliance structures in place, allowing employees and others to officially report suspicious activity within firms would significantly contribute to disrupting criminal efforts.³

Measuring effectiveness will continue to be a challenge, but if the existing literature is to be believed, one way to assess not only legal, but also economic, effectiveness in the future is by looking at the number of recorded incidents, attitudes and trends to allow a mapping of the evolution of crime in light of regulatory developments.⁴

This study’s suggestion that the perception of being compliant could, in fact, be different from the achievement of an effective AML framework is consistent with other research in developing countries, which has suggested that ‘Anti-money laundering regulation of customer record keeping has a weak impact on money laundering’.⁵ The same might apply to developed countries, but it is misleading to suggest policy inefficiency without first attempting to better the implementation process and tools already available.

This paper suggests that future action should focus on promoting a culture of compliance overall, focusing investment in priority areas as agreed with the UK government and building trust with regulators to diminish ‘fear’ and increase ‘clarity of mission’. FIs are generally able to achieve legal effectiveness, but the extent to which crime is de facto disrupted continues to be unclear and dependent on the improvement of existing practices.

3. Ibid.
AML requirements and what could be called the ‘compliance industry’ are often targeted by critics for not offering sufficient impact in the reduction of criminal offences. In fact, it has been pointed out in the literature that many FIs have been found guilty of allowing criminals to operate through their systems.\(^6\) However, the increase in the number of SARs submitted suggests that action is being taken to address criticism and, at least in some way, contribute to law enforcement monitoring and awareness of suspicious transactions. The reasons behind the submission of SARs continue to vary, although most relate to doubts about what constitutes suspicious or defensive behaviour. As the figures in Box 7 attest, FIs are the biggest submitters of SARs in the UK, indicating that there is significant action being taken around compliance requirements, although it is not clear that this action is based on a willingness to be more effective or simply comply.

What kind of action is being taken by FIs and to what extent is it having a positive effect on AML attempts? According to one of the interviewees, there are two kinds of AML operation: those that take place because they must; and those that take place because they should.\(^7\) For example, FIs investing in internal FIUs and a broader understanding of financial crime as it relates to their specific business are, allegedly, going above what is required or must be done to implement AML.

Ultimately, the ways in which FIs define their internal structures, and decide how to manage, invest and carry out compulsory compliance functions, depends directly on their institutional beliefs: that the function is either important in its own right, or that it is a ‘burden’. Interviews have shown that there is widespread conviction that the right structures cannot be built without a belief in the outcomes that the structure is designed to achieve. This paper suggests that the first step to successfully ensure legal effectiveness is the creation of an institution-wide ‘culture of compliance’ and the belief that actions in the area of compliance are not only important for legal reasons but also lead to economic effectiveness.

To a large extent, compliance teams and strategies continue to be shaped by regulatory pressure and what teams perceive to be ‘supervisors’ wishes. With increasing international efforts

---


\(^7\) Author interview with senior financial crime expert at a financial institution, May–June 2016.
to combat terrorism and tax evasion it is unlikely that this regulatory pressure will subside soon. In this context, clarification and cooperation are the only means likely to generate more effective behaviours.

RUSI interviews carried out with some of the major FIs between May and June 2016, and a survey conducted by PwC in 2016, have found that, according to FIs, the most significant challenge to compliance with AML/CTF requirements is the pace of regulatory change and the burden that this brings.\(^8\)

Although spending on compliance is likely to continue to rise as a whole, the focus of that spending is shifting. A study in the US found that businesses believed that investment in compliance staffing would fall over the coming months.\(^9\) Meanwhile, expenditure on technology, external consultants and training was predicted to either rise or remain at the same level.\(^10\) Increased investment in external training, consultants and technology are thought to be linked to the fear of fines and the belief that internal efforts alone are not enough to curb criminality.

At present, the types of investment in compliance undertaken by businesses do not appear to be guided by any particular principles, or by impact assessment exercises, but by regulatory pressure, as exemplified in the responses gathered by PwC’s Global Economic Crime Survey 2016 (see Figure 1, Chapter III).

Internal policies and compliance structures are determined by a bank’s assessment of how it can balance its commercial objectives with existing regulations, which naturally affects the ways in which compliance is pursued. Gathering additional data on specific types of investment and addressing why FIs invest in certain areas could offer an indication of the extent to which an organisation has a growing compliance ‘culture’ or whether investment in AML staff is simply a result of enforcement measures, fear of additional penalties or regulatory pressure.

Whereas several studies exist on the state of compliance – especially in the US – not many refer to, and reflect on, the structures that determine its implementation, or the issues that guide it.\(^11\) This paper begins to fill the gap that exists on the implementation of compliance and the actions that surround it in the UK. The collection of data on how AML is implemented in the UK illustrates how many FIs share the same concerns, obstacles and doubts. Understanding what these are, without the fear of giving away ‘trade secrets’, is potentially very important to reforming policies and informing future regulations.

---

10. While US-focused studies were used to inform this paper, the UK picture is believed to be similar given the importance of the financial services industry and transatlantic relationships.
V. Conclusion: The Road to Effectiveness

This paper offers an overview of the current AML regime in the UK, its structure, actors, strategies and the perceived obstacles that stand between it and effectiveness. By engaging with the relevant stakeholders, the research team mapped out compliance in the UK and the ways in which firms continue to need investment, expertise and enlightenment.

This paper finds that, while challenges to a more effective AML framework continue to be significant, a few simple adjustments and an overall increased commitment to AML could lead to radical improvements in levels of effectiveness, at least as believed by those on the job. It makes the following recommendations in order to overcome the identified barriers and move towards a more effective AML framework:

People

- Leadership (supported by highest-level management) is crucial to the setting up and management of effective AML practices. Strong leadership would encourage the proper implementation of the risk-based approach. FIs should have a leadership that is able to balance business priorities with compliance requirements. This in part is being addressed by the introduction of the Senior Managers Regime.
- Companies should encourage investment in knowledgeable, expert and motivated compliance professionals. Expertise should be supported through training and innovation. Hiring, training and retaining efficient compliance staff is key to building the 'culture of compliance' and greater effectiveness.
- Companies should nurture business awareness at all staff levels in order to implement well-rounded operations that consider the business context, specific risks and impact, along with legal imperatives.
- Companies should try to reduce the high turnover levels of staff experienced as a result of the high demand for specialised and expert compliance officers. Staff satisfaction should be improved in order to retain the right expertise and ensure that it is kept in-house. Companies should maximise levels of investment in training.
- Companies must promote a culture of compliance. Desired behaviours should be set and role modelled from the top, then ‘cascaded’ through all tiers of management. This allows employees to understand what is expected of them and why. This needs to be underpinned with support and guidance on emerging good practices, how these practices apply to specific institutions and the ways in which it is important to manage risk as a core part of business dealings.
Resources

- The UK government, regulators and law enforcement agencies should upgrade mechanisms and practices to respond appropriately to the efforts of FIs. Investment in AML generated by the private sector should be mirrored by equivalent capabilities within law enforcement investigation units and competent authorities. FIs need responsiveness, greater guidance, feedback and interaction to be able to comply with standards in a way that leads to real and effective results.
- Companies should build internal risk and opportunities awareness through targeted investment. The burden of compliance can be mitigated if FIs focus investment on understanding their own individual risk matrix and on the right expertise, tools and resources to manage it. These efforts should be supported by clearer guidance from regulators and law enforcement. The introduction of FIUs by organisations is a positive step in targeting investment.

Mission

- Regulators need to achieve greater clarity for monitoring, evaluation and enforcement regimes. Regulation – in particular the risk-based approach – is difficult to comply with due to the perception that there are moving goalposts in terms of what regulators are ‘happy with’ and penalties can be enforced ad hoc. Overall, regulatory and supervisory authorities should become more sympathetic to the ‘results-driven’ rather than formulaic nature of AML.
- Improve coordination and collaboration between actors. Platforms similar to JMLIT should be encouraged, supported and refined. It is important to foster these relationships from planning and strategic to operational and investigative levels in order to have an inclusive stakeholder approach.
- Implement AML standards with a view to maintaining the integrity of the financial system and simultaneously contributing to the disruption of crime. To increase the overall effectiveness of AML, the financial services industry must be able to operate within an independent and expert-based environment, free from political, resource or perception-related constraints.

Overall, the paper is a collection of impressions on the implementation of AML in the UK. It represents an assessment of how AML is viewed by those involved in its making and development. Its objective is to inform policymakers’ thinking and reflect on how best to achieve effectiveness as far as it is possible through improving perceptions and commitment to a more efficient system.
Appendix A: Survey and Interview Methodology

In order to collect data pertinent to this project, a list of 52 questions was drawn up to pose to relevant individuals (money laundering reporting officers, heads of compliance, etc.) in 60 financial institutions (FIs). The questions covered areas including AML risk assessments, core Know Your Customer/Customer Due Diligence controls, information sharing, compliance monitoring and governance.

The questions were drawn up with the intention of allowing the authors to collect a range of quantitative and qualitative data which could be used to understand FIs’ interpretation of AML, their compliance with the law and their economic effectiveness.

The sample was chosen to reflect a wide range of FIs, from new challenger banks to large global banks. This allowed for a difference in answers from both larger incumbent institutions and smaller streamlined businesses, which are all regulated and are required to comply with the same laws.

The survey was created using third-party software and distributed to the selected sample by email. In order to encourage FIs to participate, the survey results were anonymised and neither PwC nor RUSI is aware of which institutions answered the survey. There were unforeseen circumstances which the authors believe caused the response rate to the survey to be much lower than had been hoped. These included the leak of the ‘Panama Papers’ in April 2016, which occurred shortly after the survey was issued. There were also a number of other surveys issued earlier in 2016, including a survey by the Department for Business, Innovations and Skills, as part of its Cutting Red Tape AML Review, which reportedly caused a certain level of ‘survey fatigue’ among financial institutions.

In order to supplement the data obtained from the survey, the authors subsequently asked money-laundering reporting officers from ten financial institutions the qualitative questions from the original survey (see Appendix B).
Appendix B – Survey Questions

Institutional Reference Data/Background

1. What is your job title/role?
2. What geographies are serviced by your enterprise?
   a. UK
   b. EMEA
   c. Americas
   d. APAC
   e. Russia/Central Asia
3. Where is your enterprise headquarters located?
   a. UK
   b. EMEA
   c. Americas
   d. APAC
   e. Russia/Central Asia
4. What proportion of your turnover do you derive from the UK market?
5. Which of the following services do you offer in the UK?
   a. Retail banking
   b. Corporate and Institutional Banking
   c. Private Banking
   d. Wealth Management
   e. Asset Management
   f. Investment Banking
6. What type of customers are serviced by your UK business?
   a. Individuals
   b. SME banking
   c. Corporate
   d. Government
   e. High Net Worth
   f. Correspondent
   g. Financial Institutions
7. How many employees do you have enterprise wide (globally)?
   a. 0 - 1k
   b. 1k - 10k
   c. 11k - 50k
   d. 51k - 100k
   e. 101k - 150k
   f. 151k - 200k
   g. 200k+
8. How many employees do you have in the UK?
   a. 0 - 1k
   b. 1k - 10k
   c. 11k - 50k
   d. 51k - 100k
   e. 101k - 150k
   f. 151k - 200k
   g. 200k+

9. How many UK customers do you have?
   a. 0 - 100k
   b. 101k - 500k
   c. 501k - 1,000k
   d. 1,001k - 3,000k
   e. 3,001k+

10. How many new UK customer applications do you receive per month?
    a. 0 - 1k
    b. 1k - 5k
    c. 5k - 10k
    d. 10k+

11. What are your annual costs associated with Anti-Money Laundering (AML) / Counter Terrorist Financing (CTF) compliance in the UK for business as usual (e.g. client on-boarding, on-going compliance, transaction monitoring, etc)?
    a. 0 - £5,000k
    b. £5,001k - £10,000k
    c. £10,001k - £15,000k
    d. £15,001k - £20,000k
    e. £20,001k +

12. What are your annual costs associated with AML/CTF compliance in the UK for projects (e.g. remediation, process revision, etc.)?
    a. 0 - £5,000k
    b. £5,001k - £10,000k
    c. £10,001k - £15,000k
    d. £15,001k - £20,000k
    e. £20,001k +

13. To what extent do you agree that your spend on AML compliance returns value for money in disrupting financial crime?
    a. Prefer not to say
    b. Not at all
    c. Moderately
    d. Significantly
    e. Completely

AML/CTF Risk Assessment
14. How frequently is your UK AML/CTF risk assessment updated?
a. Monthly
b. Quarterly
c. Bi-annual
d. Yearly
e. Never

15. Does senior management sign off your UK AML/CTF risk assessment?
   a. Yes
   b. No

16. What proportion of customers of the UK business are assessed as high, medium, and low for AML/CTF risk accordingly?

17. For the UK business, do you capture data on the number of customers rejected or exited due to AML/CTF risk?
   a. Rejected - Yes/No
   b.Exited - Yes/No

18. For the UK business, approximately how many customers have been rejected and exited in the last 12 months?
   a. Number of rejected relationships
   b. Number of exited relationships

19. To what extent do you feel the risk-based approach helps you identify, resource and fund your AML/CTF risk mitigation program?
   a. Prefer not to say
   b. Not at all
   c. Moderately
   d. Significantly
   e. Completely

**Know Your Customer / Customer Due Diligence**

20. On average, how many staff hours does it take your business to perform a Customer Due Diligence (CDD) check on a customer of the UK business?
   a. Retail banking - Hours
   b. Corporate banking - Hours

21. For the UK business, what are the CDD refresh rates (period review) in years for corporate customers by high, medium and low risk?

22. How many Full Time Equivalents (FTEs) are involved in CDD/Know your Customer (KYC) activities associated with the UK business operations?

23. To what extent do you feel that the regulations and guidance relating to CDD in the UK help you to properly identify and understand the AML/CTF risks associated with your client base?
   a. Prefer not to say
   b. Not at all
   c. Moderately
   d. Significantly
   e. Completely
**Transaction Monitoring**

24. How many FTEs are dedicated to monitoring and investigating AML alerts in relation to the UK business (this excludes sanctions and Politically Exposed Person (PEP) alerts)?

25. To what extent do you agree that the customer risk rating and CDD information obtained at customer on-boarding drives your transaction monitoring activities?
   a. Prefer not to say
   b. Not at all
   c. Moderately
   d. Significantly
   e. Completely

26. How many manual, internally raised Suspicious Activity Reports (SARs) are generated by staff? How many of these are reported to the NCA?
   a. SARs Generated - Number in the last 12 months
   b. SARs Reported to the NCA - Number in the last 12 months

27. How many automated potentially suspicious activity alerts are generated? How many of these are submitted as SARs to the National Crime Agency (NCA)?
   a. Alerts Generated - Number in the last 12 months
   b. SARs Reported to the NCA - Number in the last 12 months

28. To what extent do you feel that transaction monitoring assists you or adds value in mitigating AML/CTF risk within your customer base?
   a. Prefer not to say
   b. Not at all
   c. Moderately
   d. Significantly
   e. Completely

**Reporting**

29. How many production orders for the UK business have you received in the last 12 months?

**Information Sharing and Intelligence**

30. Does your organisation have a Financial Intelligence Unit (FIU) function?
   a. Yes
   b. No

31. What activities are included within the remit of the FIU?
   a. Operational Intelligence
   b. Strategic Intelligence
   c. Investigations
   d. EDD
   e. Transaction Monitoring
   f. CDD
   g. High Risk Customers / PEPs
   h. Non-Financial Crime activities

32. How many FTEs are assigned to the FIU?
33. To what extent do you agree that the output of the FIU impacts the control environment relating to AML/CTF?
   a. Prefer not to say
   b. Not at all
   c. Moderately
   d. Significantly
   e. Completely

34. Does any other function within your organisation carry out intelligence activities relating to AML/CTF?
   a. Yes
   b. No

35. To what extent do you believe that implementing a centralised financial intelligence function would allow you to better understand and mitigate AML/CTF risks arising and/or existing within your UK operations?
   a. Prefer not to say
   b. Not at all
   c. Moderately
   d. Significantly
   e. Completely

**Compliance Monitoring and Audit**

36. Do you have a dedicated AML compliance monitoring function?
   a. Yes
   b. No

37. Do you have a dedicated AML internal audit function?
   a. Yes
   b. No

38. For the UK business, how many FTEs are responsible for compliance monitoring and internal AML audit respectively?
   a. Number of FTEs responsible for Compliance monitoring
   b. Number of FTEs responsible for Internal AML audit

39. Were there any AML internal audit findings related to the UK business in the last 12 months?
   a. Yes
   b. No

40. To what extent do you believe that compliance monitoring and AML internal audit return value for your spend in identifying failures in mitigating AML/CTF risk within UK operations?
   a. Prefer not to say
   b. Not at all
   c. Moderately
   d. Significantly
   e. Completely
Governance, Roles and Responsibilities

41. To what extent do you believe that the three lines of defence model (operations, risk and compliance, internal audit) is the correct approach to mitigating AML/CTF risks in your business?
   a. Prefer not to say
   b. Not at all
   c. Moderately
   d. Significantly
   e. Completely

42. For the UK business, how are AML/CTF duties primarily divided amongst the first, second, third lines of defence?
   a. Risk Assessment
   b. Policies and Procedures
   c. KYC/CDD
   d. Surveillance Screening
   e. Transaction Monitoring
   f. Reporting
   g. Intelligence
   h. Training

Third Party Outsourcing

43. For the UK business, what percentage of each of these AML/CTF activities are outsourced to third parties?
   a. AML/CTF Risk Assessment %
   b. Policies and Procedures %
   c. KYC/CDD %
   d. Surveillance Screening %
   e. Transaction Monitoring %
   f. Reporting %
   g. Intelligence %
   h. Training %

44. Do you believe that there is an increasing reliance by the banking industry on third parties to carry out AML/CTF related compliance activities?
   a. Prefer not to say
   b. Not at all
   c. Moderately
   d. Significantly
   e. Completely

45. What are your costs associated with third party usage, in respect of the UK business?

Sanctions and PEPs

46. For the UK business, how frequently is screening performed for a) sanctions b) PEPs? (Please select all that apply)
   a. At on-boarding
b. Daily  
c. Weekly  
d. Monthly  
e. Annually  
f. Part Transaction  
g. As part of a batch processing transaction

47. On average for the UK business, how many staff hours does it take your business to perform a screening check against a) sanctions hit b) PEP hit?
   a. 0 - 1  
   b. 1 - 2  
   c. 2 - 3  
   d. 3 - 4  
   e. 4 - 5  
   f. 5 - 10  
   g. 10 - 20  
   h. 20+

48. How many FTEs are associated with handling screening checks associated with the UK business operations for a) sanctions b) PEPs?
   a. Number of FTEs - Sanctions  
   b. Number of FTEs - PEPs

49. Number of alerts, per annum, escalated for consideration and/or further investigation relating to a) sanctions b) PEPs?
   a. Number of Alerts - Sanctions  
   b. Number of Alerts - PEPs

50. With respect to the UK business, how many accounts have you frozen in the last 12 months following a confirmed sanctions list hit?

51. With respect to the UK business, how many PEP relationships have you exited in the last 12 months?

52. To what extent do you feel that the UK’s regulatory requirements help you to mitigate the risk to your business associated with PEPs?
   a. Prefer not to say  
   b. Not at all  
   c. Moderately  
   d. Significantly  
   e. Completely
About the Authors

**Inês Sofia de Oliveira** is a Research Fellow at RUSI within the Centre for Financial Crime and Security Studies where she leads projects on illicit financial flows and works on projects aimed at improving public–private partnerships and information sharing. Inês has a PhD from the University of Edinburgh which focused on the investigation of international anti-money laundering standards.

**David Artingstall** is an independent consultant specialising in AML/CTF and regulatory risk issues. His roles as a consultant over recent years have included assignments as an international contracted expert for the IMF, Council of Europe and European Commission providing technical assistance on national AML/CTF frameworks. Prior to becoming a consultant, David held financial crime policy and intelligence roles in various public sector organisations, including the Financial Services Authority, the UK financial intelligence unit and Special Projects Branch at the National Criminal Intelligence Service, and the Metropolitan Police Special Branch, where he specialised in terrorist finance, terrorist finance intelligence and investigation.

**Florence Keen** is a Research Analyst at RUSI within the Centre for Financial Crime and Security Studies. Her work focuses on public and private responses to financial crime and terrorist finance, and she is currently undertaking research into the role of open-source and social media intelligence in tackling financial crime. She is also interested in the impact of illicit financial flows in the developing world, and drug trafficking. She holds a Master’s in Security Studies from University College London.

**Matt Russell** is a Partner in PwC’s London Forensic Services practice, specialising in the integration of financial crime investigation, detection and prevention activities within Financial Service clients, covering fraud, money laundering and market abuse. Matt leads PwC’s Global Financial Crime Operational Effectiveness initiative. This is PwC’s response to the regulatory challenge to be more outcomes-focused, helping financial institutions move from simply complying with minimum regulatory standards to developing frameworks that are driven by the effectiveness of systems and controls and their outcomes.

**Ben Luddington** is a Director in PwC’s London-based Forensic Services practice and UK Lead in financial sanctions. He is a specialist in financial services and his recent experience includes managing a team assisting a large global bank with preparation for an FCA Systematic Anti-Money Laundering Programme review. His experience also includes conducting monitoring assignments in respect of two Iranian banks in London specialising in trade finance; financial crime reviews for a number of medium-sized financial institutions; S166 reviews for the regulator into the activities of London-based banks and compliance with relevant AML requirements; and AML file reviews as part of a remediation exercise for a UK trade finance bank.