AML Guide for Fintechs
Contents

01 Introduction 3
02 Compliance & Risk Management 4

Section A – Core Compliance

03 Core Compliance Responsibilities 6
04 Appointing an MLRO 8
05 Client Due Diligence 9
  Onboarding – ID&V, CDD/KYC 9
  Ongoing Checks – Screening, Monitoring 11
  Investigations, Case Management and Actions 12
  CDD/KYC: Paper, People, Platforms 13

06 Suspicious Activity (SAR) and Other Reporting 16

07 Record Keeping 17

08 Registration and Regulators 18

Section B – Risk Management

09 From Compliance to Financial Crime Risk Management 20
10 Ongoing Risk Management 22

Section C – Putting it Together

11 Conclusion: Putting it Together 24
Financial Technology – ‘fintech’ – is one of the most promising places to be in financial services at the moment. Technological innovation has changed the landscape of banking dramatically, opening the door to new market entrants and exciting new developments across financial services; Cloud Computing has allowed businesses to use distributed networks to process data cheaply, while Application Programming Interfaces (APIs) have created channels for communication between different types of application.

Not only that, but regulatory developments have lowered many of the barriers to change. Reforms such as the European Union’s (EU) Payment Services Directive 2, which entered into force in January 2016, have allowed customers to share their data between different financial institutions. Often referred to as ‘Open Banking’, such changes have made it easier for customers to exploit many new financial possibilities. In combination, a technologically evolving industry and a supportive regulatory environment have created the space for a new Financial Technology (Fintech) ecosystem.

In any developing ecosystem, however, there are always challenges that a growing business needs to keep aware of, and – better still – tackle with the same energy that goes into delivering on customer experience. Two areas that all new banks need to navigate as they grow are getting compliance right and managing financial crime risk. In reality, these are really the same thing – if you manage your risks sensibly you are almost certainly going to be compliant – and they are also an important way to ensure a secure and sustainable customer experience. Although it can be easy to see these different areas of activity separately, they all positively reinforce each other.

At ComplyAdvantage, we are experienced with helping clients who are relatively new to some of these issues. We therefore thought it was time to consolidate and share some of the insights we have gained while working with growing companies as they develop their financial crime frameworks. There are a number of key questions the business can address early on, and if they do so intelligently, they benefit in the long-term. What we have seen clearly is that doing the right thing for your customers, your business and society, all go hand-in-hand.

This guide is not an ‘official’ handbook, but is intended to provide growing Fintechs with a checklist of key issues that they will need to consider when they are developing their financial crime framework, and some practical ways in which they can go about tackling them.

The guide therefore provides:

- An outline of core financial crime responsibilities in countries that follow the guidelines of the international standard-setter Financial Action Task Force (FATF) – which is most countries;
- Suggestions for how to take a ‘Risk Based Approach’ (RBA) to these responsibilities; and
- A set of principles and actions which can help shape your own flexible framework.

When it comes to financial crime, the key elements of success are not only knowing your obligations but truly understanding your risks. If you can develop a financial crime framework that seeks to do both – in an integrated way – then you are on the right track.
When new banks come to think about how they will respond to financial crime, the discussion quickly becomes about the concept of ‘compliance.’ In other words, whether the business is meeting legal and regulatory requirements when it comes to Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), sanctions obligations, fraud, etc.

As we suggest in the introduction, however, the concept of compliance needs to be seen in the wider context of societies’ campaigns against financial crime and the predicate crimes – human trafficking, the drugs trade, etc – that generate illicit funds. The international community looks to the financial services sector to play a full role in preventing and disrupting criminality. Compliance obligations are vital ‘minimum standards’ in that fight, but they are really only a part of what AML/CFT is about. What leading regulators are increasingly looking towards is compliance as an integral element within agile risk management, taking advantage of technology to deliver better outcomes.

Recognising that this is what tackling financial crime is really about is the first step towards a healthy approach. Meeting obligations is not only something you have to do, but is also the right thing to do. Fintechs have cultures which want to better serve customers and communities, and it makes perfect sense therefore that they should see their financial crime risk management structures as part of their mission.

However, recognising ‘compliance’ as important is only the first step. It is not so much a case of what you do, but how you do it. Because making your financial crime framework effective really comes down to the sensitivity and intelligence with which you undertake your obligations, and that means thinking about them in the context of the specific risks your business faces. A one-size fits all, blanket approach will just not work.
Section A

Core Compliance
The FATF Playing Field

If you are based or operating in the EU or the rest of Europe, your business will almost certainly be operating under a legal and regulatory financial crime framework guided by the 40 Recommendations of the Financial Action Task Force (FATF), the international standard setter for AML, CFT and other financial crimes set up by the Group of 7 leading industrialised nations in 1989.

Across the EU, these standards have been translated into national laws and regulations by a series of ‘directives’ drafted by the European Commission and approved by the EU’s Council of Ministers and Parliament. The Anti-Money Laundering Directives (AMLDs) are now on their sixth iteration, which EU member states were required to transpose into national law in December 2020 and be fully implemented by 3 June 2021.

However, most of those countries that are not part of the EU are also part of FATF, or a related organisation called ‘MONEYVAL’, which operates under the auspices of the Council of Europe, a separate organisation to the EU. This means that wherever you are in Europe, you are almost certainly operating under the broad requirements set by FATF.

National Variations

How countries implement the rules can vary somewhat, with some choosing to take a more stringent approach than the minimum standard. It is vital therefore that you acquaint yourselves with the relevant guidance coming from your national regulators such as the Autorité de Contrôle Prudentiel et de Résolution (ACPR) in France, Bafin in Germany, or the Financial Conduct Authority (FCA) in the UK, for example. Increasingly, national regulators are producing their own official handbooks to help businesses navigate their way around the detail of national law, and self-regulatory bodies and industry groups such as the Joint Money Laundering Steering Group (JMLSG) in the UK have issued guidance to flesh out how to apply the rules in a specific national context.

Core Obligations

For the purposes of this guide, however, we will focus on the core obligations which are common across the countries following FATF standards and EU AMLDs.

Each business with AML/CFT obligations sits within an ecosystem that we show in a simplified form below in the diagram below. The three key external touchpoints for a business from a financial crime perspective are with:

- **The regulator** (or regulators), which oversees the implementation and effectiveness of a business’s financial crime framework;
- **The Financial Intelligence Unit (FIU)**, a national body typically sitting within a regulatory or law enforcement agency that receives suspicious activity reporting from businesses; and
- **Clients**, who are, of course, the focus of financial crime measures, both for their protection, but also as a potential risk.
The AML/CFT Ecosystem

This ecosystem shapes the five core responsibilities of a business:

• An organisation needs to appoint a senior figure responsible in law, known as the **Money Laundering Reporting Officer (MLRO)**.

• The business must undertake an appropriate range of **Customer Due Diligence (CDD) and Know Your Customer (KYC)** measures to provide assurance about the identity and behaviour of the clients throughout the client life-cycle. This is the heart of what day-to-day compliance is about.

• In the course of undertaking CDD, businesses will sometimes find reasons for concern – possibly by finding a name on a watchlist or identifying an unusual or suspicious pattern of behaviour. If this occurs and further checks do not provide comfort, it is the obligation of the business to **report their concerns** to the authorities through authorized channels.

• **Undertaking 1–4 usually generates a significant amount of data, and in order to help the work of regulators and law enforcement, banks are expected to maintain records** on AML/CFT operations for a minimum period.

• **Obligated entities are required to undergo a registration process** with responsible regulatory bodies.

Some obligations are more straightforward to meet than others. Making sure that regulators know you exist, and that you have an MLRO in place is more straightforward than executing ongoing CDD requirements. Naturally enough, we will focus more on the ‘core operations’ in the following pages, but this should not detract from the importance of all of the obligations.
Appointing an MLRO

The basic starting point for building a resilient financial crime structure is appointing a dedicated individual responsible for AML/CFT and other anti-financial crime activities in the business. This individual is often referred to as the Money Laundering Reporting Officer (MLRO), or the ‘Nominated Officer.’ They are accountable outside the firm (to regulators), and internally (to the board and investors) for the conduct of financial crime compliance and risk management.

The MLRO’s primary responsibility is to ensure that the business has measures in place to identify any potentially suspicious activity by clients or their counterparties, and report them to the national FIU – a task we explore in more detail later.

MLROs are also usually responsible for:
- The development and oversight of financial crime related policies, procedures and control, especially around all aspects of CDD;
- The oversight and conduct of risk assessments; Maintaining records; and
- Ensuring staff are trained to recognise financial crime risks and react appropriately.

In the past, banks have tended to manage AML/CFT and fraud separately, with MLROs focusing solely on AML’s distinct regulatory obligations. However, Fintechs are increasingly looking at fraud prevention as part of the wider financial crime problem, which raises many of exactly the same questions as those raised by AML/CFT: do we know who the customer is, and does their behaviour make sense? As a result, many are taking a more integrated approach to AML/CFT and fraud, both in terms of function and leadership, but also data, platforms and technology.

Whatever the scope of the role, the choice of MLRO is incredibly significant, as it sets ‘tone from the top’ for the whole business on financial crime. That person needs to be a senior and permanent member of staff (consultants are not typically allowed), and have sufficient capability, capacity and knowledge to undertake the role. In small companies at the outset, it is not unusual for people to wear many ‘hats’, and it is not unreasonable for a senior person to ‘double hat’ as MLRO in the early days.

Even so, MLROs need to ensure they have enough knowledge and support around them to make good decisions, and businesses need to recognise that being MLRO is not something that can be done “off the side of the desk.” It needs to be taken seriously.
On the commercial side of any bank, there is a clear customer life-cycle: onboarding of the new client, expansion of the relationship with new products, and eventually the end of the relationship brought about changes on the client-side or by decision of the bank itself, typically known as ‘an exit’.

The process of Customer Due Diligence and ‘Know Your Customer’ procedures (CDD/KYC) mirror the commercial life-cycle, and are intended to monitor and manage the financial crime risks at each stage of the relationship. A large amount of effort goes into the initial stages of CDD/KYC – in other words, when a customer is being ‘onboarded’ – but the reality is that good CDD/KYC is a continuous process, making access to reliable information and agile systems essential.

**Onboarding**

The business needs to have in place standard processes and procedures for onboarding that are both fully understood by customer service staff and consistently applied by them, as well as adequate tools and technology to support them in their tasks. In a very simple way, we might describe this as the need for ‘paper, people and platforms’, a trio of requirements that can be applied across many other areas of AML/CFT.

The key elements that onboarding typically covers are:

- Identification and Verification (ID&V)
- Know Your Customer (KYC)
- Screening
- Customer Risk Assessments (CRA)
- Enhanced Due Diligence (EDD)

**Identification and Verification (ID&V)**

This usually involves the checking of standard state-issued documentation such as national ID cards, passports or driving licenses. In the past, the ID&V of new customers has been a face-to-face exercise, with in-branch staff checking and copying ID with the customer in attendance. Now, however, mobile technology, machine learning and Digital Identity (DI) schemes have made it possible to do much of this process online.

**Know Your Customer (KYC)**

Collecting client information is what compliance professionals typically think of as the essence of CDD/KYC: developing a full picture of the economic and financial status of the customer or business being onboarded. This is vital when it comes to monitoring for financial crime risks because client information provides the benchmark for what is ‘normal’ or ‘unusual’ for that customer. Historically, CDD/KYC involved the customer filling-in a hard copy form and providing a range of documentation — pay slips and utility bills for individuals, and commercial data for businesses, for example — which would be validated in-branch. Now, as with ID&V, nearly all such form-filling can be conducted online, and platforms can be used to enrich customer-provided data with information from commercially available or open access government databases.
Screening

The screening process is required to identify sanctioned individuals and others who might pose elevated financial crime risks, especially what are known as ‘Politically Exposed Persons’ (PEPs). In the screening process, businesses will compare customer names with those appearing on relevant sanctions lists (UN, EU, US and UK lists being some of the most significant for European businesses) and ensure that ‘true matches’ are not onboarded and reported to appropriate national authorities, such as the UK’s Office of Financial Sanctions Implementation (OFSI).

PEPs are altogether more challenging to identify, not least because of the variations in how countries have defined the concept. The EU has followed FATF in defining them as “individuals entrusted with a prominent public function”, including:

- Legislators;
- Ministers;
- Members of the armed forces and judiciary;
- and the senior management of state-owned enterprises.

The definition now covers both domestic and foreign officials, and also includes close relatives of those individuals. Again, businesses are required to review available lists to check for potential matches and take appropriate risk mitigation measures if a true match is found (of which more in the EDD section below).

In the past, banks conducted manual screening, but as sanctions lists have become longer and requirements more complex, most have turned to varieties of name matching technology. The leading solutions now apply machine learning algorithms not only to ensure ‘fuzzy matching’ of equivalent names (for example, transcription variations such as Husain or Hussein, or homophones such as Jacqueline and Jacklyn) but also ‘fuzzy logic’, allowing characters to be inserted, omitted or replaced (for example, matching ‘Yeltsin’ with ‘Yelstin’ or ‘Yelpin’). Such techniques can help avoid missing true positives as a result of geographic or cultural variations, spelling areas, and transliterations from non-Latin scripts.

Customer Risk Assessments (CRA)

All the information now available to the institution provides a sense of the potential inherent financial crime risk (as well as other types of risk) that come with the customer. This level of risk is valuable when it comes to calibrating the level of financial crime controls for different types of individuals, and therefore to simplify matters, at this point, banks should apply a standardised form of Customer Risk Assessment (CRA). This is typically based on a model which looks at core categories such as:

- The customer’s occupation and income/business clients’ type of business and turnover. For example, for a retail client, one consideration might be if they are in full-time employment and likely to receive a single salary payment each month, reducing the likelihood of numerous incoming payments.
- Their location and geographic areas of operation; some jurisdictions are deemed higher risk by the EU. Other particular geographic risks might need to be taken into account depending on other business client characteristics, especially in economies with bribery and corruption risks.
- The products they are using, whether they are basic retail facilities, credit, foreign exchange, etc. Some combinations of product and customer profile might be deemed higher risk than others, such as the combination of a student retail account with foreign exchange facilities.
- The channels they are likely to use, such as branches, phone or online services. Face-to-face interaction in-branch has often been treated as low risk, but ‘real-feel’ face-to-face interaction via digital channels is also advancing rapidly.
- The types of transactions they are likely to conduct, such as cash or electronic transfers. Again, high volumes of cash transactions is often perceived to be higher risk. Another key issue here links to geographic risk, and whether there is likely to be significant cross-border traffic to higher risk jurisdictions.
- Other High Risk Factors. A key issue here is whether the client is a PEP, or closely related to a PEP, and whether they might therefore be exposed to potential bribery and corruption risks. In the EU this covers domestic and overseas individuals with political exposure as well as state-owned businesses.

Using standardised inputs for these criteria which will then be weighted to reflect the business’s assessment of the significance of the risk, new clients are risk-rated with an overall high-medium-low risk rating, along with a more granular score that will place them in different positions within each group.
Enhanced Due Diligence (EDD)

Customers that are assessed to be in the high risk category are required to undergo ‘Enhanced Due Diligence’ (EDD). What EDD entails has been open to dispute in the past, but the EU’s recent directives have become more specific about what it includes, with regard to gathering additional information on:

- The background and reputation of the customer/business client
- The sources of funds or wealth of a customer
- The beneficial ownership details of a business client, and their source of wealth/funds
- The business and revenue of a business client
- The nature of the business relationship
- The reasons behind likely future transactions types

EDD also requires senior management approval for a high risk business relationship, and the implementation ongoing enhanced monitoring of customer activity (of which more in ‘Ongoing CDD/KYC’), chiefly to validate expected behaviour.

It is important to remember, however, that FATF, the EU, governments and regulators all endorse a ‘RBA’, calling for a tailored approach that is necessary and proportionate to the risks that have been identified. For example, if you have a high risk business client operating in a jurisdiction adjacent to a sanctioned country, it might make most sense to focus on their history of cross-border business and any historic sanctions problems they might have faced. Applying the same blanket EDD approach across different types of high risk customers is neither efficient or effective, and although it might seem like the path of least resistance in the short-term, it can have dangerous effects later. You will miss things.

One of the most commonly applied tools in EDD is Adverse Media Screening (AMS) or what are also called ‘negative news checks’. In many cases, businesses undertake AMS at a rudimentary level, using ‘keywords’ (eg the client’s name and a risk word such as ‘crime’) or linked ‘strings’ of keywords to look for potential issues of concern in a standard search engine. However, such techniques are inaccurate and inefficient, leading to patchy and unsystematic results.

To remedy this, financial institutions are instead turning to technology, but in many instances this involves only the use of automation; while this increases the speed of processing, it unfortunately retains the problems of the manual approach – many missed hits and the generation of false positives to be sorted through by analysts.

The better alternative is the use of Artificial Intelligence (AI), and in particular the machine learning technique of Natural Language Processing (NLP). NLP provides a rapid capacity to identify, categorise and link people, businesses and risks, in order to compile all risk-relevant adverse media related to the entity into a single profile.

Ongoing CDD/KYC

The activities described above all take place during onboarding a client, but it is vital to remember that CDD/KYC and EDD, if necessary, are not just one-off events that take place when the client walks through the door for the first time. By its very nature, due diligence should be ongoing, calibrated to a customer risk-rating.

Screening and Monitoring

The core of ongoing CDD/KYC is ensuring that we can remain confident about who the customer is, who they are interacting with, and what kind of activity they are involved in. Thus, ongoing due diligence involves three tasks:

- Ongoing Transaction Screening (TS): Banks will continue to monitor clients’ overseas transactions for potential counterparty name matches to sanctions and other watch lists.
- Ongoing Customer Monitoring: Banks will conduct new scans of their client base when watchlists or sanctions designations change, or – for high risk customers – when AMS databases have been updated.
- Ongoing Transaction Monitoring (TM): Under FATF standards, banks are expected to be able to evaluate the extent to which their clients’ behaviours are in line with expectation at onboarding, and in some jurisdictions there is a further expectation that banks will monitor clients accounts for suspicious patterns of financial behaviour that might indicate fraud, money laundering, terrorist financing, tax evasion or corruption.

Most European countries do not specify how these kinds of checks are undertaken, allowing some firms to continue to use a manual approach. However, such techniques are slow, costly and prone to errors, and firms are increasingly turning to full automation for their screening and monitoring solutions.

In the cases of transaction and name screening, platforms are similar to those used for similar tasks at on-boarding. These platforms monitor client and counterparty names for matches with existing lists, and when a potential match is found, the systems will produce an alert that can be investigated by a compliance officer.
In the cases of transaction and name screening, platforms are similar to those used for similar tasks at on-boarding. These platforms monitor client and counterparty names for matches with existing lists, and when a potential match is found, the systems will produce an alert that can be investigated by a compliance officer.

In TM, by contrast, platforms apply sets of ‘rules’ to transactions that are believed to indicate potential examples of suspicious behaviour. When a scenario matches with a pattern in the transactions, an alert comparable to a potential match in sanctions screening is issued, which then requires review. Typically, conventional TM platforms have analysed transactions retrospectively, producing high rates of false positives long after suspicious money has left an account.

More innovative solutions however are now dramatically improving this performance. Leading platforms now draw upon extensive rules libraries, which combine industry-specific rules with bespoke scenarios developed in-house, which can be reconfigured at speed through ‘soft-coding’. Such platforms increasingly allow for real-time monitoring as transactions happen, and can enrich alerts with additional data to provide a holistic customer view.

A further problem for many existing screening and monitoring systems has been their poor integration with the wider AML/CFT technology suite. In many financial institutions, standalone platforms cannot communicate effectively, meaning that the business can end up with an inconsistent view of their client across different platforms. Luckily, the best contemporary systems can now apply APIs, which effectively allow platforms to ‘talk’ to each other to provide a consistent view, and create an integrated internal AML/CFT ecosystem that ensures all platforms work together coherently.

Investigations

Ongoing screening and monitoring produce alerts that need to be investigated. Nobody can assume that every alert is valid, and there is a need for human review to validate the potential concern. In Fintechs, this can often be undertaken by the MLRO and a small number of staff, but where larger volumes of customers and transactions are involved, most banks – even relatively small ones – have dedicated teams of investigators to look at alerts through shared Case Management Systems (CMS). In the past, investigators have often been expected to conduct investigations purely using the bank’s internal data, but investigators are now increasingly being tooled-up with Social Network Analysis (SNA) tools, which allow them to identify hidden connections and access wider open source contextual information.

The larger the institution the more ‘levels’ of investigation often exist, and it is not unusual to see different types of financial crime alert be investigated by dedicated ‘AML’, ‘Fraud’ or ‘Sanctions’ teams. Although it is worth noting that even some large legacy banks are now seeking to better integrate and streamline all types of financial crime investigation in one place because of the basic similarities of the process being undertaken. As can be seen in the diagram below, there are basic similarities between different forms of monitoring which have one of three types of outcome – no further action, an internal client review, or some form of report to the authorities (discussed in the section on reporting).
Client Reviews

In the diagram, we note in stream (B) that one of the potential outcomes of an alert in ongoing screening and monitoring is a ‘CDD/KYC’ review. This – known as an ‘event driven review’ – typically occurs when investigators have looked at an alert, and come to the conclusion that there is a reason to believe the activity is unusual, there are not sufficient grounds to make a report to the authorities. The investigators will pass the case to those responsible for overseeing CDD/KYC information (possibly those involved in onboarding), and ask them to look again at what this means in terms of customer profile and behaviour. Their review can lead to changes in basic client information and also to changes in the CRA, which should of course be reflected in appropriate due diligence measures being taken. It might also possibly lead to changes in the character of the relationship if variations are significant enough, or possibly even to a client exit.

Alongside event-driven reviews, however, banks also need to schedule periodic and regular reviews to ensure that CDD/KYC is up-to-date. The scheduling and depth of these reviews is also usually driven by the risk-ranking of customers, with high risk clients reviewed once a year, medium risk every two years, and low risk every three years. However, these timescales are not set in stone, and in some cases high risk clients might be more appropriately reviewed several times a year.

CDD: Paper – People – Platforms

None of this course happens out of thin air, and as noted above, compliance processes typical have three practical underpinnings – paper, people and platforms – by which we mean there are well-articulated explanations of the activities documented (digitally, if not physically), there are individuals with responsibilities to undertake them, and they have the tools necessary to achieve their aims. As this is an initial guide rather than a textbook, we will not go into too much detail on how you might apply each of these aspects to every obligation, but we will make some general comments to point you – hopefully – in the right direction.

Paper

When you are in the thick of running a new enterprise, the idea that you need to spend your time immersed in documentation seems far from enticing. That is an arguable point with any aspect of business, of course, but it is definitely not the case with issues relating to financial crime. When you have an audit, or when the regulators come to visit, they are going to want to see documentation that explains and underpins what you are doing. Indeed, they will want to use it as a benchmark against which they will assess what you do in practice. Around each aspect of a financial crime framework, a business should look to develop three documents:

- **Policies** – which set out and codify what obligations need to be met. Having a ‘policy’ is often seen as a bureaucracy, but they do not need to change often, and act as a guide to the firm and act as confirmation to the regulator(s) that you know your responsibilities.

- **Processes** – setting out what is done to meet the policy requirements, often in a schematic way. Processes are more open to periodic change than policies.

- **Procedures** – setting out how processes are executed in practice. These are typically more like ‘how to guides’, and are the most likely document to be revised on a regular basis. They play a vitally important role in all the elements CDD.

By way of example, an EDD policy would set out the need to identify high risk clients in order to ensure that control and services in place were commensurate with the risk; the related process document would explain the CRA, the range of considerations and tools to be used during EDD, as well as the potential outcomes, and procedures would outline how, at each step, these tasks would be carried out – for example, through the use of a configured AMS search.
People

As will have been obvious when considering policies, processes and procedures, the question will be: ‘who does this?’ At the level of overall policy, there are the issues of roles, responsibility and accountability (typically resting with the MLRO), but with regards to processes and procedures, businesses need to think with a little more granularity about the the team they might need, its size, its skill-set and how embedded it is within the wider business. These decisions will depend on a number of factors, such as volumes of business, resources and perceived levels of risk (of which more, later).

In many financial institutions, basic due diligence activities at onboarding are conducted by the same customer service staff who undertake the day-to-day maintenance of the client relationships (what is often called the ‘First Line of Defence’), with ‘specialist’ financial crime activities around EDD, monitoring and investigation and the ongoing maintenance of policies, processes and procedures conducted by a separate and dedicated team around the MLRO (the ‘Second Line of Defence’ – with audit as the third). This latter team is often referred to as a ‘financial crime compliance’ function, and its structuring will again depend on the size, scope and character of the overall business. In legacy institutions, complex organizational structures have developed with multiple dedicated teams (see a typical example in the diagram).

However, in younger institutions many of these structures are simplified and integrated to ensure fewer hand-offs between different parts of the function.

At the next step down from overall structures, however, it is vital that the business gives thought to the kinds of people brought into a financial crime team. It can be a common response in a new business to bring in energetic but less-experienced individuals who are expected to learn on the job, and although this often works well, it can also need to be leavened with at least some compliance experience, whether introduced through the hiring of some staff with previous compliance experience, or the occasional use of compliance consultants or trainers. Either way, it is also important that thought is given to the development of those working on financial crime teams, as there is an evolving body of knowledge and expertise in the field of which team members should have a grasp. Useful forms of training are provided by leading professional organisations, including the Association of Certified Anti-Money Laundering Specialists (ACAMS) and the International Compliance Association (ICA).

Platforms

The further key elements are the tools the business needs to accomplish its tasks. Historically much was done manually, but it is now unusual to find banks that do not use some platforms alongside human staff, especially given modern volumes of business and type staff costs. Indeed, although platforms might seem expensive, they are invariably much cheaper and more efficient than large teams. To recapitulate the discussion above, banks will have a number of systems that cover the client life cycle and its due diligence requirements:

- **Customer Relationship Management (CRM)** systems for onboarding, managing client data, client risk assessments and ongoing relationship management;
- **Identification & Verification (ID&V)** platforms to capture identification material, now often digitally;
- **Screening** tools for sanctions, PEPs and Adverse Media;
- **Monitoring** tools for transactions;
- **Case Management Systems (CMS)** to manage alert investigation; and
- **Social Network Analysis (SNA)** tools to support investigations.
For each of these types of systems, there are a couple of questions that all new businesses ask themselves:

**How Advanced Should We Go?**

There seem to be two schools of thought here: (a) start with basic legacy models and then get more sophisticated over time; or (b) think forward and go for the long-term. Both have their attractions and their downsides; it can be reassuring to take a conventional approach that you can be confident a regulator is comfortable with, but at the same time this can lumber you with a less agile system that produces a lot of false positives, driving up your costs. Newer approaches will probably deliver improved performance and efficiency, but might (at least at first) lead to more challenging regulator interactions.

It is important to take into account that the benefits of new technology are significant. Machine Learning algorithms have the clear potential to identify and categorise individuals, business entities, along with patterns of unusual or suspicious behaviour, at volume and speed. Screening against real time data enables faster onboarding and therefore reduces account opening times, making a radical difference to efficiency and effectiveness.

These developments have been made possible by the advance of Cloud computing. A ‘Cloud’ is in effect a network of distributed servers and databases linked via the Internet, which enable the storage and access of vast volumes of data and levels of computing power. A key element in making Cloud computing work is the Application Programming Interface (API) — a communications protocol which allows different parts of the Cloud to communicate with each other. This means not only can multiple platforms operate at speed with large amounts of data, they are more agile and easier to configure, and have the potential to communicate with each in a way that most legacy systems do not. Indeed, best-in-class systems operating in the Cloud and driven by Machine Learning can dynamically refresh CDD/KYC information and risk assessments based on changing patterns of customer behaviour, integrating compliance processes like never before.

**Should We Build or Buy?**

Again, new businesses have two broad strategies with regard to this question: (a) we have technical people, so we can build our own systems; or (b) better go with a vendor. At the outset, (a) can be very attractive, especially as you are likely to have internal technical staff who have been involved in the development of client-side and customer-facing systems. It is not unusual to come across new banks that have built impressive risk engines to undertake various aspects of CDD/KYC, and which work well when the business is at an early stage. However, there is a tendency to find that, as business grows and requirements become more complex, in-house technical teams without a background or rooting in the common issues of compliance platforms can start to get out of their depth, be called upon for other projects, or simply leave the business. Key-person dependency is one of the great unspoken problems for new businesses who are dependent on niche skills.

Experience suggests therefore that new businesses need to consider how to develop a sustainable strategy on the use of in-house and vendor solutions. It is worth remembering that this does not have to be ‘all or nothing’. Your approach might be deciding to stick with your own systems, but also working with a partner that has access to, and knowledge of, the kind of risk data you need. If that is the case, then it will pay to work with a flexible partner that has demonstrable experience in the integration of systems using APIs. As you consider these options, it might be helpful to bring in external expertise, to think through the options.

If you decide to go with vendor solutions, you need to have a clear focus on what you need from each tool, the funds and resources available. Although it is perfectly reasonable to use solutions from different vendors, it comes with challenges, especially when using systems of different levels of sophistication or systems that are difficult to integrate into existing workflows. Businesses could well find that the most sustainable solution is to find a vendor that can deliver an integrated suite of solutions, removing the need to meld disparate platforms together. This can also the need for later technical remediation, and ensure that as the vendor solutions evolve, they will evolve in tandem with the wider AML/CFT suite.
When an ‘event’ such as a transaction monitoring alert or a sanctions match occurs, then the business is required to conduct appropriate investigations to validate their levels of suspicion or confirm the credibility of the match, on which the MLRO needs to sign off. Businesses are then obliged to report their concerns to the authorities via standard channels.

**SARs/STRs**

For SARs and STRs, where there are suspicions of potential money laundering or terrorist financing, these will go to national FIUs, such as Traitement du renseignement et action contre les circuits financiers clandestins (Tracfin) in France, Zentralstelle für Finanztransaktionsuntersuchungen (‘FIU’) in Germany, and the UKFIU in the UK. It is common now for FIUs to have an online portal through which to report suspicions. Each jurisdiction will have different time limits for how long the institutions to report suspicions, which are detailed on FIU websites, although it is typical that most use some form of language along the lines of ‘as soon as is possible’ after detection. Regulators can find businesses at fault not only for poor decision making when it comes to SARs, but also tardiness in reporting.

**Sanctions Violations**

For suspected sanctions violations, governments will often require businesses to make reports to relevant ministries such as foreign affairs, finance and economics, or trade, depending on the type of sanctions involved, and in some jurisdictions, there are now dedicated such as the UK’s Office of Financial Sanctions Implementation (OFSI) to which to report.

**Fraud**

When a potential fraud is detected and verified with the customer, or reported directly by the customer to the bank, it is the bank’s responsibility to take all appropriate measures to protect the customer’s account (such as the cancellation of cards, etc.) and consider the potential for reimbursement. However, it is the customer’s responsibility to report the fraud to law enforcement, unless, of course it is the bank itself which believes it has been defrauded, and the bank will typically be required to aid the police with information under an order for the production of evidence.
As the final section of the last chapter suggests, banks are expected to be in a position to help the authorities in the successful prosecution of a crime. The key to this is maintaining good and consistent data that affect all areas of compliance operations. This would include:

- **Client CDD/KYC Data** in CRM systems;
- **Transactions Data**;
- **Alerts Data** for scanning and monitoring systems;
- **Case Files** for alerts, including details of investigations undertaken and decisions made;
- Copies of Statutory Reports issued, such as SARs;
- Internal Reports leading to decisions on the nature of a relationship or potential exits.

According to the EU’s 4th AMLD, banks are required to retain securely relevant financial crime-related information for five years. Again, this is another place where Cloud computing adds value, given the potential volume of storage space available and the possibility of more easily integrating data from different compliance systems.
It might seem a little strange to place the need to register with AML/CFT competent regulators as the last ‘core’ compliance responsibility, but there is value in ensuring you have some basic compliance groundwork in place, or at the very least its implementation in train, when you register.

As part of the FATF-based framework, countries are required to have national bodies with specific oversight for the implementation of AML/CFT controls by obligated businesses, including banks. These bodies - usually described as ‘regulators’ or ‘supervisors’ are responsible for conducting regulatory examinations of individual firms, identifying problems, and enforcing punishments if necessary. It is therefore essential that you get off to a good start with your regulators by registering with them in good time and in the way they prescribe.

Commonly, AML/CFT oversight will sit alongside other forms of regulation in institutions dedicated to the financial services sector, including capital and liquidity requirements and consumer protection. In some cases in Europe, such oversight sits with the national central bank, as is the case in Italy, with the Banca D’Italia, but other jurisdictions have independent regulatory bodies for the financial services sector, such as Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) in Germany, ACPR in France, or the Financial Conduct Authority (FCA) in the UK.

Registering with these agencies will usually require the provision of information across the whole spectrum of regulatory issues and not just AML/CFT. The precise requirements of registration vary between different jurisdictions, and it is important to ensure you familiarise yourself with the requirements on the relevant regulator’s website. But all regulators will want to have a clear understanding of your business’s:

- Governance arrangements (MLROs, relationship to senior management structure, etc.);
- Internal control frameworks and mechanisms, including written policies and procedures (especially around all aspects of CDD and reporting);
- AML/CFT training programmes and materials; and
- Enterprise Wide Risk Assessment (covered in the next section).

As noted elsewhere in this guide, having good documentation to underpin your approach is an important anchor for the business, and can help increase the comfort of regulators. For new and fast moving businesses, spending time on putting together such material can seem less exciting than operational activities, but doing it well pays significant dividends when regulators come to assess how well the business is meeting its obligations.
Section B

Risk Management
From Compliance to Financial Crime
Risk Management

The previous section outlined the range of compliance obligations that businesses are legally required to fulfil. But as noted at the outset, compliance is only one part of the equation, and both FATF and the EU look to obligated businesses to take a ‘Risk Based Approach’ (RBA). This means that how these core obligations are undertaken is affected by the perceived risks involved – it is not appropriate to take a ‘one-size-fits-all’ approach.

For reasons of simplicity, we have pulled out elements of risk management from ‘core compliance’ responsibilities, but it is vital to remember that the two are inextricably linked. Developing a risk-based view of financial crime should develop alongside the creation of your core framework, rather than be added as a ‘nice to have’ later in the process.

Risk Concepts

We have seen evidence of the importance of an RBA at the customer level already, looking at the potential risks that might come with a customer, assessing that risk in a standardised way, and then calibrating the character of controls in place to match the risk posed. Indeed, the concept of EDD has evolved directly out of the need to treat customers with different risk profiles in a bespoke way.

However, businesses are also expected to take a RBA at a company as well as a customer level, with what is often called an ‘Enterprise Wide Risk Assessment’ (EWRA). In simple terms this means understanding what risks the business faces, how well the current financial crime controls mitigate them, and then what needs to be done strategically and tactically to ensure that risks and controls are aligned. When undertaking an EWRA, there are a number of key concepts to consider:

- **Risk Appetite**: The level of financial crime, reputational or regulatory risks the business is willing to bear to meet its commercial objectives. Risk appetite is typically shaped by company values and strategy, attitudes of investors and other key stakeholders, and the capacity and capability to tackle potential risks that become real issues.

- **Inherent Risk**: The level of financial crime and linked risks posed by the type of business that the company undertakes;

- **Control Effectiveness**: The mitigating impact that financial crime policies, processes and procedures (in combination what might be described as ‘controls’) have on those inherent risks; and

- **Residual Risk**: What risk is left, leading to the questions of what actions might be taken to accept and mitigate them further, depending on risk appetite.

**Conducting a Risk Assessment**

There is a lot of excellent material available about how to conduct EWRA, but one useful and straightforward model is used by The Wolfsberg Group, an association of 13 international banks dedicated to helping financial institutions identify and mitigate financial crime risks. The Group suggests a three stage process, as outlined in the diagram below.
Inherent Risks

At the first stage, an EWRA should identify the basic or ‘inherent’ risks that come with the nature of business you do, based on an assessment of the likely risks from your client base, products, services, geographies, channels of delivery, etc. In many ways this is exactly the same process that needs to be undertaken at a client level, but more strategic.

When looking at the different categories of inherent risk, businesses need to think about different types of financial crime risk (money laundering, terrorist financing, fraud, tax evasion, bribery and corruption, etc) and the potential level of risk (high–medium–low) for each category. For instance, students and young people might be considered lower risk from the perspective of tax evasion or bribery, but potentially of more concern with regard to fraud or money laundering. Payment platforms might be particularly high risk for types of fraud. As the analysis develops, a risk matrix is likely to emerge, which, taken together can provide an overview of the financial crime risks that the business faces.

Control Effectiveness

At the second stage, the business needs to assess how well its financial crime controls mitigate the risks. At the outset of a business of course, this is more about setting effective initial controls to match to ensure they keep risks within the margins of risk appetite, leaving accepted levels of residual risk. As a business grows and undertakes a cycle of EWRA’s over several years, the process often becomes more about how to recalibrate the controls in the face of a changing or better understood environment.

How to approach this task? Typically, businesses will map the elements of their control framework – especially to the key essentials of ongoing CDD/KYC – to the inherent risks identified at the first stage. For example, assessing the control effectiveness of ID & V will require a careful consideration of the client base, and their potential vulnerability to or involvement in ID fraud or identity theft. If the inherent client risks are high then a basic onboarding solution might well be inadequate. In another case, inherent product risk for remittance services might be deemed high, especially with a high volume of small transactions, but the current transaction monitoring solution might be set to high value thresholds or lack granularity in its scenarios.

As these examples suggest, the essence of reviewing control effectiveness is a form of ‘gap analysis’, providing an overview of the current vulnerabilities the business faces. If undertaken systematically, this can provide a prioritised list of those inherent risk areas and key vulnerabilities that could lead to significant problems in the future.

Residual Risk

The third and final stage of the EWRA is making decisions about what needs to be done to the control framework – whether strategically or tactically – and how the firm’s risk appetite might be affected. For example, minor problems with a transaction monitoring platform might suggest the need simply to reconfigure monitoring scenarios; in contrast, the discovery that inherent risks are not being captured and cannot be captured by a given platform can lead to the decision to replace the pre-existing solution with something more effective, or possibly even stop doing certain types of high-risk business. As a result, a well-executed EWRA is a vital tool in effective risk management for any business, acting as a useful corrective to often intuitive rather than evidence-based decision-making.
Any initial EWRA is likely to be quite basic, given a lack of experience and data. The question that businesses often ask as a result is how often they should refresh their EWRA. Although there is a recognition that risk environments change, there can often be an inertia about revisiting too quickly, given the apparent scale of the task. There is really no rule for how often to do an EWRA, but most mature businesses will schedule a ‘full-dress’ process once a year. However, as with customer reviews, EWRA should also be event-driven and respond to the evolving environment, whether negative or positive.

Triggers – Negative and Positive

An external risk trigger, such as an economic downturn, a coup, or a major public health event like the pandemic and the social restrictions is likely to act as a ready prompt to refreshing an EWRA, as too would be the planned introduction of a new product. But businesses are often much less ready to think about EWRA as the result of unexpected good news. A massive surge in customer numbers could be one such trigger. For example, if a business expects 10,000 customers in the first six months for a given product, but achieves 20,000 in three, then the environment has changed, and the business needs to consider what this means for its risk as well as celebrating its success. Although it is easy to just focus on the good news alone, it can be dangerous to do so, and some rapidly growing businesses find themselves with desperately out-of-date risk assessments and hidden and unmanaged risks. Hidden, of course, until regulators identify the problem somewhere down the line.

New Businesses and Rapid Learning

Another important consideration for new but growing businesses is around the quality and depth of their data. At the early stages, business projections and risk assessments are largely educated guesses based on very information. However, like a new-born child, a growing business is soon bombarded with a whole range of external stimuli and information that can help it better navigate its environment. In that sense, therefore, there is an argument to say that a young business should be looking at its risk assessments much more regularly than an established firm. When you are young, and growing, there is considerably more you need to take into account and learn.
Section C

Putting it Together
Sending the Right Message

At the early stages of a business, there can be a temptation to look at compliance and risk management as secondary issues, because of the assumption that they are not directly connected to growth and customer experience. However, they are important and mutually supporting factors in business success. Building-in seamless and efficient financial crime controls from the start not only protects your business and your customers, but ensures that you do not need to go through time consuming and costly remediation further down the line. It also sends a message to the regulators, the market, your customers – and the criminals – that you take these things seriously.

Risk Management as Compliance

It is also important to remember that although perfection is not possible and it is easy for businesses to fall into a ‘tick-box’ approach that focuses on doing ‘just enough’ to meet legal and regulatory requirements, more needs to be done. Businesses are expected to play a full role in the fight against financial crime, and this means understanding your business’s risk environment, and ensuring that you are prepared for it.

Framework or Risk First?

This leads to the critical questions of how you go about putting this all in place. Unfortunately, there is no ‘one size fits all’ answer. Most businesses want to have a control framework first, before then calibrating the controls to the perceived level of risk in the risk assessment. This is like building a car and then deciding how to drive it in different conditions; it demands a vehicle that is versatile and flexible, and able to master many environments.

However, there is nothing to stop a business starting with its risk assessment, and then thinking about its financial crime framework in the context of current risks, which is more like building a car with the likely driving environment in mind, resulting in a vehicle that works well in certain conditions. Both approaches have their benefits and disadvantages; for businesses where volumes of activity and risks could change rapidly, having a framework with more flexibility to change in response to the environment is key, whereas for those operating in more niche markets with greater consistency of conditions might look to a more bespoke model. Either way, an essential requirement is to ensure that the framework development and risk assessment processes fully inform the other.

Managing Expectations

How long is this all likely to take? Obviously there are going to be variations depending on the dimensions of your business, but it is safe to use a year as a rule of thumb for both designing and implementing your framework, with the design element likely to last around three months, and implementation around nine. The key issue to consider will be the dependencies; in many jurisdictions – the UK is one example – it is possible to apply for a banking license once the core compliance framework is designed and the risk assessment completed, but prior to full implementation. This can help shorten timescales. Another aspect to consider – especially when talking to vendors – is how their requirements will impact on your timescales. The quicker you want to be able to move to market, the more responsive your vendor needs to be.

Conclusion: Putting it Together
Focus on the Goal:
Compliance and risk management are there to help tackle financial crime, first and foremost. Keep that in mind when you are making decisions about your approach.

Take a Holistic View:
Compliance and risk management support business success, and compliance and risk management support each other. They are not mutually exclusive.

Integrate Early:
Do not wait to ‘add on’ a financial framework to your business model somewhere down the line; make sure it is fully integrated into your approach from the start to manage costs and client experience.

Balance Sustainability and Flexibility:
Ensure your framework has the resilience and scope to ‘flex’ in the face of changing circumstances, especially if you are looking to grow quickly or face an uncertain risk landscape. That will almost certainly require the intelligent use of technology.

Find the Right Partners:
Look for partners who are keen to deliver solutions that support your needs and meet your risks, and have the capability and capacity to respond with agility.
About ComplyAdvantage

ComplyAdvantage is the financial industry’s leading source of AI–driven financial crime risk data and detection technology. ComplyAdvantage’s mission is to neutralize the risk of money laundering, terrorist financing, corruption, and other financial crime. More than 500 enterprises in 75 countries rely on ComplyAdvantage to understand the risk of who they’re doing business with through the world’s only global, real-time database of people and companies. The company actively identifies tens of thousands of risk events from millions of structured and unstructured data points every single day. ComplyAdvantage has four global hubs located in New York, London, Singapore and Cluj–Napoca and is backed by Ontario Teachers’, Index Ventures and Balderton Capital. Learn more at:

complyadvantage.com

Our Customers

Get in Touch

**EMEA**  
London  
+44 20 7834 0252  
[Demo Request](#)

**AMER**  
New York  
+1 (646) 844 0841  
[Demo Request](#)

**APAC**  
Singapore  
+65 6304 3069  
[Demo Request](#)