Building and scaling a financial crime team

cable

Cable is building innovative technology to reduce the amount of financial crime in the world.

Financial crime comes with devastating consequences – from the horrific human cost to the downstream impact on government, businesses and communities – but despite increased regulations and global efforts, we are still failing in the fight to prevent it.

Banks and financial institutions are paying the price, with more than $2.3bn of fines given every year for failures to do with anti-financial crime regulation, and each fine averaging $100m. Of those fines, nearly half mention ineffective controls.

These numbers are all increasing and they don't even include the cost of remediation.

How can anyone get more effective at something, if they don't know how effective they are right now? And how can banks and financial institutions know how effective they really are, when the only way to find out is by limited manual review of a tiny percentage of accounts or transactions?

Cable provides automated, independent effectiveness testing and assurance of financial crime controls. We help banks and financial institutions understand and improve the effectiveness of those controls, and help them to save time and money.

Contents

Introduction

NATASHA VERNIER
CO-FOUNDER AND CEO, CABLE

For almost every financial institution, the first step in fighting financial crime is to hire some experts and build an anti-financial crime program. Given the fundamental importance of getting this right, there is remarkably little guidance and advice on how to build and scale a financial crime team in an effective way.

When I was building the financial crime team at Monzo Bank back in 2016, we had the fantastic opportunity to think about how to structure the team and build tools and infrastructure in an innovative way. At the time, what we did was new and different, and I am extremely proud of where we got to. I was, and am still, often asked what we did and how we did it, and as time goes on, I realise how many excellent examples of financial crime teams exist in the fintech ecosystem that look totally different to what we did at Monzo.

And so as we at Cable begin our journey of improving the effectiveness of financial crime teams around the world, we want to share some of the great ideas from industry leaders who are also trying to achieve this. We start at the beginning, with thoughts on who the first financial crime hire should be, and move through the evolution of a fincrime team from when growth begins, to scaling to thousands or millions of customers, and on to outsourcing and the three lines of defence. Our hope is that this eBook provides financial crime teams, nascent and established, with some new ideas on how to improve their constantly evolving team structure.

I am hugely grateful to our authors for sharing their insights with us, and hope that you are as excited as I was to hear about their learnings. Thank you to Nicole Butler, Laurence Twelvetrees, Rona Ruthen, Rebecca Mariott, Nicole Heinonen and Pravin Chandrasekaran.

“Your first hire should be empowered to perform their role effectively - this means getting buy-in from senior leadership and the board to embed a culture of good financial crime compliance throughout the business”

NICOLE BUTLER
HEAD OF INTERNATIONAL COMPLIANCE & MLRO, PLAID

From 0 to 1: who should the first financial crime hires be?

PLAID

NICOLE BUTLER
HEAD OF INTERNATIONAL COMPLIANCE & MLRO, PLAID

The legal and regulatory landscape surrounding financial crime is constantly evolving in response to the increasingly sophisticated methods criminals are employing to avoid detection. Financial conduct regulators and law enforcement have long maintained that it is critical for firms to develop strong anti-financial crime architecture from day one. Now, more so than ever, retail consumers and small businesses are living their financial lives online. This has led to a colossal increase in the volume and variety of cyber attacks, money laundering, terrorist financing, fraud and other predatory crimes that fintechs are forced to identify, mitigate, and report on.

Irrespective of whether this is your firm's first strike at the regulatory bat; or whether you are seeking to expand your business into a new market - you are going to need to hire an individual that can proactively identify, mitigate, and monitor your business's risks in order to build out and maintain the firm's financial crime program.

If the stars align and you manage to find an MLRO/BSA Officer sooner rather than later then you will no doubt save the business a great deal of time, not to mention money, downstream. Back down on planet earth; however, finding someone with the requisite level of experience, together with a risk appetite that compliments the business' mission and growth mindset can be a difficult and time consuming process. It can be even more challenging to find a seasoned professional that is also willing to join an early stage fintech, but a little bit more about that later.

As an interim hedge, many nascent firms appoint a local compliance consultancy firm to fulfill their legal and regulatory obligations in relation to, and amongst other things, financial crime. This can be an excellent way to ramp up quickly to meet the regulator's baseline requirements, and to gain insights into how other firms built their respective programs. Conversely, this is undoubtedly a more expensive route to market, and typically one that will be less customised to the firm's bespoke needs - meaning that the incoming MLRO/BSA Officer will have to spend time recalibrating the initial program.

Expectations of the First Hire

The MLRO/BSA Officer role is arguably one of the most onerous within a regulated firm because it carries with it personal liability that cannot be delegated or insured against. Failure to properly

discharge their duties under relevant financial crime legislation could result in the MLRO/BSA Officer being liable to personal fines and/or imprisonment. As such, the individual may need to be approved to perform the role by the regulator - to do so, the regulator must be able to conclude that the proposed candidate has sufficient seniority, authority, and resources to carry out their functions properly. This includes having the ability to challenge decisions that front line staff are making, and maintaining an independent reporting line into the board of directors.

Your first hire should be empowered to perform their role effectively - this means getting buy-in from senior leadership and the board to embed a culture of good financial crime compliance throughout the business. They will need to be sufficiently resourced from both a personnel and systems/controls perspective to successfully build, document, and execute the program. In return, your first hire will be equipped to start enabling the business to realise its mission in a compliant and ethical manner.

Given all that is required, it can be a huge plus for the first senior hire to come from a hyper regulated environment such as a traditional bank or financial institution. They will come with a clear understanding of the rules, best practice, and a level of experience likely to satisfy the regulator. That said, candidly speaking, this kind of background can sometimes be quite off-putting to a fintech. Fintechs do not want risk, compliance, and financial crime employees changing the tech-centred ethos of the company; or causing, what they deem to be, unnecessary friction during the client onboarding process in what is already a highly competitive space. Of course, a “unicorn” hire would have experience of both fintech and traditional financial services; and is prepared or, better still, happy to roll up their sleeves.

The Next 3-5 Hires

The next 3-5 hires will depend upon your firm’s overall exposure to financial crime. In view of the numerous factors that will play into the design of your firm’s program - there is no such thing as a one size fits all approach. The same can be said of your financial crime team. Your next few hires should reflect the intricacies of your bespoke program, from skillset to level of experience.

As with your first hire, it is not imperative for any subsequent hires to have worked at similar companies - in fact, it is rather unlikely considering the scope and pace of fintech - but clearly the more relatable experience someone can bring with them, the better.

Building a team that has independently witnessed different parts of the ecosystem firsthand should be the north star. With this in mind, you could widen the net and also consider ex-regulators, law enforcement, and consultants for these roles as well.

Attracting the Talent

The fact of the matter is that it may not be quick or easy persuading financial crime experts to join your startup, not least because you likely cannot pay bank salaries from day one. But you can offer prospective employees something banks cannot, and that is the opportunity to influence change, both within the business itself and at regulatory level. This brings about a sense of creativity that is less common within the more traditionally regulated firms. Lean into that in order to attract the right talent, together with your firm’s mission, culture, and potential upside opportunities.

Do not underestimate the power of your network - personal recommendations count for a lot, and of course they work both ways.

“...if there is a new fintech on the block, the fraud industry will assume your systems won’t be up and running or airtight straight away”

LAURENCE TWELVETREES
GLOBAL HEAD OF RISK AND COMPLIANCE, BLOCKCHAIN

Growth begins: learning to move fast

Blockchain.com

LAURENCE TWELVETREES
GLOBAL HEAD OF RISK AND COMPLIANCE, BLOCKCHAIN

Once your small team of 5 or so people is in place and you are onboarding your first 100 or 1000 customers, the operations of your financial crime team become really important. This is when you want to start thinking hard about which vendors are right for you, and about which, if any, team leads you need to hire.

KYC is the First Test

The first real test will be of your Know Your Customer (KYC) system. This is the first thing that will be hammered and you'll have an opportunity to see where the bugs are, where you can or can't verify people, how people try to get around the controls, and if there are linked or duplicate accounts. It's a good time to kick the tyres on your system. If you built your own onboarding flow, make sure you have some tests in place to check what is and is not working, and so you can understand how serious the issues are.

If you have a third party vendor, this is the time to push them about things that are not working. With every KYC vendor I've used, it's never totally rosy to start with. You need to work together to make sure you're happy with the solution, and you might also need to make a decision on whether you have the right vendor based on your customer base or business model. It's not uncommon to need to switch vendors out early on, once you have real data to look at. This is also why it's really important not to engage in long term contracts before you are fully satisfied that they can do what they say they can do.

The first type of crime you will experience will be fraud, and it will come quickly. Fraud is an industry in and of itself, and if there is a new fintech on the block, the fraud industry will assume your systems won't be up and running or airtight straight away, and you'll get targeted on a Friday night or over a holiday weekend. This is especially true if you are enabling card payments. So, having comfort that your KYC system can stop criminals is really important from day one. And a fast follow to a good KYC system are some basic fraud controls, such as ways to block or hold payments.

Avoiding Painful Operational Processes

There are a handful of operational processes that can go wrong quite quickly if ignored. One of these is screening for Politically Exposed People (PEPs)

and sanctioned entities. If you are fighting off a fraud attack and trying to tighten up your KYC process, it may go unnoticed that you are flagging 20% of customers as potential PEPs or sanctions. Not only does this quickly cause backlogs and a lot of operational work, but it's also a rubbish user experience, because the chances are that customers will be held in a sign up flow. Tuning the PEP and sanctions screening is really important, especially if you are not a big team.

Transaction monitoring is an interesting one to think about, because it's tempting to immediately sign a contract or have a trial with a recommended vendor. My advice, though, is to see what you can do yourself before engaging a third party once you have completed your risk assessment. There are some rules that you might need to have in place to start with, but beyond those few, you have got to take the time to understand how your good users behave. If you onboard a vendor and use their standard 20 rules immediately, you might end up flagging 50% of your customer base.

Any in-house system you build might be a bit clunky, but as long as you have a clear roadmap and triggers for when you need to upgrade your system, based on the number of users or the transaction volume etc, then you can quickly work out what is actually needed based on data. With transaction monitoring, not drowning in your own mess is half the challenge.

It's worth remembering too that financial crime is never binary. There are always edge cases and things you haven't seen before. Trying to build all operational processes in-house will require a full time engineering team, and there are some great vendors out there that manage the customer life cycle for you. If your company is committed to building everything in-house then you need to make sure you work very closely with the engineers from the start.

Iterating on your Risk Based Approach

Getting your risk based approach right is very important, and should be considered an ongoing evolution. The customer risk ratings you put in place at the start are very different from what you need in place 6 months or 12 months later. Don't think you'll have it all figured out at the start and can forget about it.

As you get more data, you'll know your business and the risks better than anyone else, and so you need to make sure you have a process for updating your risk ratings, which can be harder than it sounds. You'll likely be focussed on operational workflows, training, finding and testing vendors etc, so you need to proactively make time for understanding how you risk rate customers, what the KYC flows for different risk ratings are and how you monitor different customers.

This is where a key hire might be useful. You should look for someone who knows financial crime, is pragmatic, and can work with data. They should be able to take the usual risk factors such as jurisdictions, transaction values etc, but layer in more data and be more creative over time. Your risk rating model is likely to become more complex, and you may end up with a model rather than a few simple rules.

Getting the Next Hires Right

To begin with you will likely be working the operational tasks that flow out of the first 100 or 1000 customers that onboard. But quite quickly, you need to get boots on the ground and hire people who will be able to do tasks, such as KYC exceptions, screening and transaction monitoring alerts.

As you start to grow, I've found it works well to split the work into areas. You might want to bring in a key person to lead KYC and onboarding, someone else for transaction monitoring, and someone else for law enforcement and suspicious activity reports. If you're able to find good people to lead each of those areas, then they should be able to work out short to medium term operational projections so you can build up a hiring plan.

In a fintech it's often easy just to value the creatively minded - those who have an appreciation for technology and automation - and it's good to have some of those people around. But it's always important to have a few people with a lot of experience there too. They will have seen what works well at bigger companies, can help you with your policies and procedures, and set up things like assurance testing and monitoring.

“It’s key to understand and acknowledge that whatever structure we have in place, it won’t be the end structure”

RONA RUTHEN
VP CUSTOMER OPERATIONS, MONZO

The growth years: scaling fincrime ops within a customer operations org

monzo

RONA RUTHEN
VP CUSTOMER OPERATIONS, MONZO

When you intend to build a fast-growing startup like Monzo, you need to understand and acknowledge that whatever operations set up you start with, it will not be the same structure you have in 2 or 5 years time. For us, that timeframe has actually been much faster, and we have continued to adapt and evolve our operating model every 6-12 months. High growth and scaling is hard. As cliché as it sounds it really is building a race car while driving at high speed. In operations, that means quickly scaling to hundreds of people and beyond and requires different structures, rituals and best practices than other parts of a startup/scaleup.

We therefore decided on scaling our fincrime operations, and all of our other operations teams, within one Customer Operations org.

What Are You Optimising For?

Our Customer Operations org has developed over time, in large part because what we were optimising for changed significantly at different points in time. This isn't surprising, in a high growth scaling company; what our customers need and expect from us changes, our product changes and our customer base and team grows quickly.

A couple of years ago it was key for us to optimise for flexibility, making sure we were ready and able to support the growth and the fast pace of product delivery. That was true across Customer Operations, as well as in Fincrime Customer Operations. Fraud and financial crime evolve all the time and so do we - in scale, complexity of the tasks we handle, variety of features we support.

Now that we are larger and more complex, with those early requirements still in mind, we need to be more robust in some areas and balance flexibility / adaptability with a high level of expertise.

Another important element of the evolution of our operating model has always been about creating development and career progression opportunities for our customer operations team. At different points in time that progression has developed from developing generalists, to cross skilling and now to more specialisation.

This change is apparent in our hiring. Initially, we relied heavily on hiring COps (our Customer Operations agents) for frontline work and focused on their development into Fincrime Customer Operations agents. Now we have a mix of an internally developed financial crime team, with

experienced financial crime experts that we have hired from outside of Monzo.

A Badge Structure Built for Scaling

We decided early on to build a COps team with an operating model based on what we call badges. Badges represent upskilling COps and the different capabilities (and level of competency) they acquire. The badges framework enabled flexibility in our operation as well as enabling COps to have varied development and career opportunities. In practice, a frontline COp, initially supporting customers on chat and calls, could apply for a Fincrime transaction monitoring badge and a complaints badge. Over time, they may decide that they want to go deeper into fincrime, and so also become trained in more advanced fincrime badges.

Our badge framework works well, and we continue to evolve it. It has allowed us to build a model for how many people we need in different areas within fincrime, and to build a funnel of new COps for the areas that are prone to fluctuate in volume.

All of our COps go through a robust training programme that includes an initial 7 weeks, and then there are different training modules for different badges, which include shadowing other COps, coaching and quality assurance checks. In total, it can take 3 months to get to competency.

Squads in COps

Within Customer Operations we have multiple Squads, which are groups of 10-12 COps led by a Squad Captain, who ultimately report up to a Fincrime COps Lead and then me. These Squads are not currently based on task type, but all the Fincrime COps are in domain specific Squads. We will likely move to a more task based structure in the next year. The Squad Captain is someone who has been trained in all of the relevant fincrime badges and is skilled at coaching.

The purpose of these Squads is largely to have a group of supportive peers who do similar work, so that they can build the right culture and support system, as well as the social interaction of being part of a team.

Interacting with the Fincrime Domain

To make sure that the Fincrime Domain and the Fincrime COps interact effectively, we have a Fincrime Ops Team whose job is to be the interface between the two areas of the business. This team includes a Fincrime Delivery Manager who reports to the VP of Fincrime, a Fincrime Ops Lead, a Service Manager and Fincrime COps Partners. Fincrime COps Partners work with the different Fincrime product teams to support any changes that are rolled out, new task types, training etc. Together, this team manages all the initiatives and projects that are needed to ensure Fincrime COps continue to execute effectively.

Keeping Up with the Changing Fincrime Landscape

2020 saw a significant increase in fraud and financial crime scams and typologies. More than ever before we have to make sure we can quickly adapt and make changes in how we prevent, identify and handle them to protect our customers and Monzo.

These new crimes might be identified through our Financial Intelligence Unit which sits within the Fincrime Domain, through systems and through our COps raising concerns. Because of this, it's important to have some controls in place to manage spikes in work.

It's key to understand and acknowledge that whatever structure we have in place, it won't be the end structure. As we grow, change and evolve quickly, we define milestones as to when we should stop and review things. These might be time-based such as annually, or based on the number of customers or tasks. As leaders in Fincrime and COps, we need to know if things are working well or if change is needed.

We use data heavily and make sure that our systems and processes are connected so that we know if anything is going wrong. We look at volumes, values, quality of delivery and people data on an ongoing basis.

And with hiring, it's important to understand that in a high growth environment and especially in fincrime there will always be unexpected changes. These must be built into the plan. Our capacity planning looks at the number of people needed per task based on different drivers, how any development in our internal tooling could lead to a lower rate of hiring, and the impact of new products and features. It also considers changes in the market, such as regulatory updates or new codes.

More than anything the Fincrime Domain and Customer Operations work very closely together and have joint clear goals.

“We make a really conscious effort to communicate effectively. This can’t be underestimated. You need to overcommunicate to really make it work”

REBECCA MARIOTT
VP RISK AND COMPLIANCE AND MLRO, TIDE

Non-UK office: setting up and running an office outside the UK

tide

REBECCA MARIOTT
VP RISK AND COMPLIANCE AND MLRO, TIDE

From very early on in Tide's story we had Android developers in Sofia, Bulgaria. As we started to grow quickly, we realised we needed another office somewhere other than the UK, to be able to hire the high number of quality people that we needed. Given our existing connection with the city and the benefits it had to offer, Sofia was the natural choice, and so in 2018 we opened an office there and hired some customer support colleagues. Over time, our Sofia office has grown significantly and a large proportion of our financial crime team sits there. More recently we have opened a third branch in Hyderabad, India.

Choosing a Location

Although we had developers in Sofia already, a lot of time went into considering whether it was the best place to build and grow a team. We have an Internationalisation Team, whose job it is to look at locations, markets, salaries, education systems, experience etc.

One of the reasons we wanted to open an office outside of the UK was to find another talent pool to hire from. There are lots of fintechs and financial service companies in London, and so competition is high, so we were looking for a country that had a similar regulatory environment to the UK and was a reputable financial services country. We also wanted to make sure that there were other financial services companies in the city to make sure we had access to a big talent pool.

Other considerations like the cost benefit, the penetration of English language speakers and time zone were important. Sofia has been great in these regards, and the people we have managed to hire have come with very relevant, multi-year experience.

Deciding What Financial Crime Work to Move out of the UK

When we first started hiring financial crime professionals in Sofia, the team there worked on Know Your Customer (KYC) tasks and low risk manual customer reviews. We intended to keep the rest of the more complex work in the UK. Over time, we introduced things like medium risk customer reviews and the lower risk Suspicious Activity Reports (SARs).

Now, because we are able to hire really excellent people with sometimes 5 years of directly relevant experience, our team in Sofia works on complex SARs, high risk customer reviews, typology investigations, sector reviews and everything else our UK team does. We have team leaders and people doing QC there, and we are confident that there is no difference in the quality of work between our teams in London and Sofia.

Despite this, taking a staged approach to rolling out the work did help us set up our training, QA and QC procedures so we have comfort in the quality of the work. It also gave us time to hire team leaders in each location.

Training, QA and QC

Everyone gets the same training, regardless of their location. Our colleagues in Sofia and Hyderabad are part of our team, and so we never wanted to introduce different types of training. Building the culture from that first interaction is so important.

We have a trainer in Sofia that specialises in KYC, and one in London that specialises in investigations and SARs. Depending on what role we hire for, the analyst gets the training package relevant to that role.

We have Quality Assurance analysts sitting with the trainers, and as a new financial crime analyst is onboarded they work through different stages of permissions. To begin with they can't approve their own cases, they get buddied with a senior analyst, and then over time depending on their QA scores and the feedback they receive, they can do everything needed for the role.

Our QA team is in our first line of defence, and they are really focussed on quality of interaction, tone of voice, whether a good service was provider, the SLA etc. The QA process is pretty hands on, with 1:1 training and mentoring, and looking at a small number of cases in detail.

We have Quality Control in the second line of defence, and they look at our compliance to policies and procedures on a risk-based approach. This feedback also gets back to the training managers.

Communicating Effectively

We make a really conscious effort to communicate effectively. This can't be underestimated. You need to overcommunicate to really make it work.

We have a number of meetings like a team all hands, a monthly Risk and Compliance team meeting, deep dives to learn about new risk areas and individual team meetings. We also use Slack channels a lot.

On an individual level, managers have 1:1s with their reports, and we make sure that there are managers in all locations so everyone has local support.

The Challenges

Initially, the biggest challenge was that we had no brand or name recognition in Sofia. We wanted to attract top talent, but it was hard. We spent a lot of time working on this, attending certain hiring events and really committing even before the benefits paid off.

Time zones are a challenge, and that will be more obvious as we expand our team in India. We use some tricks like a Slack app that enables you to delay messages so they don't come through at midnight. We have also moved all shared meetings to the mornings.

Culturally, there are lots of obvious differences, especially between the UK and India. We have made a conscious effort to make sure we incorporate and embrace the different cultures. Our senior leaders have all been reading books to educate themselves, and people travel to the different locations. Before Covid-19 hit, I spent 1 week in every 6 in our Sofia office, and had been to India twice. It's really important that the people in different offices know who the management team are, and we want to ensure knowledge sharing between offices.

The Benefits

There are some obvious benefits, like cheaper offices and a larger talent pool. But some things that surprised us were the depth of the experience we could find in Sofia and Hyderabad, and the business continuity advantages.

From a financial crime perspective, we've also been able to have 24/7 KYC, and almost 24/7 transaction monitoring. It helps us be more effective at meeting our financial crime requirements and gives our members a better experience.

“I believe that you can outsource anything, with the right controls in place”

NICOLE HEINONEN
HEAD OF RISK & FINANCIAL CRIMES OPERATIONS, STRIPE

Outsourcing: choosing and managing an outsourced team

NICOLE HEINONEN
HEAD OF RISK & FINANCIAL CRIMES OPERATIONS, STRIPE

If you are thinking about outsourcing financial crime work, it is really important to know exactly what your needs are and what the risk is for you specifically. What do you want to outsource? What is your reason for outsourcing? How much technology do you already have in place to allow for outsourcing? How black and white are your procedures? Only by understanding these things can you outsource effectively, and with minimal risk.

Reasons to Oursource

The real benefit of outsourcing is the ability to scale at speed. If you are in a situation where you have to rapidly build an operational team, conduct a lookback or remediation within a short period of time, and/or need to get things done correctly as fast as possible, then having the flexibility to bring people on and ramp up quickly is key. In many organizations, it can be difficult to get permanent headcount, and once a programme is mature, you may find you do not need as many internal people as you originally thought. Outsourcing provides a flexible solution to solve these problems.

Additionally, most vendors do this work for multiple companies, so if you are just starting to scale and are building out your financial crime programme, they can often point out areas for improvements in your processes.To maximize the benefit of outsourcing, I always try to outsource repeatable tasks to a vendor, while leveraging my internal headcount for more in-depth or complicated projects. While not always true, outsourcing can provide operational cost savings, especially overtime as you evolve your process, technology, procedures to reduce average handle time.

Choosing an Outsourcing Vendor

The questions I ask of vendors are:

GENERAL QUESTIONS:

- Length of time offering the service. This can be specific (PEPs) or general (AML services), depending on your needs.
- Proportion of overall business serving Fintech clients (or whatever industry you are in)
- Ability to do all the work in-house (no subcontracting)
- Business Strategy & alignment with my company/needs

SITE OPERATIONS:

- Experience of analysts onsite working in the areas needed
- Recruitment process - how are they hiring quality analysts, what is their basic analyst profile?
- Hiring Timelines - timelines to on/offboard? Ramp up time?
- Learning & Development - does the firm support ongoing education? Do they have their own in-house education program? How will they ensure their analysts are staying up to date with industry trends?
- Attrition - what is their annual % attrition? This is often a key indicator on how the vendor treats their employees. A lower attrition means you will spend less time on onboarding new analysts and will likely have increased productivity and engagement of the vendor team.
- Operational Support - Do they offer onsite trainer/QA and manager? How will they manage their own analysts? How do they coach or manage poor performance?
- Workforce Management - Do they have standard business reviews and reporting in place? Do they proactively monitor volume and add or remove headcount as needed for various queues?
- Security - Is their workspace secure? Can they accommodate our requirements of closed off space? Badge access? What are their policies?

PRICING:

- How do they set up pricing? I've found this to be the largest differentiator between vendors and is one of the most important factors when choosing a outsource vendor. Do they bundle? Productive hours or itemized?
- Do they charge services specifically for recruiting?
- Do they provide hardware or do I need to?
- What are all the additional fees/fine print?
- Tip: Know what you are willing to pay before reviewing the proposals and *always* negotiate.

PROGRAM IMPLEMENTATION:

- Timelines - can they move fast?
- Methodology/Approach - Does their approach make sense?
- Dependency - How heavily do they need to rely on us vs they can offer us?

VALUE ADDED ACTIVITIES:

- What makes them stand out (or not)? Is there additional value they can add?

For global companies, it may also be worthwhile to look for outsource vendors with a footprint in the regions you operate within. While you can use one vendor and train them on the specific regional requirements, it can be easier long term to locate and partner with vendors in those regions that already have the background, experience, and skill set to comply with the applicable regulatory frameworks for those areas. In some cases, regions specifically require the AML team to be in the country; be sure you know the specific requirements for your business.

Deciding What Financial Crime Work to Outsource

I believe that you can outsource anything, with the right controls in place. We currently outsource all of our Financial Crimes operations, with the exception of the actual reporting of any sanctions, suspicious activity reports etc.

Think about the specific workstream coupled with the vendor options to assess the risks involved. For example, outsourcing PEP reviews to an offshore non-compliance vendor may be low risk, high reward. Whereas if you are outsourcing an AML investigation you should probably stick with an AML specific vendor who has the right background to conduct these reviews.

In terms of the controls that enable you to do this, it's things like looking for vendors who approach security in a similar way to you, understanding how they handle issues by running through some made-up scenarios, finding out whether you can request to offboard analysts, ensuring the right ratios for team leads and QA are in place, and providing clear desktop procedures.

Keeping Quality High

To ensure quality is high from the outset, we go onsite to conduct train-the-trainer sessions with the vendor trainers for the first batch of analysts. We then shadow the trainers for the second batch of analysts and score their delivery based on our

training certification programme. Every trainer must pass the certification programme before we feel comfortable with them training analysts directly on their own.

After the initial training and nesting period (2 weeks post training to ramp up), the focus turns to quality assurance (QA). The QA Leads at the vendor sites go through the normal analyst training and work a small number of reviews each week to keep their knowledge of the desktop procedures fresh. They present their QA scores by workflow in weekly business reviews, highlighting any low scores and remediation plans to address. Further, we conduct weekly calibrations with the QA Leads across sites. To do this, we send 3-5 reviews to every QA Lead to score. We then meet up to calibrate the scoring, ensuring everyone has the same understanding and is scoring consistently across the board.

Additional controls in place that help with maintaining quality include having a low QA Lead to Analyst ratio - no more than 1:10. Build these ratios into your contract. Use stratified sampling to determine the right number of reviews or cases to QA by workflow. Every task that is outsourced should have a corresponding desktop procedure and a QA test plan.

Quality is probably the most important metric to measure to ensure stakeholder buy-in and trust. Prior to outsourcing, be sure you know what and how you will measure quality, as it's the first thing stakeholders will ask about once you go live.

Communicating Effectively

It is an investment to outsource effectively and it takes a team with various skill sets to really set up an ideal operational infrastructure, outsourcing or not. We've implemented a Shared Services team, consisting of Learning & Development, Change, Quality, and Partner Management. This team works together to support the larger operations, inclusive of outsource vendors.

I've found the best way to manage the daily communication and performance expectations is to have a dedicated person or internal team responsible for the day-to-day relationship of vendors. For the first two years we had one dedicated person solely managing our Financial Crimes vendors. As our company scaled and we took on more risk work, we were supporting 6 sites globally with over 500 analysts. We added an additional person and formalized what we call our Partner Management Team. While they speak with the vendors almost daily, we require the vendor to host formal weekly and quarterly business reviews, to understand productivity metrics and quality scores. In addition to this, I meet with the site directors every quarter and we ask our vendors to host annual business reviews for our larger stakeholder groups focusing more on metrics for the year, company directions and longer term plans.

Our Change Management programme ensures all vendors receive communications about workflow or policy updates. The Change Management programme consists of one person that works to collate all policy, workflow, and tooling updates throughout the month and sends out a Process Improvement Review (PIR) memo to all internals and vendors the first week of every month. The analysts are required to attest to reviewing and acknowledging the changes included in the PIR.

Our Quality Lead maintains oversight of the quality program, including owning and driving the quality metrics at each site, running calibrations, and holding the sites accountable for remediation plans to improve quality scores. Similarly, the Learning & Development Lead owns coordination of the training curriculum, materials, delivery, and the Trainer certification program. The training team also secures internal subject matter experts as mentors during the training and nesting period for any questions. And you'll also likely require support from your IT or security teams.

The Role of Technology

If you don't have your own technology which the vendors can use, outsourcing becomes much more risky. Working out of spreadsheets and documents is neither secure nor ideal from a scaling or even audit perspective. As you think about setting up operations, it will be important to map out which customer data you (or your company) is willing to share with vendors. Investment in product solutions will be required to outsource effectively, regardless of if they are home grown or off the shelf.

We have two main products that allow us to assign and manage workload. A queue based system for reviews (PEP, Sanctions, etc) that assigns reviews from a queue to the analyst to resolve and a case management system for work that requires evidence and a report, such as an AML or Due Diligence investigation. We just recently leveraged the queue based system to launch a new QA assignment tool, which we expect to reduce QA handle time significantly. By using

a queue or case management system, it limits the accounts a vendor can see to only the accounts they need access to in order to complete their review. A big win for data security.

By using our own technology, we have much more control and oversight of the work being completed by vendors. It also ensures that any escalations or reporting can easily be sent to our internal teams for review and next steps. Nothing ever leaves our systems. Further, by using your own technology, you gain much more data that can be used for metrics, reporting, and budgeting.

“Quality is probably the most important metric to measure to ensure stakeholder buy-in and trust”

“Defining the lines of defence is helpful, but financial crime isn’t clear cut”

PRAVIN CHANDRASEKARAN
BSA OFFICER, VARO

Moving to the three lines of defense: when, how, who

Varo

PRAVIN CHANDRASEKARAN
BSA OFFICER, VARO

Varo's intention was always to get a banking licence. When I was hired as the BSA Officer 18 months before we were granted a charter by the OCC, I had the opportunity to build our AML capabilities around the three lines of defense model well before we would reap the benefits of such a structure. By being cognizant of this early on, our programs are able to scale quickly without much concern of volumes or new products.

Defining the Three Lines of Defense

If you were to mimic the most traditional financial institutions, then the three lines of defense model would look like this:

1ST LINE OF DEFENSE: The business or product organizations. This includes things like how you onboard people, what the product will look like, how you'll make money, and people dealing with customers. The 1st line also usually includes risk management functions, for example a fraud operations group.

2ND LINE OF DEFENSE: Independent credible challenge, policy writing and understanding regulatory change and in some cases centralized functions to perform AML or Watchlist screening functions. Often in AML there are economies of scale in centralization.

3RD LINE OF DEFENSE: Internal audit. This team makes sure that the program we have built is appropriate based on what the regulators are asking of us.

Things can get murky at fintechs, though, since there isn't always a well formed business line. Companies usually start with product and operations teams, and with far smaller, or no, risk functions. The 2nd line may be small, and internal audit might be outsourced.

Fitting Financial Crime into the Three Lines

Defining the lines of defense is helpful, but financial crime isn't clear cut. Some fintechs and banks decide to have some strictly "operational" work in the 2nd line because of the skills required to do the work, to ensure appropriate oversight, and because of economies of scale.

Many fintech's 1st line operations teams carry out customer verifications or manual reviews, and

do the fraud operations work. These are tasks that require communicating with customers and efficiently managing queue based work. This team owns their own procedures, and the 2nd Line reviews them to make sure they align with policies.

One way to approach a 2nd line is to have two teams that could be considered operational in nature - a watchlist and sanctions screening team, and an investigations and SAR filing team (a Financial Intelligence Unit, or FIU). Overseeing both of these teams, as well as the 1st Line financial crime work, is a governance function and an analytics function. The governance function looks after things like policy writing and procedure applicability tracking. Our analytics function oversees our models, tracks and monitors metrics and KPIs, and sets thresholds and rules.

This separate analytics function isn't a requirement, but it is best practice. It enables separation of gamekeepers and poachers. The analytics team can set suspicious activity monitoring rules, and thresholds for risk appetite limits, for example. Our FIU works the output of the models and provides constant feedback, but can't actually set or change the rules or thresholds.

The final component of the 2nd Line is a centralized risk testing team. This is not specific to financial crime - they also test things like credit risk and enterprise risk. With regards to financial crime, they can choose to test things however they went. They test operational outputs, Customer Identification Program (CIP) and Customer Due Diligence (CDD) procedures, or model thresholds.

And finally, our 3rd line is a centralized independent audit function. They are not financial crime specific, but audit every part of the company. They look at what the policies and procedures say, and make sure that they are compliant and are being followed. They do this for both the 1st and 2nd lines. Our 3rd line usually does a full financial crime program audit every year, but as we get bigger and more complex, they may do reviews of different departments and deep dive on certain areas.

When to Set Up the Three Lines

In the United States, fintechs tend only to set up the full three lines if they are intending to become directly regulated. If that is the case, then you should be showing regulators that you are serious by hiring the key roles needed for this structure before they ask for them.

Things are slightly different in the UK, where it's quite common for fintechs to get E-Money Licences. In those circumstances, a full three lines model can be really beneficial from the outset.

Key Roles

If you are setting up the three lines of defense, there are some key roles you will need.

In the 1st line, you ideally need someone who has dealt with customer onboarding at another institution. The element that is tricky is working out how much you want this person getting involved on the product side, versus just the customer side. Do you want them spending time working out which identity verification vendor to use? Or, do they just need to know what CDD is, how to meet the requirements and how to remediate any problems?

In the 2nd line, you obviously need a BSA Officer/ MLRO. Underneath them, the bare minimum you need is someone to lead the watchlist screening team, and the FIU. Those are operational elements you won't be able to get away from, and experience is important. I also recommend a governance lead and an analytics lead.

And in the 3rd line, it's really a decision point for the institution. Do you want to outsource this, and would your exec team be comfortable with that, or should it be in house? Do you want specific expertise for AML, and all other areas? In our experience, if you have talented auditors, you don't need area specific expertise.

Challenges

The most challenging part of the three lines model is keeping them all in sync. That all begins with defining terms, which get misused a lot. What is QA and what is QC? What do we mean by testing and audit? Which team is responsible for which thing?

Beyond that, communication is vital. I meet with my counterpart in the 1st line every week and the Chief Auditor every other week. We always talk through the audit plan before an audit kicks off, for example.

I work with the 2nd line centralized risk testing team to make sure that between their work and our QA work that sits in the operational teams, everything gets tested, but we are not duplicating work.

Benefits

From an operational standpoint, there are definitely economies of scale. But the biggest benefit is really how quickly we can grow and scale now, because we did all the hard work to get this structure right.

There is definitely a path you can take where you start a fintech, roll out a product, hire operations staff to support the customer demand, and then before you know it something breaks and you have to throw risk people at the company. You set up a 2nd and maybe a 3rd line of defense, and you start asking the existing team to justify decisions that were already made because you need to have it written down. The existing staff are not used to the constraints and structure that the risk people instill, which creates friction, and if you can escape regulatory scrutiny, your customers will almost certainly feel some pain.

But if done right, if you put in the hard work to create an effective three lines of defense - and it is hard work - then when growth comes, it's easy, and safe, to scale.

"...the biggest benefit is really how quickly we can grow and scale now, because we did all the hard work to get this structure right"

cable

cable.tech