The Effectiveness of Financial Crime Controls

cable

Cable is the leader in automated financial crime assurance.

Anything less than full monitoring of controls leaves room for error - finally you can do away with manual dip sampling. Cable provides automated evidence of your compliance, risk management and effectiveness, allowing you to:

- **save money by eliminating expensive remediation projects,**
- **reduce the risk of regulatory fines,**
- **save time by automating reporting,**
- **improve stakeholder communication, and**
- **scale compliantly and with confidence.**

Why manually test 100 accounts when you can automatically monitor 100%?

Introduction

Regulators, international standard setters and private sector groups have all started to talk about prioritising financial crime effectiveness over technical compliance. There is growing momentum as more people come to the realisation that financial institutions must be able to prove that what they're doing is not just legally compliant, but is actually working to reduce financial crime.

The overall message from these organisations is clear, and it is only a matter of time before firms around the world are obliged to demonstrate the effectiveness of their financial crime controls.

Whilst there are clear financial benefits to measuring and evidencing financial crime effectiveness, how to do so remains unclear.

This series provides a deep dive into the world of financial crime effectiveness, covering;

1. The Heavy Cost of Ineffectiveness

2. What the Regulators are saying about Effectiveness, and

3. How to Measure Effectiveness.

Part 1: The Heavy Cost of Ineffectiveness

Summary

1. Building and maintaining a financial crime compliance framework costs a huge amount, and the best outcome is the absence of punishment from regulators.

2. In the face of poor outcomes, the financial crime industry has seen a shift towards effectiveness, most keenly reflected in the increasing number of regulatory fines that mention ‘ineffective controls’.

3. Firms have ineffective financial crime controls because they don’t know what crime to look for and have inadequate testing of controls. In addition, they are unable to evidence their effectiveness to regulators.

4. The cost of fines is only the tip of the iceberg, with remediation projects easily costing triple or quadruple the original penalty.

Do You Get What You Pay For?

They say 'you get what you pay for', but in the world of financial crime, that hardly seems to be the case. As all financial crime professionals know, building and maintaining a financial crime compliance framework can cost an enormous amount. People, technology - it all adds up. In return, the best response firms can expect to receive from regulators is the absence of punishment, while at worst they face censure, public criticism and ultimately fines and other forms of civil or even criminal enforcement action.

This happens to financial firms of all sizes and types and often not as a one-off occurrence. Once under the eye of the regulator, firms can end up in a vicious cycle of criticism, remediation and further investment to rectify problems. Cost piles on cost, and if this isn't bad enough, there will be reputational and commercial damage, the costs of which can be hard to quantify.

It is easy to take a resigned attitude to these problems. Regulatory-induced costs and criticism have been dogging the financial services industry for many years. But are we really beyond finding new ways to tackle these challenges, and do we need to just keep treating the symptoms, rather than look for a cure?

Almost certainly not. At Cable, our approach has been to go back to the root cause of the problems, and ask why firms are spending so much money and getting such poor results. What we have found is that the issue isn't about money, will, or commitment. It's a matter of effectiveness. Not only being able to make effective financial crime frameworks, but also being able to demonstrate this to regulators.

In this three part series, we will look at the question of financial crime effectiveness from several angles: the financial impact of ineffective frameworks on firms; regulators' growing emphasis on the issue; and most importantly, how innovative solutions can be applied to address the issue. Because there's no reason why the industry has to live with ineffective financial crime controls - or their costly consequences - any more.

Effectiveness on the Agenda

Over the last twenty years, the primary goal of financial crime professionals has changed. At the outset, international standard setters at the Financial Action Task Force (FATF) and national regulators focused on the concept of compliance. They set the rules and regulations, and firms were expected to meet them. How they did so was less of an issue - it was just a case of ticking the boxes.

But it soon became apparent that this approach was inadequate, and firms were next encouraged to take a 'risk-based approach', which varied the application of financial crime controls in the face of their own distinctive risk environment. Whilst somewhat of an improvement, difficulties in application remained, and the overall outcomes have remained poor.

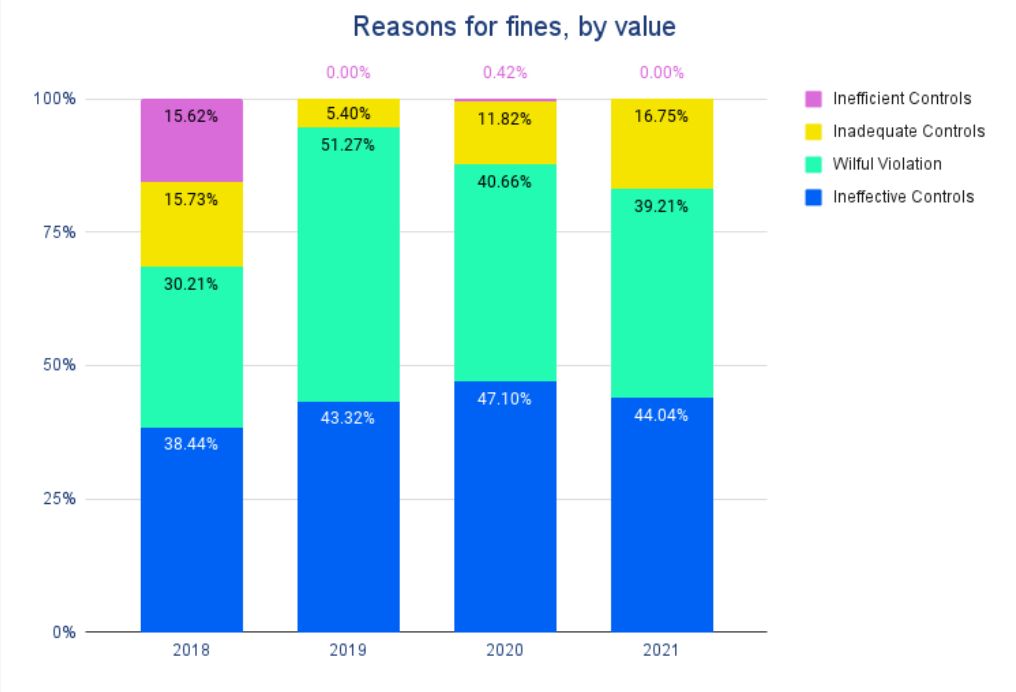
Poor Outcomes and Impact

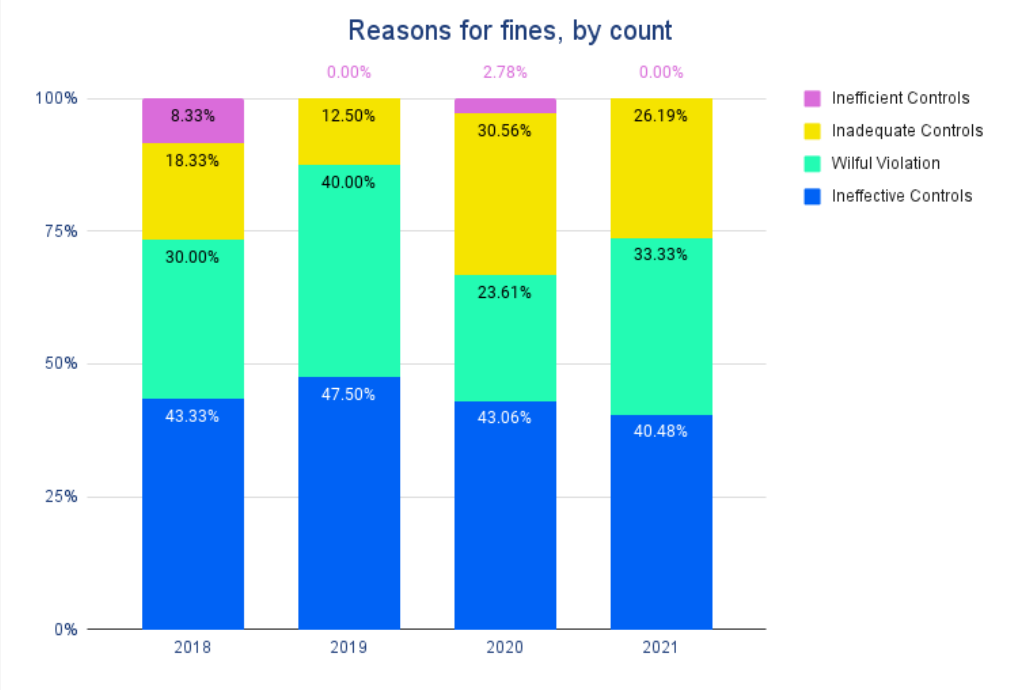
- **Private sector monitoring and screening systems have continued to produce high 'false positive' rates of 80- 90% on average, with only a small proportion of the remaining 'true positives' turning into Suspicious Activity Reports (SARs) shared with the authorities.**
- **Law enforcement agencies have continued to only find immediate use in up to 10% of the SARs they receive, while the EU agencies themselves believe that only 2% of criminal proceeds are frozen and 1% confiscated.**
- **Researchers have continued to find that levels of global financial crime remain high, with around 2-5% of global income likely to come from illicit sources. This would put the 'global criminal economy' in the top 10 of economic performance, alongside countries such as Japan, Germany, the UK and France.**

As a result, the financial crime rule-makers have increasingly emphasised the concept of effectiveness as the target at which firms need to aim. Regulators' evolving perspectives on effectiveness is a topic we will look at in more detail in the next part in this series. Suffice it to say at this stage, however, that even if there are varying opinions about what effectiveness is, there is a universal sense that it matters to regulators and is shaping how they go about their supervisory duties.

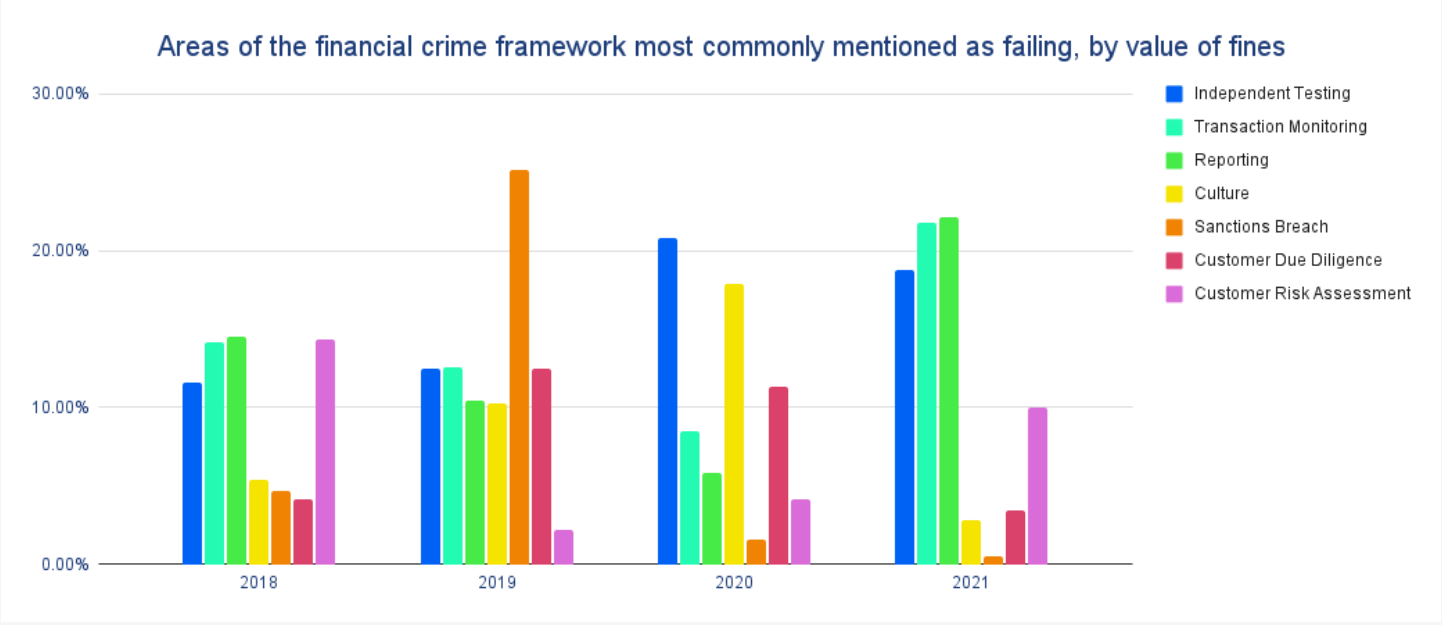
Ineffective Controls and a Lack of Independent Testing

In our own research looking at US and UK fines given for financial crime failures between 2018 and 2021, we found that the reason most often given for a negative finding was 'ineffective controls', by both value and count of fines.





In addition, inadequate or ineffective independent testing of controls has been mentioned in an increasing number of fines, demonstrating that regulators see the testing of controls as part and parcel of demonstrating their effectiveness.



Why so Ineffective?

Media narratives often blame financial services firms themselves for the prevalence of financial crime, attributing failures to laziness, greed, or even malfeasance; and, yes, some businesses do make bad mistakes, intentionally and otherwise. But in reality, most firms that get called out by regulators have acted in good faith.

So why then are they getting criticised for 'ineffective' financial crime controls? There are a number of practical - and in many ways completely understandable - reasons:

1. Controls are often poorly configured because **firms just do not know what they are looking for** when it comes to detecting financial crime. Controls are based on old typologies - 'industry lore' - about what crime looks like, meaning that firms end up with a static approach that is less 'risk-based' than many would like to claim, and almost always backwards looking.

2. This problem is compounded because most firms have **difficulties in testing, optimising and reconfiguring their controls in real time**. This comes from a lack of flexibility in available testing solutions, as well as from organisational and structural problems which make it difficult to fine-tune controls to an ever-changing financial crime risk environment.

3. Finally, even when firms do take good, risk-based decisions and detect financial crime effectively, they often **lack the systematic evidence to demonstrate this to regulators**.

Costly Consequences...

Our analysis of fines given by the US and UK regulators found that nearly $2bn worth were given in 2021. The largest fines were given to well established banks, such as Natwest, who were fined £265m, and Capital One, who were fined $390m.

Amongst challenger banks and fintechs, there can be a tendency to think that these kinds of fines are something that regulators only impose on large banks. But although there is a legal onus on regulators to take a proportionate approach, that doesn't mean that younger firms are immune to significant regulatory fines either, and as such firms grow, they are gaining more regulatory attention. Indeed in 2021 alone, Bitmex were fined $100m and N26 were fined $5m. These are expected to be the first of many more fines to hit challenger banks and fintechs in the coming years.

...Before and After a Fine

Whilst the costs most discussed by the media are the reported regulatory fines, the biggest impact on firms is usually the unreported costs that come before and after a fine.

In the face of this knowledge, the first resort of businesses has often been to throw money at the problem. Just about any market research you can find will show the level of investment in financial crime compliance rising year on year over the last decade or so. Recent research by LexisNexis and Oxford Economics suggests that financial crime compliance for financial institutions in the UK alone is estimated to be £28.7 billion, with costs expected to grow more steeply in the next two years, reaching over £30bn by 2023.

The largest part of this compliance spending is still going to staff, often in large investigatory teams who are needed to work through multiple false positive screening and monitoring alerts, and on manual testing teams trying to understand the effectiveness of controls. According to a recent report from the SWIFT Institute, personnel costs can amount to anywhere between 60 and 80% of financial crime compliance spending.

In the UK, the Financial Conduct Authority (FCA) tends to perform Section166 'Skilled Person Reviews' before deciding whether to levy a fine or not, and our research suggests that the cost for these starts in the millions; from external legal advice and consultancy fees, to look-back projects for further misses, remediation, staff training, and platform upgrades. Whilst financial crime professionals will debate the exact figure, this cost can be triple or quadruple the original penalty.

Moreover, these are rarely one-off expenditures.

As we have noted, fines can generate significant burdens for firms, and are usually accompanied by demands for further reform from regulators. The start of regulatory attention can herald a long process for firms, with close scrutiny usually revealing further failings that can themselves result in a whole new series of regulatory enquiries. In the case of Commerzbank, a US fine of $1.45 billion in 2015 for failures to detect suspicious activities led to a significant round of compliance investment, but the bank was in difficulties again in 2020, when the UK's FCA fined the bank £37.8 million for failures in its financial crime controls.

Conclusion

For the businesses that sit at the centre of the financial crime campaign it can often feel as though they are fighting a losing battle. They devote large amounts of funds to controls that do not seem to find financial crime, while also being liable to criticism and further regulatory burdens when the controls don't work as expected.

What's the answer? How do businesses break-out of - or better still avoid - this cost-laden cycle of investment, criticism, fines, investment, and what are regulators saying about effectiveness?

Part 2: What the Regulators and International Bodies are saying about Effectiveness

Summary

1. Regulators in the US and UK, as well as international bodies, have recognized the shift towards understanding the effectiveness of financial crime controls.

2. Regulators are showing signs of building the concept of effectiveness into regulations, and it is likely only a matter of time before regulated firms around the world are required to demonstrate their effectiveness.

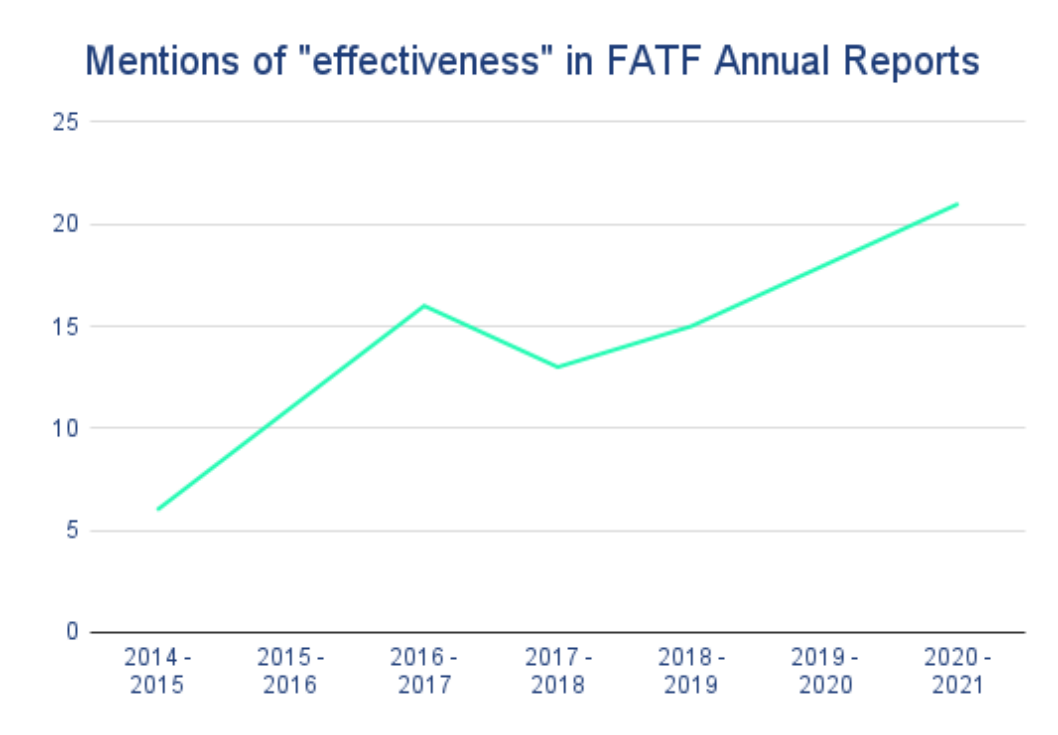
3. There are clear financial benefits to firms in measuring and evidencing their financial crime effectiveness, and understanding how to do so is vitally important.

Tone from the Top

Over the past two decades, the tone from the top has changed on 'what good looks like' in fighting financial crime. Regulators, international standard setters and private sector groups have all started to talk about prioritizing effectiveness over technical compliance. There is a growing momentum as more people come to the realization that financial institutions must be able to prove that what they're doing is not just legally compliant, but is actually working to reduce financial crime.

Global Tailwinds

Global direction is shaped by the **Financial Action Task Force (FATF)**, an inter-governmental body responsible for setting international standards to prevent financial crime. Over time, it has recognized that the components of a financial crime framework must "work together effectively to deliver results" and focus both on effectiveness and technical compliance. Indeed, when carrying out its country assessments, it has stated that "the emphasis of any assessment is on effectiveness". Since FATF's methodology is used by other assessment bodies such as the International Monetary Fund and the World Bank, it is very influential in shaping how financial crime systems and programs are appraised.



According to the **Wolfsberg Group**, an association of global banks which develops financial crime frameworks and guidance, regulators still don't pay enough attention to whether a firm's financial crime program is effective, and focus too much on technical compliance. As a result, firms are devoting too much time and effort to ticking boxes rather than trying to detect or stop financial crime. The Group is calling for national regulators to embrace FATF's approach and assess financial crime programs based on effective outcomes, and have said that firms "should be prepared to explain to their supervisors how their controls actually mitigate risk and/or provide highly useful information to government authorities".

Regulatory Priorities

Although the Wolfsberg Group clearly believes there is still more to do, it is becoming increasingly clear that effectiveness does matter to regulators. Regulators frequently indicate in their public statements that they want to move away from a tick-box approach to one that considers if firms are actually any good at detecting and preventing financial crime. This will lead to a big change in most regulators' approach to supervision.

The US
In the US, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) has started a massive overhaul of their financial crime program in order to improve effectiveness and utility. In September 2020, FinCEN published an 'advance notice of proposed rulemaking' (ANPRM), seeking public opinion on significant regulatory changes and stating that supervision should evolve to "promote effective outputs over auditable processes". The proposed changes include a new explicit requirement for regulated firms to maintain an "effective" AML program.

It is becoming clear just how important it will be that firms can demonstrate that they are measuring effectiveness, and can explain how they are implementing any new effectiveness requirement.

The UK
Regulators in the UK are also talking more and more about effectiveness, and are likely to follow the Wolfsberg Group's guidance in calling for more evidence that financial crime controls are actually effective. In a speech in 2016, the FCA recommended that firms should focus on outcomes and reconsider ineffectual processes, saying "If your bank is mired in processes that aren't effective, do not be afraid to change them". Once again, the biggest hurdle will be for firms to be able measure their own effectiveness and demonstrate this to their regulators.

Effectiveness. But, how?

So the overall message from all these organizations is clear - financial crime prevention needs to move away from tick box compliance to focus on outcomes and effectiveness. But what does this actually mean, and what does it look like in practice?

The Wolfberg Group has made the best effort at defining effectiveness, saying that effective controls should:

1. comply with financial crime laws and regulations

2. provide highly useful information to government authorities in priority areas

3. be reasonable and use risk-based controls to detect, prevent or deter financial crime

Point (1) is a given, and whilst it brings us back to tick box compliance, most financial crime professionals agree that pure compliance is still an important element of any effectiveness framework. Points (2) and (3), however, are far from clear.

With the feedback time from government authorities on reported suspicion being many months, if at all, initiating Point (2) would depend on significant structural change within those authorities. Furthermore, finding anyone who is not a lawyer who can define what reasonable means is always a challenge, and with each firm implementing their own risk-based approach, standardizing a measurement of those approaches feels far from easy.

So What Next?

Regulators and government bodies are in agreement that effectiveness is coming, and are already showing signs of building the concept into regulations. It is likely only a matter of time before regulated firms around the world are obliged to demonstrate their effectiveness, and there are certainly huge advantages to them if they can do so.

If firms can measure and evidence the effectiveness of their financial crime controls, they will be able to eliminate ineffective controls, and have much greater flexibility in allocating resources. They will almost certainly be able to move away from manual and laborious processes which do not yield meaningful results, for instance by lowering due diligence requirements for certain low-risk customers or services, or by establishing clearer and more targeted boundaries for transaction monitoring and investigations. However you look at it, effectiveness will reduce the cost of financial crime frameworks.

But how **do** you measure effectiveness?

Part 3: How to Measure Effectiveness

Summary

1. Measuring effectiveness should cover regulatory and internal control compliance, adherence to your risk-based approach, the performance of controls, unknown unknowns and pure financial crime.

2. Manually measuring effectiveness based on dip samples and external reviews is the traditional approach. It is well understood, although it does have some limitations.

3. Automated assurance is the next evolution in financial crime and fundamentally changes and upgrades the nature of your assurance process.

Assessing and understanding the effectiveness of your financial crime controls should be top of mind for financial institutions regardless of size. It's good for financial institutions, because they can eliminate ineffective controls, reduce costs and improve stakeholder communication. It's good for regulators, because it gives them a better understanding of whether firms are just ticking boxes or actually managing their risks. And it's good for society, because it helps us understand how much financial crime we are stopping, and tells us how to stop more.

Regulators are increasingly promoting the concept of effectiveness. It's only a matter of time before this is embedded in regulations themselves, with firms obliged to prove to the regulators that not only do they have controls in place, but that those controls actually work.

Firms can frequently find themselves playing catch-up with regulatory developments and changing systems or processes which they've only recently implemented or reviewed. So when regulators signpost a change in direction, as they are now, there are clear advantages to getting out in front of those changes.

But, how do you measure the effectiveness of your financial crime controls?

What to Measure

It's all very well to say that firms should measure effectiveness, but what does that actually mean? What specifically should you be measuring, and what metrics and data will tell you if your program is effective?

Regulatory Compliance
The basic starting point is establishing whether your program is compliant with regulatory requirements. If not, you're in trouble.

You need to ensure that you're collecting all the mandatory KYC information, all customers and payments are correctly screened, and all appropriate actions are taken when you identify suspicious activity. The question you're asking here is essentially a binary one - are we meeting our regulatory obligations, yes or no? Provided you understand your obligations and have access to the relevant data and information about your program, you should be able to answer this question.

Internal Control Compliance
As well as regulatory compliance, you need to ensure your financial crime program complies with your internal policies and procedures. If you commit to implementing certain controls, you must adhere to those controls. The basis of any good program is a clear risk appetite, so this is a good place to start. You should confirm your risk appetite is being met through both prohibitions such as "we won't onboard customers in certain sectors" as well as limits such as "no more than 5% of our customers will be high-risk". It's relatively simple to tell what 'good' looks like; you established a defined risk appetite statement, so it is important to be sticking to it.

Adherence to your Risk Based Approach
A cornerstone of all financial crime programs is the adoption of a risk-based approach, so you need to confirm this approach is being implemented in practice. Are you correctly applying different levels of KYC to different types of customers? Are you conducting periodic reviews at the correct intervals? Are higher-risk customers being escalated for senior approval?

As well as confirming if you're implementing a risk-based approach, you should consider whether it's giving you the results you expect.

Did the outcome that you expected to happen, actually happen?

Are you classifying the right customers as high-risk, or do you actually identify more suspicious activity amongst low or medium-risk customers? If you're applying different transaction monitoring rules to different customers, are you missing suspicious activity by low-risk customers, or drowning in unhelpful noise from high-risk customers?

Performance of Controls
Most assurance processes involve confirming if controls are being implemented as expected. But not all consider if the controls are actually performing. Are they doing what is expected, and are the right outcomes being generated, for the right reasons?

Did the outcome that you expected to happen occur because of the thing that you expected to trigger it?

For instance, did suspicious activity that you deem connected to money laundering get flagged by transaction monitoring rules looking for money laundering, rather than fraud or terrorist financing? If you amend your transaction monitoring rules to reduce unnecessary false positives, or conversely to capture more activity, you need to measure whether the number of alerts has gone up or down as expected. And at a deeper level, you need to measure whether the activity now triggering alerts is relevant - i.e. has an increase in the number of alerts highlighted your awareness of suspicious activity, resulting in more investigations and more SARs? Has a reduction in the number of alerts led to fewer investigations and SARs, meaning you're not just cutting out noise but also suspicious activity?

Unknown Unknowns
An additional challenge is measuring not just what you are doing, but also what you're not doing. Your controls may be working well, but are there other controls which you lack which you can't even begin to measure? Are there risks that you are experiencing that you don't know about?

Fortunately, there are ways to assess your program holistically to identify where there might be gaps. For instance, if transaction monitoring regularly flags fraudulent activity, consider how other elements of your program address fraud, to prevent such activity happening in the first place. Can you refine your customer risk assessment to better identify fraud indicators? Can you invest in new tools or integrate additional data feeds to calculate fraud scores? Gaps may appear over time, so you need to continuously monitor what your assurance process is showing you. For instance, if you start filing fewer fraud-related SARs, this could be explained by changes to KYC or monitoring controls, or by the fact you've hired a new team of analysts, who need more training on fraud typologies.

Keeping on top of industry trends and typologies will also help you understand the unknown unknowns. Unfortunately financial criminals are always coming up with new methods, so your financial crime controls need to be updated just as frequently.

Financial Crime
Finally, we come to a paradox. The metric which should be the most important and the most integral is also the one which is hardest to assess.

The aim of fincrime programs, the reason we're all here, is to stop financial crime. So are we? And if so, how much?

If we can't tell, how can we possibly assess whether what we're doing is working? The good news is, while it's hard to accurately calculate comprehensive figures, there are ways we can assess progress by looking at whether controls are becoming more (or less) effective. SARs are a key indicator, e.g. the number of SARs filed over time, the number filed compared to your peers, the value of the transactions covered by SARs, whether your SARs cover all known typologies, and the number of SARs triggered by internal alerts vs. those triggered by intelligence from law enforcement or other financial institutions. Fraud losses are another good metric - e.g. the amount of money identified as the proceeds of fraud which you stop before it leaves an account, vs. the amounts reported which you do not stop.

How to Measure

Having looked at *what* to measure, let's think about *how*.

Manual Assurance
Traditionally, this has been an intensive manual exercise. Regular testing generally comprises financial crime compliance analysts performing monthly or quarterly dip testing, supplemented by annual testing by the third line of defense or an external party.

Dip testing involves reviewing a certain number of samples of a prescribed list of activities (e.g. KYC files, screening hits, transaction monitoring alerts, SAR filings, etc.). Sample sizes can be chosen arbitrarily or calculated using complex statistical measures. Samples may be entirely random, or stratified - e.g. 60 high-risk customers files, 30 medium-risk customer files, and 10 low-risk customer files. They are reviewed to confirm if the correct procedures were followed; for instance, whether all the correct pieces of information were collected at onboarding, or whether SARs contained the right information presented in the appropriate manner. This generates numerical outputs ("what percentage of KYC files contain all the required data?"), ideally supplemented by narrative on common issues or shortcomings.

Manual testing is the most common way of evaluating fincrime controls, and it has a few advantages. It can be scaled up or down in response to available resources (although clearly scaling down decreases the quality and reliability of the output). It can focus on high-risk controls or customers, in line with a risk-based approach, and it is effective at identifying clear-cut issues. It ultimately asks straightforward binary questions about surface components of the program ("were all PEPs escalated per the policy - yes/no"), so the outputs are easy to understand and failings are easy to define.

However, there are clearly serious problems with this approach:

1. Sample-based testing means there's a chance of missing things, as it doesn't offer 100% coverage.

2. It is backwards-looking, so can only identify issues which started in the past; it cannot identify issues in real time. This means once an issue is identified, a remediation project is often needed to go back through ALL the client files, transaction monitoring alerts, etc. to identify other instances when the process did not work or procedures were not followed. This can be a massive exercise.

3. Given its partial nature, dip testing doesn't reveal the extent of a problem. If 5% of your sample fails the test, how confident are you of a 5% failure rate across all your records? Has the problem started recently, has it improved over the past year, or is it a continuous long-term issue? Based on this, what resources will you need to remediate and fix it?

4. This lack of information makes stakeholder engagement with senior management, partner institutions and the regulator very difficult.

5. As you grow, you need to either grow your headcount to maintain sampling levels, or reduce sample numbers and therefore assurance over your financial crime program.

Automated Assurance
So, if dip testing is not the answer, what is?

Rather than a manual process, you can adopt an automated one, which fundamentally changes and upgrades the nature of your assurance process.

There are clear benefits of an automated approach:

1. It can test and measure 100% of accounts and activity. This means you will never fail to identify an issue, and will always know the full extent of any failings that arise.

2. As automated testing runs continuously, you become aware of problems as soon as they emerge. Being able to identify issues in real time is a gamechanger. It enables you to fix problems before they have too much of an impact, limiting your exposure to financial crime threats. It also means you can avoid huge, expensive remediation exercises.

3. Automated testing can link different components of your program together, meaning if weaknesses emerge in one of your processes, or you introduce improvements, you can immediately see if there is a knock-on effect elsewhere.

4. The ability to react immediately and provide clarity around the scale of a problem can transform stakeholder management. If you can tell a regulator exactly how substantial an issue is, when it began, and how long you'll need to fix it, you'll be in a much stronger position and should be able to reduce the risk (and cost) of any regulatory fines.

5. There are savings benefits to introducing an automated process, as well. You no longer need a team of analysts performing time-intensive dip testing, and can instead redeploy your valuable second-line resources to higher value areas like in-depth investigations of suspicious accounts, or improving your controls.

6. You don't need to grow the assurance team as the business expands; the tech will continue to offer 100% coverage, so you can scale with confidence.

Automation can also help ensure consistency, another topic regulators are super keen on. This applies both internally, across different pools of analysts and over time, and across programs for sponsor banks and Banking-as-a-Service providers. Using an automated solution means you can monitor the controls of every program in your portfolio, giving you complete oversight and total coverage even as the number of customer programs grows.

Conclusion

There may not yet be a universal definition of financial crime controls effectiveness or specific regulatory instructions, but now you hopefully know that this needn't stop you introducing a robust process to measure and understand your firm's effectiveness.

The benefits of automating this process should also be evident; ensuring you have 100% coverage, understand the breadth and depth of any issues, and catching problems in real-time. This is the next step in the evolution of financial crime. The first wave of automation targeted the operations of the first line of defense (KYC, screening, transaction monitoring etc.). The next leap forward will be harnessing the power of technology to revolutionize assurance and enable financial institutions to understand and evidence their financial crime controls effectiveness.

cable

cable.tech