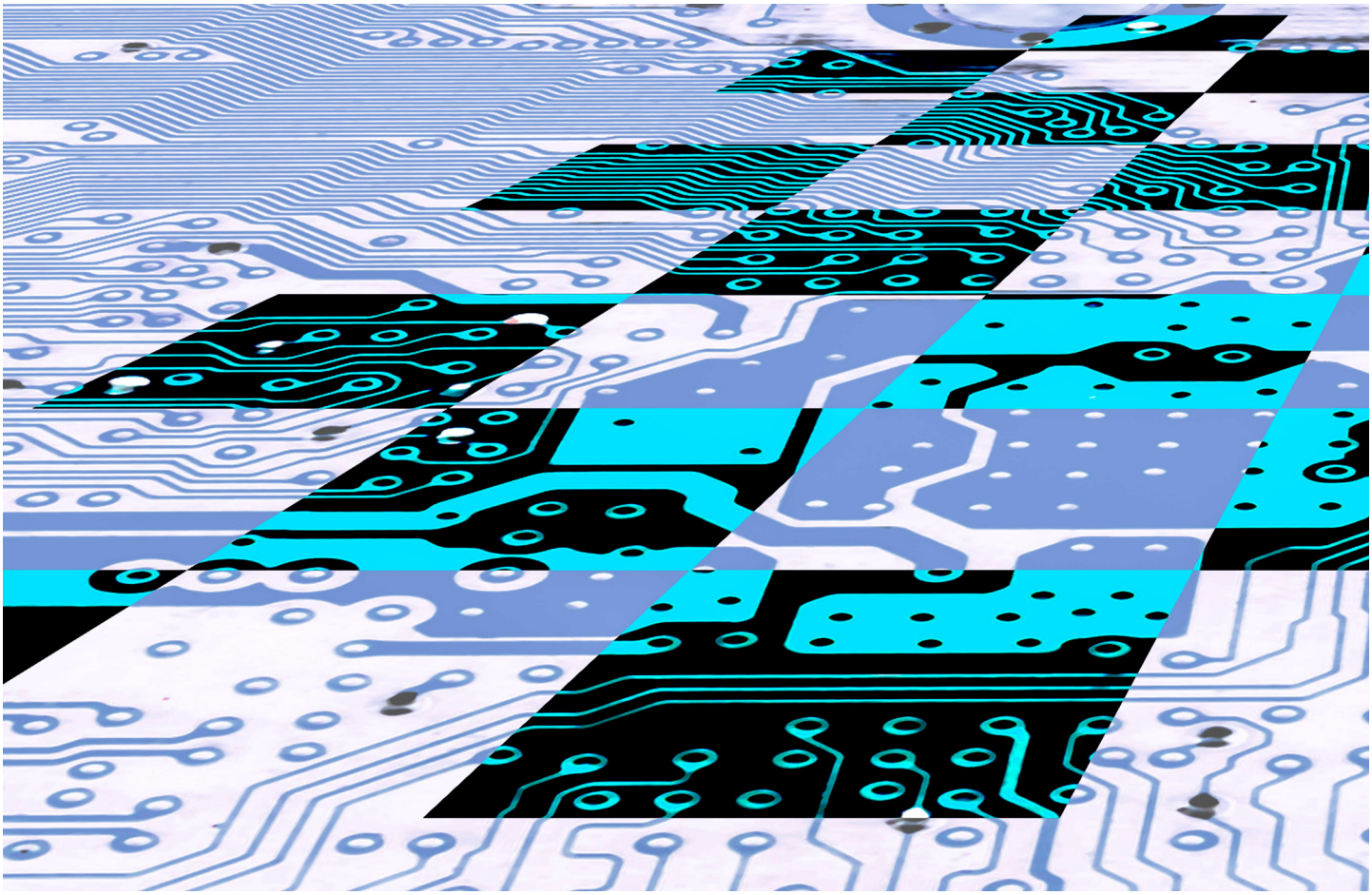
Risk publications

Check mates

AI and the future of KYC

Risk.net May 2019

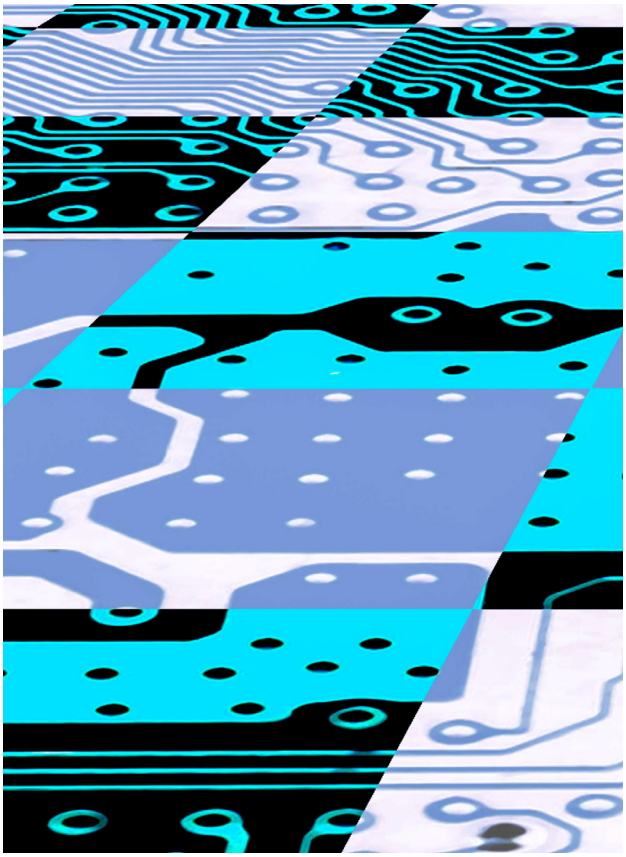


Survey report &
white paper

Risk.net

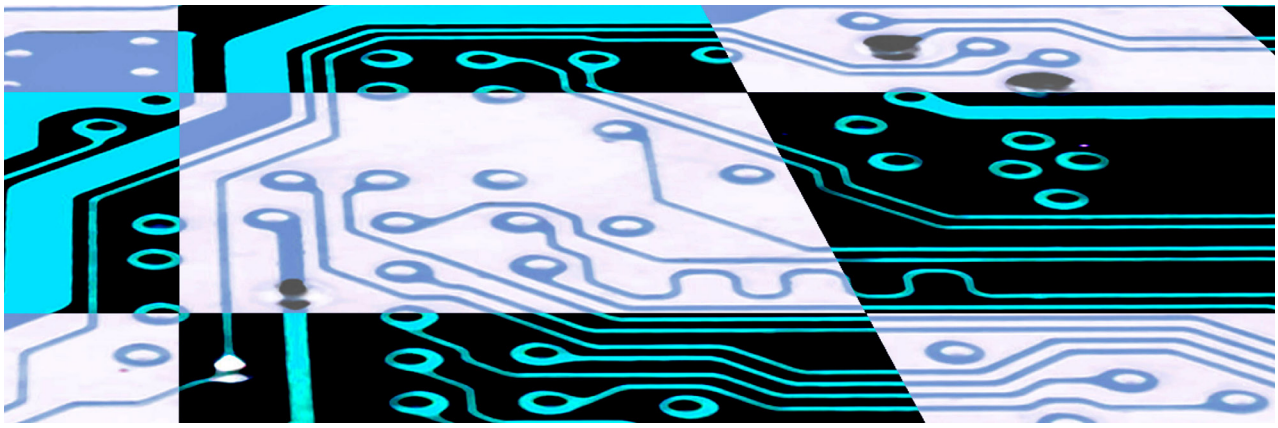
NICE · ACTIMIZE

Contents



Introduction

Financial crime prevention is an increasingly complex task for financial services firms. Criminal activities such as money laundering and fraud have rocketed, and the perpetrators are getting smarter. Amid tightening regulation and the threat of substantial fines for compliance breaches, firms are under intense pressure to improve their customer due diligence and know-your-customer programmes, as well as case investigation. But how are they coping? *Risk.net* partnered with specialists NICE Actimize to survey senior financial crime executives in banks and other financial services firms to assess the efficiency of current resources, processes and systems, and the potential of artificial intelligence-assisted technology to reverse a vicious circle of spiralling costs and resources.



With the possible exception of cyber security, no operational or reputational risk strategies today are as enterprising as financial crime. Catching up with the changing nature of illicit schemes – and putting in place the deterrents and checks to curtail them – is an immense challenge, like playing a game of chess, except far more strategic, more difficult and with much higher stakes. Firms need to stay several moves ahead of financial criminals, but they don't always have full visibility across the board. Bad actors are opening up new fronts and strategies every year, using increased variety and sophistication. They are smarter and more brazen. And, unlike chess, there is no such thing as an expendable pawn in combating financial crime – not when the consequences could involve serious losses or a costly enforcement action.

Once the stuff of settlements quietly finessed with regulators, those enforcement actions are now making headlines, and with good reason. Recently uncovered schemes have exposed large vulnerabilities at several major banking institutions, with some surviving for years and laundering billions of dollars without being properly detected or disrupted. The resulting fines, sometimes running into the hundreds of millions of dollars, send an unequivocal message. Like market or credit risk considerations, managing the risk of bad actors is now a balance sheet issue, and anti-money laundering (AML) is the most clamorous trouble spot. Today, controls must also monitor for a wider array of more subtle criminal activities, such as authorised push payment (APP) frauds and other spoofing techniques.

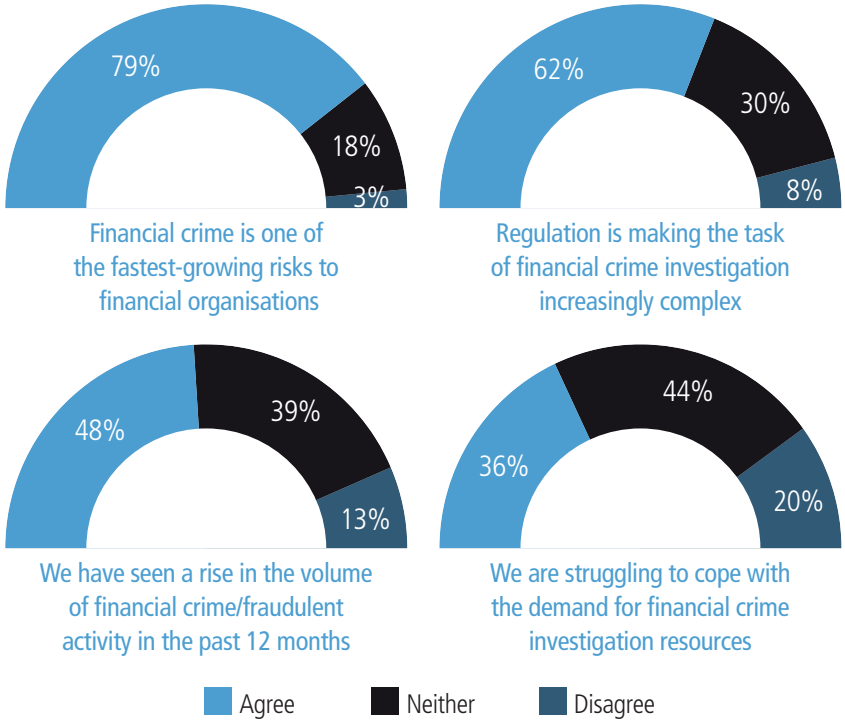
Dealing with these matters starts with the construction of an effective know-your-customer (KYC) check, and the test of a KYC process comes with two questions: is it efficient, and is it built smart enough? On the former point, the industry has undertaken a wave of collective efforts; for instance, by standardising and streamlining the identifier information required in widely available databases and utilities. The benefits of these improved inputs are undisputed, but bringing down costs and improving industry visibility are necessary – rather than sufficient – conditions of effective crime prevention. The second crucial component – building an intelligent internal framework that can carry KYC case management from initial data management to escalation and forensic analysis and finally to resolution – remains an open and more complex problem for many firms.

Risk.net and partners NICE Actimize spoke with 94 operational and compliance personnel across a cross-section of financial services firms, seeking to isolate the key issues and potential solutions as KYC continues to climb its way up the ladder of institutional priorities. The research aimed to characterise a robust and efficient KYC process for 2019, identify the common shortcomings firms are grappling with, and examine their rising technological maturity – in particular, the acceptance and implementation of robotic process automation (RPA), artificial intelligence (AI) and machine learning applications. The results presented in this report confirm a changing mindset around KYC, and an enterprise function that needs to do some rapid catching-up.

KYC – Pressure and time

Even before today's increased collective awareness, KYC posed a resource-intensive and often cumbersome challenge for bank and investment managers' customer onboarding. It begins with a volume issue. The globalisation and electronification of markets has increased the sheer number of customers to check, as well as the kinds of legal entity construction and different levels of opacity to break down and sort through, and as quickly as possible. In recent years, this has coincided with a veritable explosion of new national and international mandates aimed at curbing illicit financing activities or the outright restriction of market access to certain persons and entities for political reasons. In combination, these elements have pushed KYC and customer due diligence (CDD) spending to incredible new heights. A 2017 estimate by Thomson Reuters put it as high as half a billion dollars annually – just for a single large financial enterprise.

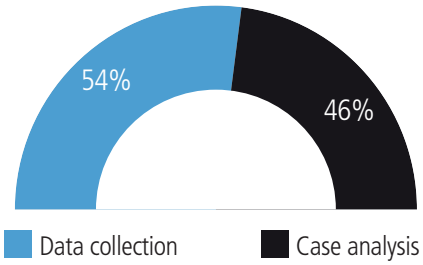
1 Do you agree or disagree with these statements?



The raw spend is only half the issue, however. Because many KYC/CDD matters are far from black and white, today's cases must be analysed against risk appetite and the transaction at hand. While there are certainly best practices from which to borrow, KYC case management frameworks vary considerably from one institution to another. A new client doubling a fund's assets under management or a major securitisation deal will, and should, inevitably invite more due diligence than a far smaller one-off transaction with fewer legal ramifications attached. The counterparty always matters. But so too does the context, the existing exposure to the customer across the enterprise, the downside risk, the potential revenue generated and the window or deadline within which to complete the trade or deal. KYC, therefore, is more than a simple check against historical activity patterns or a sanctions list. It is a matter of pressure and time and, as a result, initial decisions often rely on incomplete information.

The industry has rightly focused on technological steps to improve KYC and CDD. As the financial technology – or fintech, as it is known – revolution reinvents core pieces of payments and trading infrastructure, KYC is now being baked in. KYC registries, faster checks sitting closer to trade execution, straight-through processing mechanisms for illiquid instruments, payments, innovations and elements embedded in distributed ledger-based 'smart contracts' all reflect the need to streamline and automate processes around KYC, and especially the need for attaching and distributing KYC data as it flows downstream.

2 What percentage of your current investigation process is spent on data collection versus case analysis?



But we aren't there yet. One of the most urgent takeaways from the research is that, despite growing spend and these new points of progress, firms remain in a KYC/CDD morass.

Nearly eight in 10 respondents (79%) identified financial crime as one of the fastest-growing risks to their organisation, but only 20% reported meeting the demand now placed on their financial crime investigation function (see figure 1). This share was lower still – around 15% – among larger institutions (or those managing more than $10 billion in assets).

In both cases, the strugglers far outweighed the strivers. And the source of this frustration is clear: while a strong majority of KYC teams' time should be spent on case management and analytical activities, respondents said that more than half their time (54%) is instead spent on data collection (see figure 2).

False positives – The old bugaboo

What are the intricacies of this data issue? How do they manifest, and what emerging technology can be deployed to mitigate them? The first point of departure always comes down to process inefficiencies, and those surveyed pointed to an old source of disquiet for KYC: false positives.

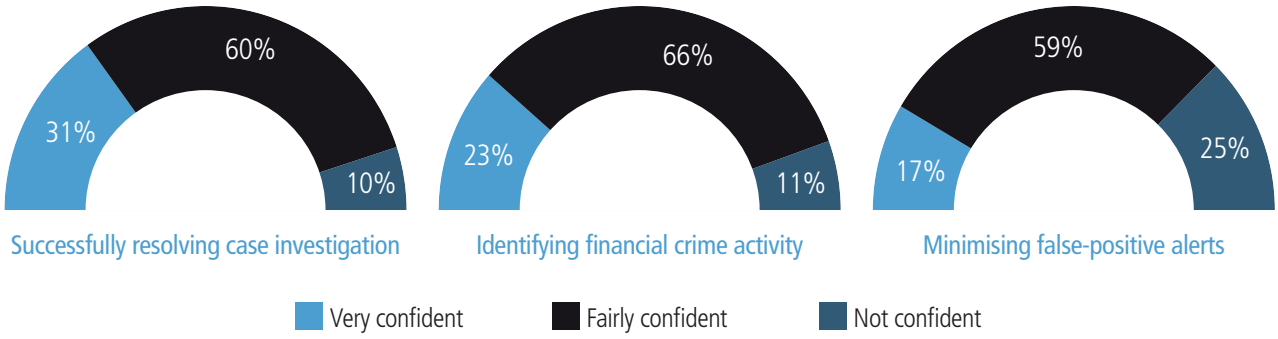
Screening millions of data points for targets worth escalating for investigation is fraught, because similar or identical names naturally overlap, lists and thresholds become outdated as political winds or regulation changes and, being large datasets, they can suffer from traditional data governance problems or poor curation over time.

Again, introducing new varieties of fraud such as APP into the mix can only serve to accentuate these shortcomings. Those surveyed noted minimising false-positive alerts as the most problematic element they face today, with a confidence score much lower (25%) than other aspects of the process (see figure 3).

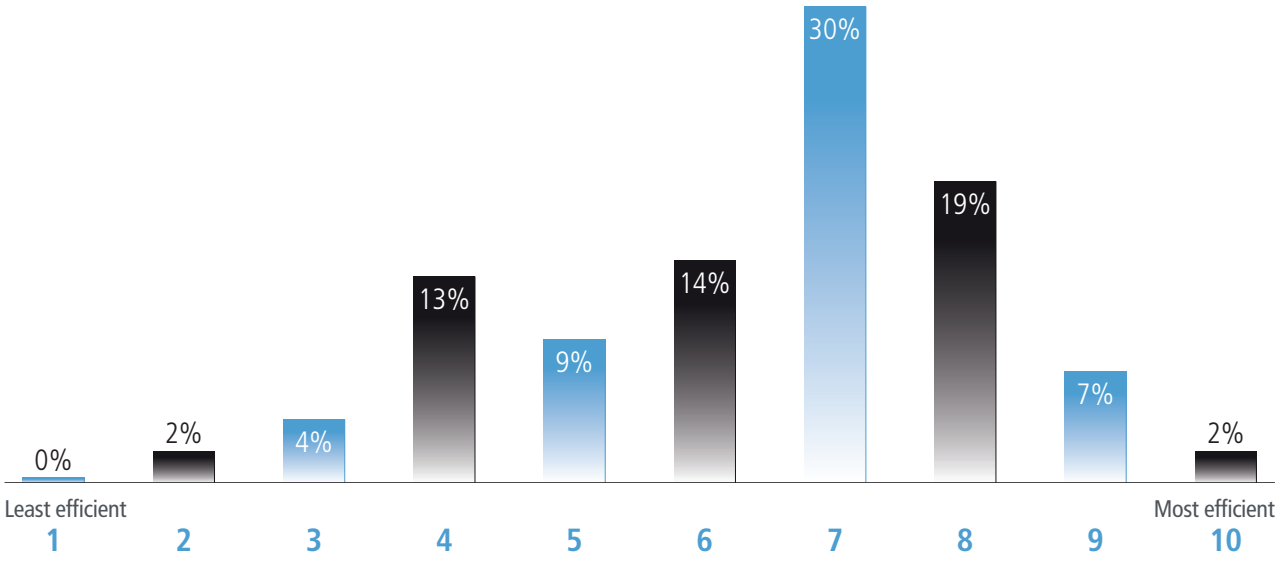
This preoccupation goes a long way towards explaining firms' perception of themselves in terms of efficiency and of KYC/CDD operations as a sort of 'middle-of-the-pack' function. Asked to rank themselves on a scale of 1–10, the largest single response across large and small firms was an above-average 7 (30%), although nearly that same number ranked themselves at 5 or below (28%). Only 9%, meanwhile, saw themselves as a centre of excellence with a 9 or 10 score (see figure 4).

The results are also interesting after deeper segmentation. Smaller firms reported having a much harder time with false positives, with only 17% very confident in their capacity to cope. Meanwhile, few of the larger firms declared themselves "very confident" in their crime identification and case resolution. These extremes also played out in the efficiency question. Smaller firms tended to spread out more evenly across the whole spectrum, with more than 20% saying they were between 2 and 4, and more than 10% at 9 or 10, whereas larger institutions played slightly more to the middle.

3 Confidence in organisations' current systems and processes



4 Rank the efficiency of your existing investigation process



The life of a transaction

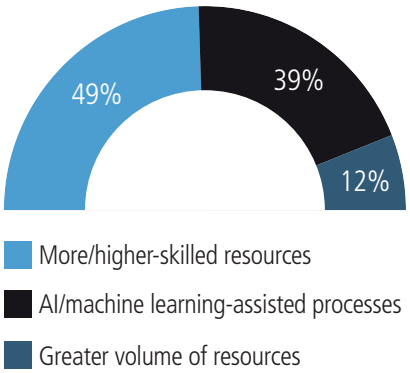
The survey next dug deeper into exactly where these inefficiencies are located, and what kinds of resources are required to solve them, including potential AI-fuelled automation. These questions exposed a link between foundational problems associated with KYC data management and broader problems that manifest throughout the rest of the KYC programme and beyond.

To start, respondents identified the top-line aspects of KYC/CDD that they find most challenging. By far, the broadest consensus on this question was "inaccessible and unaligned data", particularly true of larger enterprises, where it gained almost three times as many "top challenge" nods as any other option. A strong second was "inefficient workflow and business processes", while error-prone, low-value and high-volume remediation tasks were also identified, especially among smaller firms' respondents – gaining a strong share of "second-highest challenge" votes (see figure 5).

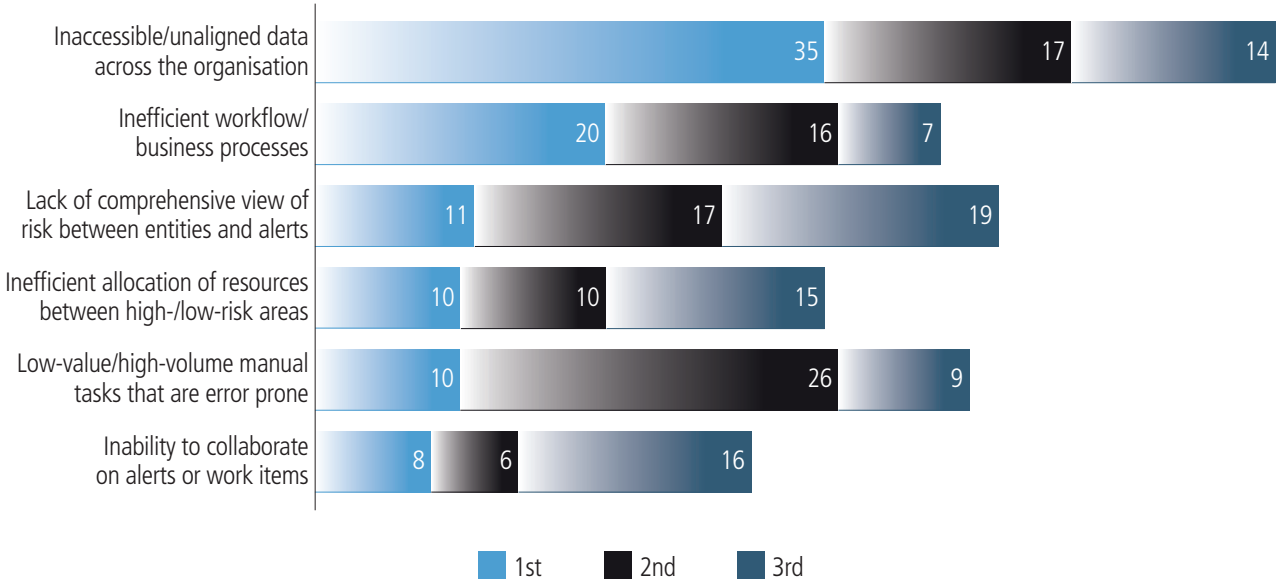
The survey then asked how these issues could best be addressed. Despite the head count that has been added to KYC, CDD and fraud prevention in past years, simply increasing the volume of resources garnered only 12% of responses (see figure 6). Tellingly, the two alternatives – more and higher-skilled human resources and AI/machine learning-assisted processes – were fairly evenly split; however, the breakdown was mixed. Larger institutions, which presumably have the budget to choose, still favour better human investigators, at 57% – although one-third (33%) pointed to AI-assisted processes. Among smaller firms, the split was converse but closer to being an even one – with a full 46% favouring AI and 40% looking to more highly skilled personnel.

The thrust here is that today's financial crime issues aren't purely about information theft; in fact, the need for rote data acquisition or supplying head count is really only a first step in transforming a KYC process. Rather, what firms need now is improved platforms and internal structures that drive towards "knowing your transaction" as well as your customer. That means ably distributing data across the enterprise and interacting with diverse analytics monitoring for AML patterns and fraud types. It means aligning KYC with other customer-facing tasks and behavioural data to alert potential mistaken actions, such as APP frauds, faster. And it means flagging up larger targets with accuracy. Today, bigger isn't better – smarter is better. In addition to more and higher-skilled resources, there is significant interest in adopting AI-driven automation – which will have the added benefit of allowing skilled resources to spend more time putting their skills to use. The question is: how much and how fast?

6 Which has the greatest potential to transform the efficiency of the case investigation process?



5 What do you consider the most challenging aspects of your current investigation process?



AI's checks and balances

To this end, the study set to identify the most likely homes for AI in KYC/CDD programmes, and the reasons why AI tools – including more rudimentary tools such as RPA – aren't in place quite yet. It found that many firms are still aiming to strike a balance with AI: using it where they can to enable personnel to proceed to more difficult investigation and decision-making tasks instead of completely delegating a task to machines. Still, there was evidence to suggest many firms see AI as a more active part of their financial crime deterrence in the future, as machine learning techniques become cost-efficient, more explicable to regulators and more flexible in their implementation.

One set of responses epitomised the current state of play, where the highest number by far – nearly half of all respondents (48%) – pointed to lower-level task automation as the value proposition for introducing AI-based tools. The reasons for this come back to the required process and explainability: KYC is one aspect of operational compliance requiring significant risk-aware judgements to inform final decisions – not only for financial crime compliance but for the business. Even those firms looking at AI seriously will prefer a layered combinatory effort when managing financial crime matters – particularly those that might need to be justified before regulatory authorities or imply real reputational and financial consequences (see figure 7).

Given this outcome, another query examined why firms may be delaying on RPA. Probably most surprising here is the low percentage of firms (13%) already exploring or using these tools. But a majority of respondents reported seeing possibilities implementing RPA, but for practical considerations. The problems they report include cost (56%) and, to a lesser extent, lack of staff/expertise (38%) and regulatory concerns (30%), which were emphasised more among responses from larger firms (see figure 8).

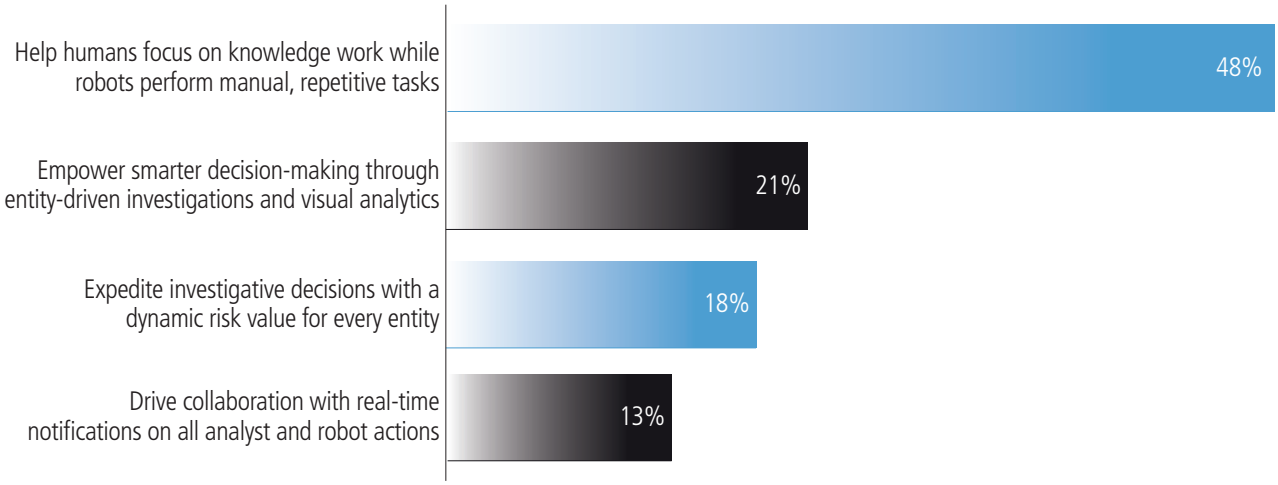
Still, the other three options in the initial question received a fair amount of support and warrant some discussion. Two of these – "entity-driven investigation support" and "dynamic risk profiling" – augur more advanced AI and would establish machine learning as a far more influential ingredient in the KYC case management process. In fact, taken together, these two choices attracted one-third of larger institutions' responses (33%) and almost half (46%) among smaller institutions. These chunks are quite notable as firms begin to think more about replacing, rather than merely supplementing, stickier aspects of financial crime oversight with AI.

So, how should these seemingly contradictory results be read? KYC, while growing in organisational stature and technical sophistication, still supports compliance functions where human eyes, not technology, tie up much of the spend and are ultimately liable for decision-making. It is worth remembering that, while AI isn't new, its application for financial services operations broadly is. Even for AI-enthusiastic firms, these results reveal it is difficult to transform overnight.

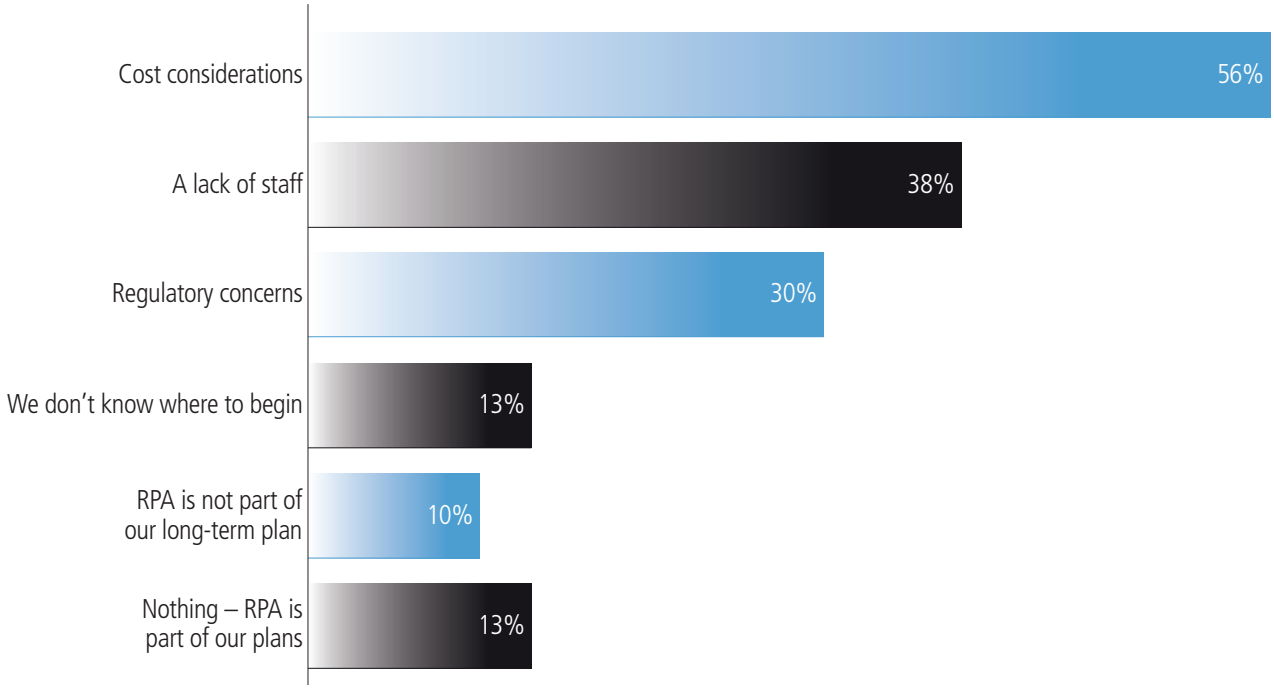
Likewise, the point of entry may be shifting. If a growing percentage of firms is looking for AI to take a more active part in the process rather than only doing the 'dirty work', then they may be in for higher costs as they seek higher forms of AI than RPA.

In short, there is a huge opportunity to bump up AI going forward and serious interest in doing so – but legitimate challenges remain in realising that potential.

7 Which of the following perceived benefits of AI/machine learning-assisted case investigation do you consider the most valuable?



8 What would prevent your organisation from implementing RPA as part of your investigations?



Concluding thoughts

Financial crime is on the move, and financial services must move with it. For those familiar with AML, fraud prevention and KYC's pivotal role at the core of these practices, the survey confirms some familiar and age-old problems but offers a fresh take in several new areas. KYC appears ready to mature and – given the emphasis now placed upon it – it must. Data is still the crux of KYC-related issues. But the nature of these issues and the way they are evaluated, the organisational strengths and process required to ground that evaluation and the innovations available to do so, all indicate a strong evolutionary trend. The most viable way to get there is through more advanced technology such as AI taking on a more prominent role – whether assisting skilled humans in stewarding KYC data, or taking up tasks of its own.

Several conclusions from our research support this approach. These include:

- Data troubles continue to take up too much time relative to case analysis; a split with far greater weight on case analysis is currently closer to 50/50. That must change if KYC operations are to become more efficient.

- Minimising false positives remains the heaviest burden for KYC functions, leading to sluggish processing and manual remediation, grave potential errors, bloated budget for head count, and misuse of skills and enterprise resources.

- Where once simply sourcing the right KYC data was a chore, the greatest problem now involves creating an enterprise-grade platform for managing the ecosystem around this data, the case management workflow surrounding it and distributing it for a wider variety of compliance, risk and business processes.

- Increasingly, your perspective on AI matters. Very few firms reported that higher head count was the solution to the previously mentioned issue; rather, they said smarter application of skills and automation was the answer. The question is in the mix and direction of each of these.

- That mix appears set to evolve. Of course, reducing false positives and enabling human resources is paramount, but just how this is achieved now is unclear. A surprisingly large number of firms reported seeing the value in a more essential role for AI-based tools, in addition to taking on rudimentary data tasks to free up human eyes.

The continued transformation of KYC and CDD should prove fascinating, and the trajectory of financial crime oversight remains decidedly linear: towards faster response times, greater pattern recognition and case analysis with fewer errors, and mastery of increasingly complex decisions. Should it remain that way, the need for a boost from AI should develop from a luxury into a necessity. The stakes are already high and, in 2019, the game is well and truly on.

Risk.net

NICE · ACTIMIZE

A RISK.NET WHITE PAPER, COMMISSIONED BY NICE ACTIMIZE