Risk publications

Smarter thinking around financial crime prevention

Risk.net January 2019

Survey report & white paper

Risk.net

IBM®

Smarter thinking around financial crime prevention

As the current approach to financial crime monitoring and investigation pushes financial firms' resources to the limit, IBM assesses the key challenges and potential risks of current anti-money laundering and customer due diligence processes, and discusses the opportunity for artificial intelligence and cognitive technologies to drive a step-change in efficiency

Introduction

Banks of all sizes must comply with increasingly onerous anti-money laundering (AML) and customer due diligence (CDD) regulations. This has necessitated a marked increase in the time and resources that must be dedicated to these areas. However, existing technologies designed to handle AML and CDD compliance are fragmented and based on rudimentary rules that cannot handle this increasingly complex area of compliance.

As a result, they provide little insight into the true risks individuals and incidents present, and often lead to lengthy manual investigations to confirm or dismiss alerts of potential criminal activity. Alongside these inefficiencies, the growth in resources that banks have been required to devote to financial crime prevention and compliance management has become unsustainable.

According to a survey conducted by IBM and *Risk.net* in November 2018 among 89 financial services professionals involved in financial crime analysis and investigations, organisations in this sector are increasingly concerned by these issues and many employees are dissatisfied with current approaches to AML and CDD.

Rather than continuing to invest more resources in this area, however, banks are beginning to see the benefits artificial intelligence (AI) and cognitive capabilities can bring to this part of the business. By providing greater automation and enhancing the insights needed to make faster, more effective decisions in relation to AML and CDD, banks are already looking into ways of using these techniques to address these problems. While some organisations are already experimenting with these technologies in limited use cases, others are holding back because of perceived uncertainty over the regulatory reaction to such new tools.

So how can banks address their responsibilities and challenges related to current AML and CDD systems and processes? How can technological innovations such as AI and machine learning be leveraged to make financial crime investigations more efficient and effective, both in terms of the resources devoted to such activities and the use of analysts' time and expertise?

Increased scrutiny

To address the need for greater financial transparency following the global financial crisis, governments and regulators ushered in a rapid expansion of requirements for financial firms, which continues to this day. As a result there is increasing regulatory pressure on banks to monitor and tackle financial crime, and enhance current systems to identify issues or events that might previously have slipped through the cracks.

As well as a long list of AML fines imposed on financial services organisations recently – including Deutsche Bank, Citi and BNP Paribas – this pressure comes in the form of new rules and requirements that banks must satisfy. One such example is the CDD Requirements for Financial Institutions rule – an amendment to the US Bank Secrecy Act that became effective in May 2018. This rule aims to improve financial transparency by strengthening due diligence requirements for banks and other financial institutions.[1]

Similar regulations are being adopted in jurisdictions worldwide. The list of countries signing up to international initiatives to increase financial market transparency continues to grow. A common theme among these regulatory regimes focuses on the need for financial firms to gather, store and report key data relating to their customers to prevent money laundering or other unlawful activity from jeopardising the integrity of local and international financial systems.

To address this growing body of regulation in an environment where financial crime activities are becoming increasingly sophisticated, banks must invest more money, time and resources in detection and prevention to continually improve and update capabilities. But are financial organisations getting the most value out of these investments? How do they know they have the best tools and resources to monitor and prevent financial crime?

Unsustainability

In November 2018, IBM and *Risk.net* conducted a survey of financial services professionals working in risk and compliance roles ranging from AML analysis and investigation to cyber-security risk management, as well as chief risk officers and chief compliance officers.

It is clear from the results that organisations in the financial services sector are devoting an increasing amount of resources to AML and CDD activities. Nearly half (46%) of organisations polled had increased financial crime employee numbers by up to 10% over the previous 12 months, while three in 10 expect further growth of between 11% and 25% over the next year.

But is this state of affairs sustainable? Banks cannot continue to push increasing amounts of resources towards such activities indefinitely, and so there is a need to find a more efficient way to satisfy regulatory requirements designed to tackle financial crime.

A large part of the investment in financial crime prevention tends to be dedicated to hiring analysts and investigators, as well as other human resources-related spending. Indeed, nearly three-quarters of respondents to the survey estimate their organisation has added up to 25% to the head count of their financial crime unit over the last year. And while a similar number (74%) believe the current number of analysts or investigators dedicated to financial crime prevention within their organisation is sufficient, only 16% believe there will be no further growth in this area in the next 12 months.

In recent years, banks have made material investments in improving skill sets and hiring additional staff for financial crime prevention teams. As such, it is crucial to ensure these analysts and investigators are spending their time in the most valuable way. However, on an average working day these analysts are often inundated with tasks relating to the collection, collation and transfer of information rather than interpretation. This means spending less time analysing and making critical risk decisions based on that information. This is an imbalance that needs to be addressed.

THE RISK.NET/IBM FINANCIAL CRIME SURVEY

This financial crime survey, conducted by *Risk.net* and comissioned by IBM, received 89 valid responses. The survey was conducted in November 2018, and respondents were drawn from financial services professionals involved in financial crime investigation and analysis.

[1] *Financial Crimes Enforcement Network,* FinCEN reminds financial institutions that the CDD rule becomes effective today, *May 2018, https://bit.ly/2C1gQsF*

A multitude of challenges

According to the survey results, it is clear that financial crime analysts working at financial institutions believe their investigation processes leave substantial room for improvement. Only one in 10 respondents to the poll assigned their organisation the top rating for the effectiveness of its investigation process, while slightly more (11%) gave their organisations full marks for efficiency in this area.

The survey provides some insight into the challenges financial crime analysts encounter in this area, which could explain this perceived lack of efficiency and effectiveness. While regulatory complexity, resourcing limitations and management pressures point to longer-term business issues that are harder to control, it's notable that respondents' top five challenges are symptomatic of shortcomings with current tools and processes. Problems such as 'false positives' or weak data, as highlighted below, are more easily tackled with the right technology in place:

False positives

40% of survey respondents see a "high number of false positives/unsubstantiated alerts" as one of the three top challenges they face during the investigation process. This number rises to 60% among the largest organisations.

Many existing AML and financial crime monitoring systems used by banks issue an alert when anomalies, suspicious issues or activities are detected. On receiving this alert, financial crime analysts are then assigned the task of researching the issues raised. They must attempt to understand why the alert was created and then make a decision to either validate or invalidate the issue. The process and the decision must also be fully documented and properly recorded within the bank's systems.

However, while detecting and managing real risks is clearly the aim of this process, all too often analysts must spend time investigating and documenting false positives. To invalidate a suspicious event or activity – to identify the activity as legitimate and of little or no risk to the institution – the analyst responsible must build a case to prove it as such. Ironically, this process may take longer than it does to submit a suspicious activity report (SAR) or a suspicious transaction report (STR) to report high-risk activity.

A complicating factor within this process comes from the volume of false positives financial crime analysts receive. With current systems, many banks are inundated with alerts, and a common statistic quoted within the industry is that, for every 100 alerts generated, only one or two result in an SAR. As such, analysts can spend far more time dismissing false positives than they do addressing true financial crime threats.

The time taken to investigate false positives that are eventually recorded as low or no risk, rather than resulting in an SAR/STR or further research, varies by organisation. For the largest percentage of respondents (32%), this task takes an average of between 16 and 30 minutes, while for 30% the average time is between 30 and 60 minutes.

Weak data and insights

37% of respondents highlighted the lack of data or insights around customers, accounts and entities within systems and processes as a major challenge during the investigation process.

Banks typically gather the information relating to these areas while onboarding clients and conducting periodic reviews. Increasingly, under most regulatory regimes, there is also an expectation to have better controls to detect higher-risk customers. However, the use of outdated processes and tools to evaluate risks in this area means the net is often cast too wide. As a result, customers can be caught up unnecessarily in due diligence refresh cycles and, aside from the potential negative impact on customer relations, this creates additional work for analysts to collect the relevant information to exclude the customer from further enquiries.

The average time taken to perform an enhanced due diligence check – to provide additional validation of a potentially risky individual, either during an initial or a periodic review – runs between 31 and 60 minutes on average, according to nearly half of respondents (47%), while a further 17% report it can take up to three hours to complete such a process.

Figure 1 Effectiveness and efficiency of existing investigation processes

	1	2	3	4	5
Effectiveness	6%	11%	32%	42%	10%
Efficiency	6%	16%	25%	42%	11%

Votes were cast using a scale of 1–5, where 5 denotes existing investigation processes are most effective and efficient, and 1 denotes least effective and efficient.

This points to inefficiencies within current systems and processes, and similar technological challenges are clearly a top priority among respondents. Further evidence is found among the 45% concerned about the time investigations take to complete, the 42% who complain systems and tools are either incompatible or outmoded, and the 29% who struggle to process high volumes of information.

The challenges identified in the survey could certainly contribute to the previously noted belief among respondents that there are not enough resources within organisations to tackle financial crime. Continually increasing investment in this area is not sustainable, so a better option may lie in improving efficiency and productivity. This can be achieved with the right technology.

Figure 2 The main challenges organisations face during the investigation process

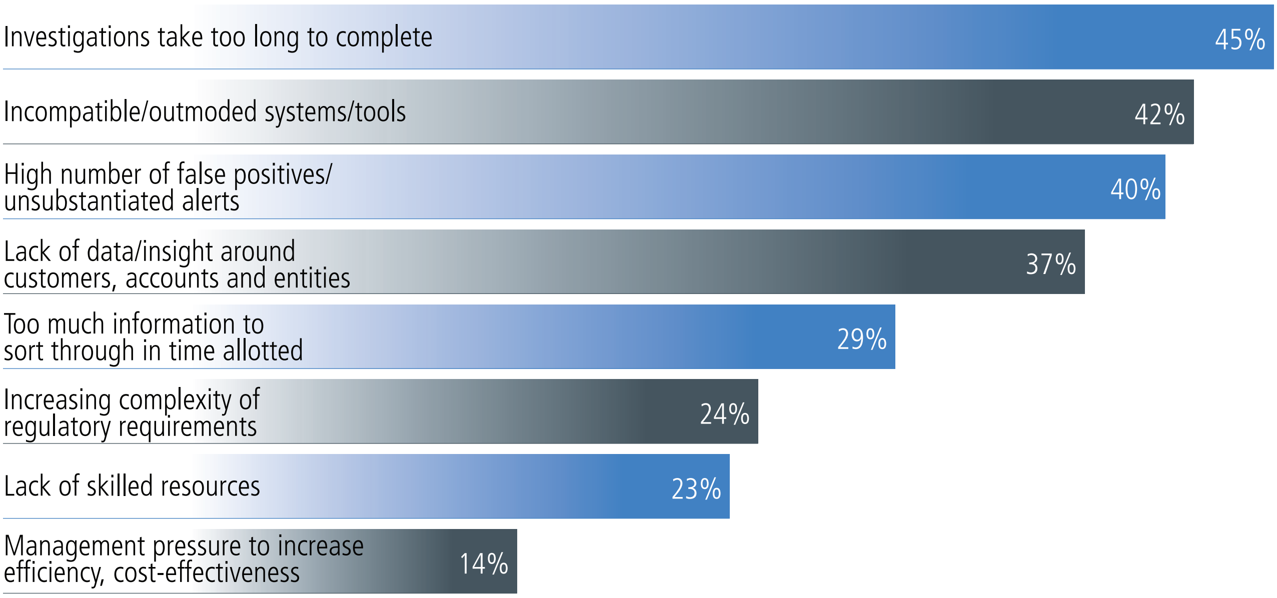
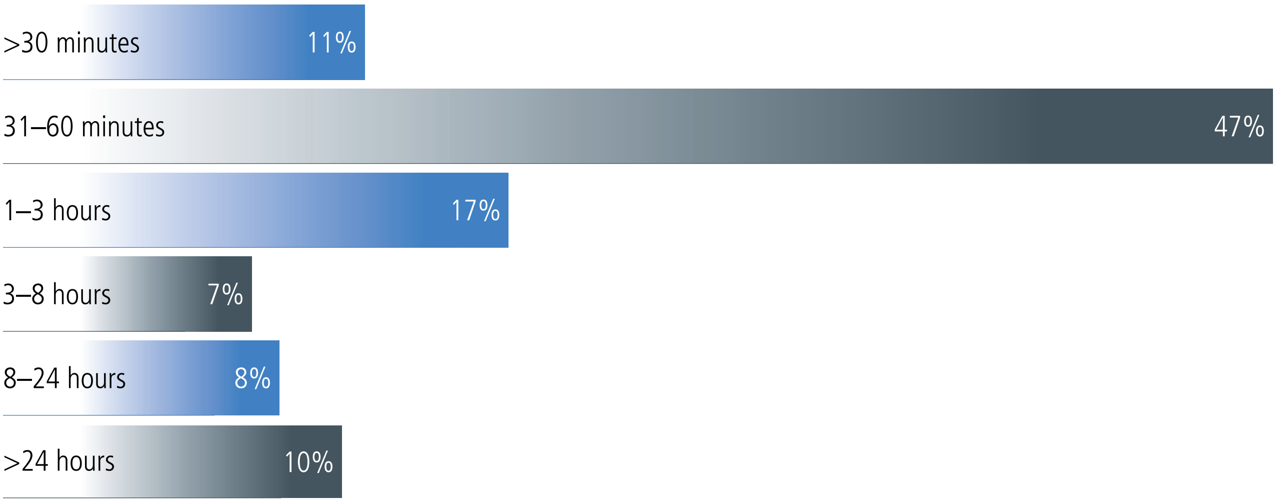


Figure 3 Average or expected time to complete an investigation, using enhanced due diligence processes



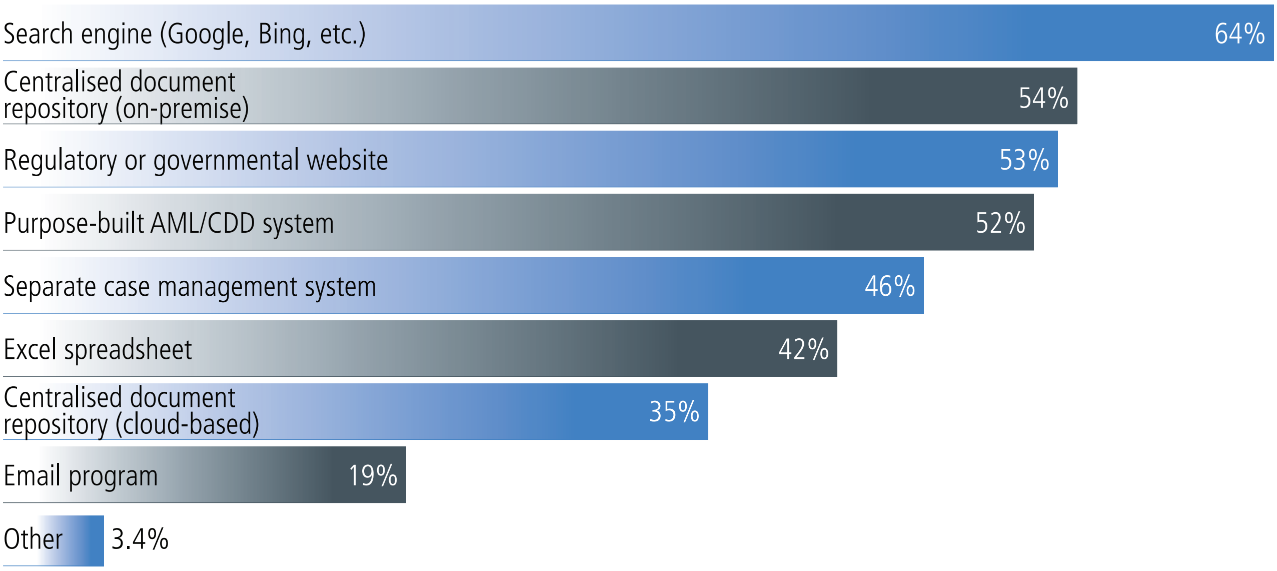
Current systems fall short

Banks need to continue to aim for the highest standards in relation to financial crime prevention, but maintaining existing systems and processes while addressing the growing slate of regulatory requirements requires investing an ever-increasing amount of time, resources and expenditure. By adopting new technology such as AI and machine learning, banks can enhance their current financial crime monitoring and detection capabilities, creating more effective systems and processes that use analysts' time more efficiently.

Financial services firms that participated in the survey currently make use of a wide range of technologies and tools during their analysis and investigation processes – the most popular being non-specialist search engines such as Google and Bing (64%), followed by websites provided by governments or regulatory bodies (53%).

In terms of internal and purpose-built tools, 54% use on-site centralised document repositories, while 52% use a purpose-built AML/CDD system. A further 42% use Excel spreadsheets, which are commonly used across financial organisations because of the ability to quickly change and develop versions customised to teams or even individuals. However, this presents the risk of mistakes being made and repeated throughout the system due to the high volume of manual inputs.

Figure 4 Technologies/tools used by organisations during the analysis and investigation process



Making a fundamental change

Most analysts using these systems spend a significant amount of time gathering information and documenting decisions as part of a predefined process relating to banks' compliance needs. Industry estimates gathered by IBM indicate analysts can spend up to half of their time collecting the necessary information about customers and transactions using current tools, while a further 25% is often spent documenting decisions for compliance purposes. This leaves only 25% of their time to concentrate on the most valuable analysis and decision-making activities.

Once the pressure to spend so much time on upfront collection of information has been removed, financial crime analysts can spend more time on in-depth investigatory work. This will have the added benefit of driving a more analytical culture within these organisations, placing a higher value on this kind of activity as performed by employees. The initial work of collating information can be performed – and often performed better – by technology.

By continuing to add employees to keep pace with demand, banks are postponing a rethink of their current approach, which ensures their existing systems and processes remain highly manual. This may explain the lack of efficiency and effectiveness identified by survey respondents. However, if institutions were to shift their approach by concentrating fewer human resources on performing low-level alert triage and data entry instead, banks could focus on getting greater value from higher-level resources such as analysts. In this way, banks can establish more efficient processes and create a more effective way of managing and detecting financial crime.

New technology offers a better way

What are the options for banks that wish to enhance current systems and processes using AI and cognitive capabilities?

Addressing false positives

Banks can increase efficiency by using intelligent robotic process automation to deal with routine tasks, reducing the need for human intervention in simple, low-value activities. By using text analytics, natural language processing and cognitive insights, these tools can parse both structured and unstructured data to generate better contextual understanding, leaving analysts to devote more time and energy to in-depth analysis.

By automating simplistic but time-intensive compliance tasks that had often been performed manually by analysts, such tools can reduce compliance risk, improve consistency and reduce costs for banks. However, most importantly in this situation, advances in machine learning utilised by such tools improve the accuracy of legacy systems and reduce the false positives banks have identified as a major challenge in relation to current financial crime investigations.

Enhanced data and faster investigations

Robotic process automation can also be used to increase efficiency and effectiveness of CDD checks and lengthy enhanced due diligence reviews. By minimising the need for time-consuming analyst intervention, such tools can perform routine tasks faster and reduce the risk of errors.

This type of technology can also provide an initial level of insight around key data points for bank analysts to work from, improving the speed and efficiency of decision-making. For the 37% of financial crime prevention employees that identified challenges in gaining insights on existing customers, such tools can enhance data aggregation, expanding the universe of information available by linking previously unconnected data.

Regulatory reactions

According to the survey, 14% of respondents do not currently see the need for AI and cognitive learning in their risk and compliance functions, while more than half are still evaluating its use in this area. So what is preventing banks from implementing a full overhaul of current systems and processes to incorporate such tools?

Quite often, regulatory response remains an overarching concern. Some banks have held back from adopting the increasingly advanced technology available to enhance financial crime monitoring and prevention because of concerns around how regulators might view such tools. Such organisations might be unsure of how to leverage new techniques that have not been 'officially' approved by regulators to satisfy existing compliance rules and parameters.

For many organisations, there may also be a perception that these techniques and their results are not 'explainable' to the regulator. There are concerns around how an alert can be dismissed on the advice of a computer system. Quite rightly, these organisations feel the need to be able to explain why the system is making a particular recommendation to an analyst. They want full control of the factors uncovered during the initial information-gathering stage that led to the decision to close or escalate an alert.

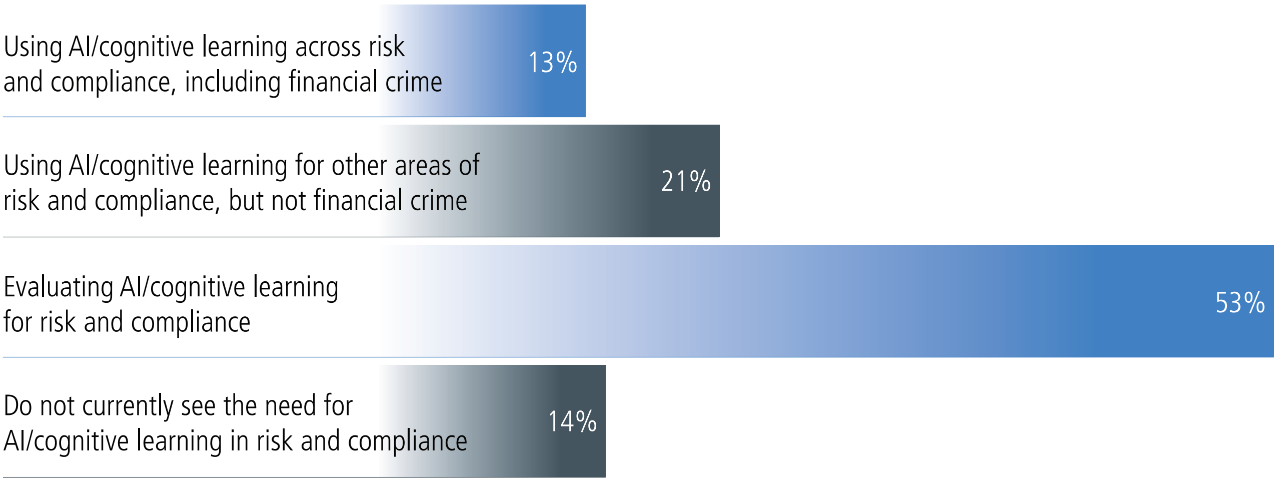
Testing new techniques

The push to innovate in this space continues in spite of such concerns. According to the survey, 56% of financial crime analysts and investigators see "automated disposition of alerts" as ripe for improvement using AI and cognitive technologies. IBM is already working with banks making significant progress in this area. Some organisations have gained approval from regulators in support of automatic dismissal of alerts relating to customers that fall below a certain risk threshold, as long as checks are made on a random sampling of these accounts to ensure quality control and accuracy.

Most practitioners agree that addressing false positives should be a key aim for the use of AI and cognitive technology, with the ultimate objective being to remove the need to dismiss an alert at all. In the short term this remains aspirational, with the next best option at present being to expedite the triage and risk prioritisation of those alerts. Indeed, nearly two-thirds of respondents identified this as an area that could readily be enhanced with the use of AI and cognitive capabilities.

Banks are starting to investigate these technologies, with 13% of those surveyed already using such tools within the financial crime unit. For the one-fifth of respondents currently using AI and cognitive learning tools within the wider risk and compliance division, but not for financial crime investigations, an expansion into this area is a potential next step. As such, those that remain cautious or sceptical at this stage could be left behind as competitive financial institutions start to seek and eventually receive regulatory approval and support for automatic dismissal of alerts.

Figure 5 How organisations are incorporating AI and cognitive learning capabilities into their risk and compliance programmes



Pushing the financial crime boundaries

AML and CDD systems currently used throughout the financial services sector are often based on makeshift rules that were last updated when the systems were implemented. As a result, these systems create a high number of alerts, which require heavily manual processes and rely on a large number of analysts monitoring and addressing alerts of suspicious activity and high-risk individuals. The valuable analytical work these personnel should be concentrating on is often pushed to one side so mundane and manual tasks such as collecting and reporting on initial findings can be completed for compliance purposes. This is quickly becoming an unsustainable situation – particularly for larger banks that are often subject to greater scrutiny.

Financial institutions are increasingly aware of the natural fit that cognitive learning and AI can bring to the fields of financial crime prevention and compliance management. In short, these techniques augment the abilities of financial crime analysts, enabling them to perform in the most efficient and effective way by automating data collection and initial risk analysis. This helps the analyst focus on making the important decisions relating to understanding suspicious activities and transactions in context.

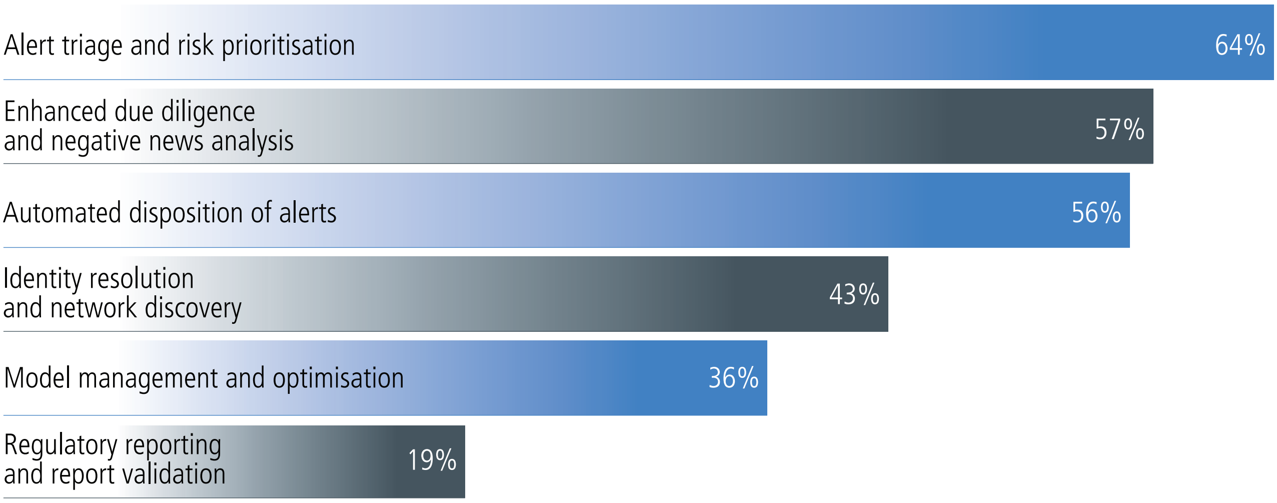
A growing number of banks are testing products and seeing early success in pilots that are being conducted with technology providers in the space. For those that wait, the competition is likely to gain a valuable lead in developing the most efficient way to comply with financial crime regulations.

Despite the perception of regulatory uncertainty, the message from many regulators is not to stifle innovation in this area, but to foster improvements in regulatory technology, as we have seen recently with guidance from both the UK's Financial Conduct Authority and a host of US agencies, including the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Financial Crimes Enforcement Network, the National Credit Union Administration and the Office of the Comptroller of the Currency. Rather than be punished for their creative approach to compliance, these leaders may help regulators define best practices and standards. Before that time, they will reap the benefits of better value from their investments, better use of resources and greater insight into both risk and their customer as a result.

LEARN MORE

For further information, visit *ibm.com/regtech* and schedule a consultation with a financial crime and compliance specialist.

Figure 6 Areas of the AML and CDD investigation process that could be improved using AI or cognitive capabilities



A RISK.NET WHITE PAPER, COMMISSIONED BY IBM