MOODY'S

Navigating the AI landscape

INSIGHTS FROM COMPLIANCE AND RISK MANAGEMENT LEADERS

MOODYS.COM/KYC

KEITH BERRY

Executive Summary

The findings of this extensive study into the attitudes, adoption, and uses for AI in the world of risk management and compliance are fascinating. What emerges for me first is that of the 550 leaders who engaged in the study, representing companies from 67 countries, everyone is on a journey to learn more, understand, and implement AI.

Some sectors appear to be further forward along the path, banking and fintech most notably, but almost 70% of respondents believe AI will be transformative or have a major impact within the next 3 years. And, almost 90% of respondents are interested in the integration of AI tools by providers of risk and compliance solutions.

AI technology has many facets, as listed by the experts who were interviewed for this study. AI solutions range from machine learning to robotics to large language models and generative AI. What emerges, however, is where people see these variants having most impact in risk management and compliance – it boils down to three specific areas:

1) **Transaction monitoring and risk detection**
2) **Individual and entity profiling and screening**
3) **Automation of manual tasks and efficiency improvements**

The message is clear that use of AI is about strengthening and enhancing the work that risk management and compliance professionals are accountable for each day. The findings show that the places early adopters or those trialing AI feel the most positive impact are in replacing manual processes (17%); augmenting staff performance (27%); or a combination of both (56%). And a vast majority (90%) of early adopters report AI is positively impacting the work they do in risk and compliance.

The correlation between data management and successful adoption of AI is, however, noteworthy. Data is so often at the heart of risk and compliance, and poor internal data could pose a barrier for many organizations navigating the AI technology landscape. The paradox is that AI could be the very solution to resolve issues with internal data. Perhaps this conundrum is still to be answered, but I certainly look forward to having the conversation with our customers.

The study also highlights the importance AI experts and risk and compliance leaders place on regulation in this space. There's 79% consensus that new legislation in use of AI is important to the profession. This points to the need for ongoing dialogue and collaboration between regulators and the industry to allay concerns, particularly around global standards, data privacy, and explainability of AI models.

Finally, while the study suggests AI technologies, particularly GenAI and large language models (LLMs), have yet to enjoy widespread adoption in risk and compliance functions, the potential to enhance capabilities is obviously being recognized. And there is broad agreement on the benefits of using AI for core risk and compliance activity.

As demand for AI-augmented solutions grows, it becomes imperative for providers, like Moody's, to support the transformation and clearly communicate how we can help organize and secure data, ensure accuracy, and deliver the kind of quality solutions needed to serve risk management and compliance leaders. These will be the guiding principles that will help organizations worldwide trust and adopt AI solutions, embedding them into the risk and compliance landscape.

Keith Berry
General Manager,
KYC Solutions at Moody's Analytics

SECTION ONE

About the research

CONTEXT & OBJECTIVES

This changes, everything?
While elements of Artificial Intelligence (AI) such as Machine Learning (ML) and 'big data' analytics have been busily progressing in the background for decades – indeed, the term 'Machine Learning' was coined as far back as 1959 by Arthur Samuel of IBM – 2023 was the year AI went truly mainstream.

The acceleration of Generative AI programs like ChatGPT, Midjourney, and DALL-E, has pushed the topic into the public consciousness, promising to revolutionize the way the world works. From healthcare to legal services and to transportation, AI has been touted as primed to send shockwaves through almost every industry. The fields of risk and compliance are no exception.

This raises key questions. We conducted primary research with a view to finding out more and exploring attitudes towards AI within a range of target audiences and regions, covering the following topics:

- Is AI a passing trend in risk and compliance, or here to stay?
- Where will its impact be felt most across risk management and compliance?
- How do risk and compliance professionals view its potential?
- What are the risks and benefits, barriers and opportunities involved in adopting AI in these fields?
- What effect is AI having on risk management and compliance practices across different industries today?
- What are the regulatory challenges?
- When is AI expected to go mainstream in risk and compliance, if at all?

METHOD

We partnered with an independent research consultancy, Context Consulting, to design and conduct the research. The study included multiple phases to arrive at a balanced and robust set of learnings.

In phase 1, we conducted one-to-one interviews with experts from the worlds of academia, consultancy, and technology to build hypotheses and inform survey development. Phase 2 involved an online survey which was completed by 550 risk and compliance professionals from a range of sectors across 67 countries. And phase 3 saw in-depth follow-up interviews with 10 survey participants in Europe,
the Americas and APAC to discuss findings of the survey and provide additional insight.

SAMPLE

Our research was broad, deep, and global in its scope – including people from a wide range of sectors and roles to get a full picture of how AI is impacting risk and compliance today.

REGION	n=
Europe & Africa	338
Americas	101
APAC	92

SECTOR	n=
Banking	219
Other financial services	131
Asset & Wealth Mgmt.	40
Insurance	48
Fintech	43
Non-financial services	200
Professional services	54
Corporates	114
Government	24

TOTAL	550

SECTION TWO

Background: A double-edged sword

The proliferation of AI technologies into different areas of life represents both a risk and an opportunity for businesses of every size in every sector. On the downside, new technologies, including AI, have the potential to help hide criminal activity, circumvent tried and tested risk infrastructures, and defraud businesses and individuals on an unforeseen scale.

As with any new technology, when it is implemented but not fully understood, AI also offers the possibility of unintended consequences. It can, for example, provide a false sense of security, meaning that companies relying on AI could miss issues that would have been picked up by human operatives. Doing nothing in relation to AI adoption is equally risky – allowing competitors to steal a march in cost savings, efficiency, and overall performance. AI could open competitive threats to incumbent players, as tech-enabled disruptors enter the market, working in faster, smarter, and more engaging ways.

On the positive side, those who adopt the right technologies first can power ahead. In an increasingly fast-paced, complex, and data-driven world, AI allows businesses to do more with less, adapt efficiently to change, and deliver the next generation of services, detection, and protection. These paradigm-shifting benefits enhance the effectiveness of risk management while ensuring compliance.

SECTION THREE

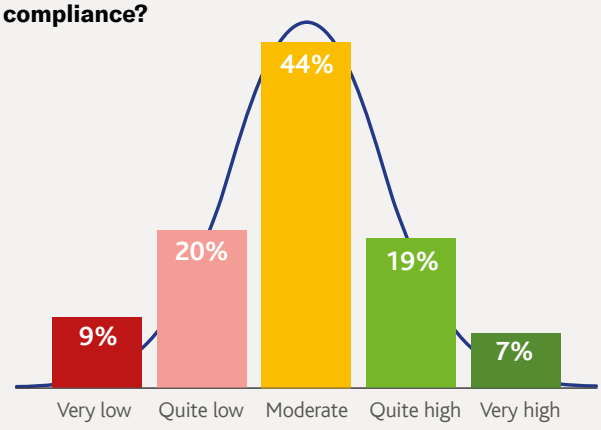
Clarifying the conversation: AI terms in risk and compliance

How well is AI understood within the fields of risk management and compliance? Despite the noise, the picture, for many, remains unclear, with survey respondents reporting relatively low understanding of AI's relevance to risk management and compliance across regions, roles, and sectors.

Just over one quarter (26%) of respondents rate their knowledge as "high" or "very high" – less than the 29% of respondents who define their knowledge of AI as "low" or "very low."

Almost half of respondents claim only moderate knowledge. Subsequent interviews suggest that this describes those with a surface-level awareness of AI and related terminology, but who lack understanding of how it relates to their function and the business case for adoption.

What is your understanding of the relevance and application of AI in risk management and compliance?

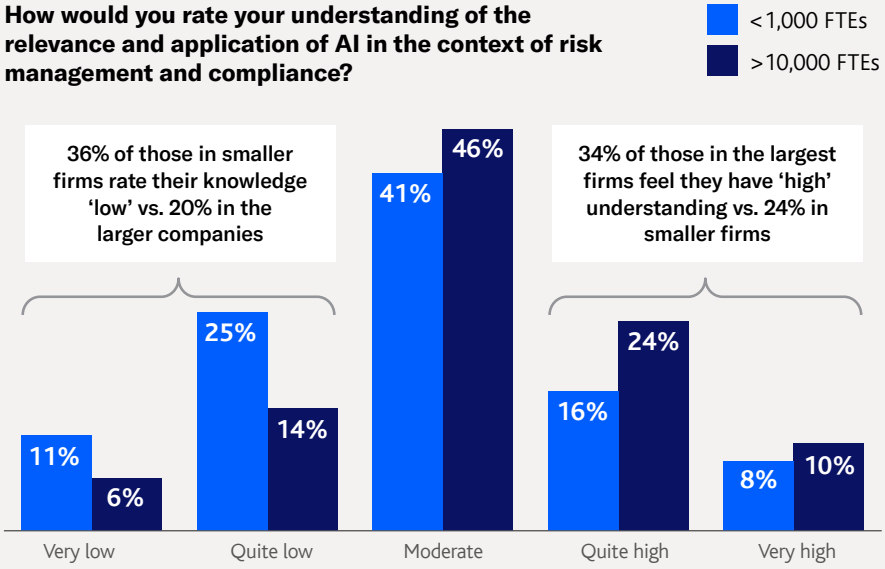


Base: Total (n=550)

SIZE MATTERS

Digging deeper into the detail is revealing. The size of company where a respondent works shows a marked difference in how they rate their understanding of the relevance and application of AI. More people in smaller companies (<1,000 FTEs), rate their knowledge as 'low' than those in larger ones, and conversely, more people in larger firms rate their knowledge higher than those in smaller firms.

How would you rate your understanding of the relevance and application of AI in the context of risk management and compliance?



Base: Total (n=550), <1,000 FTEs (n=212), >10,000 FTEs (n=185)

This can, in part, be explained by the level of AI adoption in these different sizes of firms. While we tend to think of smaller firms as nimble, digital innovators, the relative newness of AI, and the high costs involved, may be prohibitive to them, causing hesitancy when evaluating which AI technologies to adopt.

Larger firms with bigger budgets and headcounts looking for efficiency gains are more inclined to seek out tech-enabled opportunities to reduce costs, and they have the resources to put them into practice.

DECODING THE CONFUSION

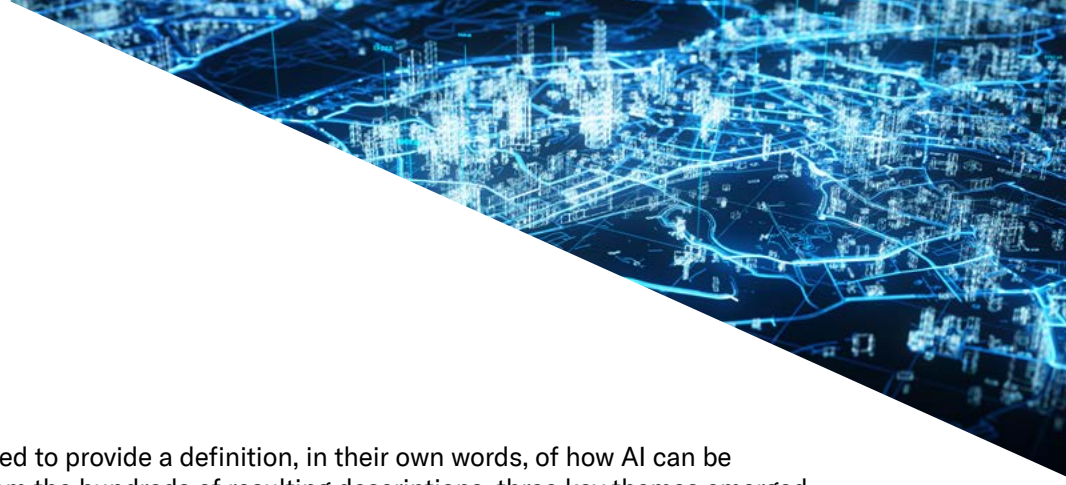
Whatever the size of firm, knowledge of AI's relevance to the risk and compliance function currently remains moderate to low. Part of the confusion centers around the sheer variety of terms used in the field and the fact AI is not one thing.

From AI to ML, NLPs, LLMs and GANs – to name but a few – people can quickly drown in a sea of acronyms. (That's Artificial Intelligence, Machine Learning, Natural Language Processing, Large Language Models and Generative Adversarial Networks, to you and me.)

With so many terms and technologies to get to grips with, it's little wonder the majority of people don't rate their understanding of AI's role in risk and compliance as "high" yet.

Which of the following terminologies do you associate with AI?

Base: Total (n=550)



THREE KEY THEMES

We asked the professionals surveyed to provide a definition, in their own words, of how AI can be applied to risk and compliance. From the hundreds of resulting descriptions, three key themes emerged:

1) Transaction monitoring and detection

The uses in this field are widespread, including:

- Identifying risks through pattern recognition
- Automating AML monitoring and fraud detection
- Identifying money laundering and terrorist financing activities
- Financial crime and sanctions prevention, unauthorized trading detection, and compliance breaches
- Advanced outlier detection when calculating fund product limits or compliance review of policies

> Currently our transaction monitoring system is using AI to do outlier detection for transactions. We are looking to get our own instance of GPT4 to be used for code review and compliance review of policies, guidelines, and procedures.

> AI enables financial institutions to study the behavior of customers to understand their transaction patterns and predict any abnormalities.

2) Customer and entity profiling

Another core pillar of any compliance and risk function is understanding the people and organizations to which you're connected and have potential exposure. There are clear roles for AI to assist in improving profiling capabilities, such as:

- Real-time customer due diligence and compliance gap detection
- More accurately predicting outcomes based on past data
- Analyzing vast datasets from vendors, customers, market trends, and industry regulatory updates
- Streamlining processes, reducing human errors, and minimizing expenses
- Enhancing processes and reducing manual controls
- Analyzing policyholder information, claims histories, and market trends

3) Automation and efficiency improvement

Finally, as in other business areas, one of the core benefits of using AI for risk and compliance is the automation of repetitive tasks to improve efficiency, for instance:

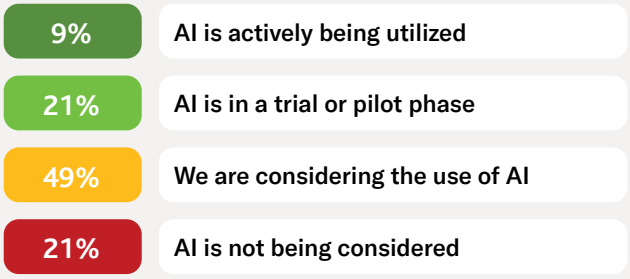
- Providing answers to compliance-related questions and composing communications
- Modeling business situations, and managing regulatory requirements
- Reviewing documents for quality assurance and performing regular maintenance duties
- Employing generative transformers such as ChatGPT and AI-driven code recommendation tools such as Kite or GitHub Copilot

> We don't use AI today, but hopefully it will be able to make our processes more efficient, and we can reduce the number of manual controls.

ADOPTION

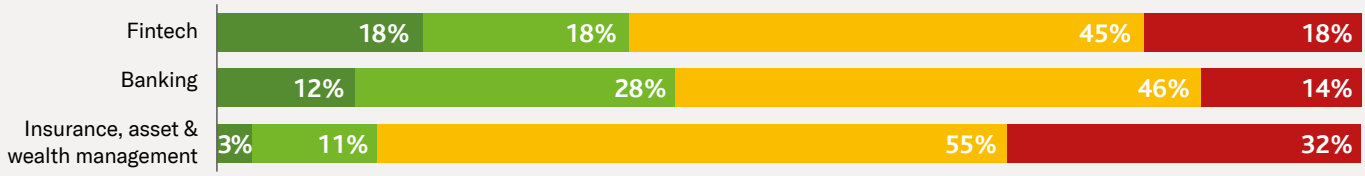
Clearly, it is still early days in AI's diffusion into the world of risk and compliance. To find out just how widespread its use is, we asked participants about their current level of implementation. We discovered that around one in three organizations are actively using or trialing AI in compliance and risk management – with 9% being active users and 21% in the trial or pilot phase. Just under half of firms are considering its use, while 21% are not.

What is the current level of implementation of AI within your company for the purpose of compliance or risk management?



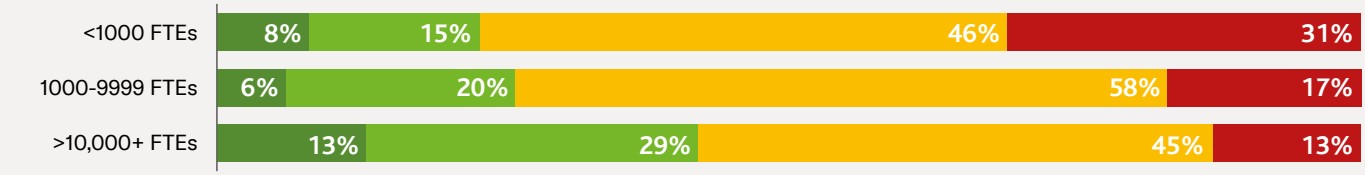
Base: Total (n=550)

The banking and fintech sectors are leading the charge with 40% and 36% respectively using or trialing AI, while insurance, asset and wealth management are playing catch-up.



Larger companies are significantly more likely to be using or trialing AI at 42% vs only 23% of small companies.

This suggests that those with large headcounts and big budgets are using their spending power to drive a shift towards AI, seeking efficiency gains, standardization of performance, and headcount reduction.



Base: Total (n=550), Fintech (n=35), Banking (n=209), Insurance, Asset & W. Mgt. (n=87), Less than 1000 FTEs (n=192), 1000-9999 FTEs (n=125), 10,000 FTEs (n=164)

THE DEVIL IS IN THE DATA

It is widely recognized that one of the preconditions of a firm's ability to adopt AI is the quality, consistency and organization of its internal data. It is incredibly hard to implement AI effectively with poor quality, disorganized data.

Everyone is at a different stage in their AI journey. Understanding data maturity and rectifying gaps is key to a firm's readiness to adopt AI it seems. So, we asked participants to identify the maturity level of their internal data across a five-point scale:

Superior	High quality	Clean	Inconsistent	Fragmented
Superior data infrastructure with real-time refinement. Seamlessly integrates into decision-making. Unparalleled breadth and depth.	Clean, structured data. Occasional quality checks in place. Moderate breadth and depth.	Clean, structured data. Occasional quality checks in place. Moderate breadth and depth.	Data is structured but contains inconsistencies. Manual cleansing often necessary. Limited breadth and depth.	Fragmented and unstructured data. Significant cleansing required for meaningful use.
2%	12%	19%	44%	23%

2 out of 3 respondents believe their organization has low data quality

The fact that two thirds of respondents rate their firm's data quality in the two lowest categories helps explain why the majority are yet to start using AI for risk and compliance.

Base: Total (n=550)

CHICKEN OR EGG?

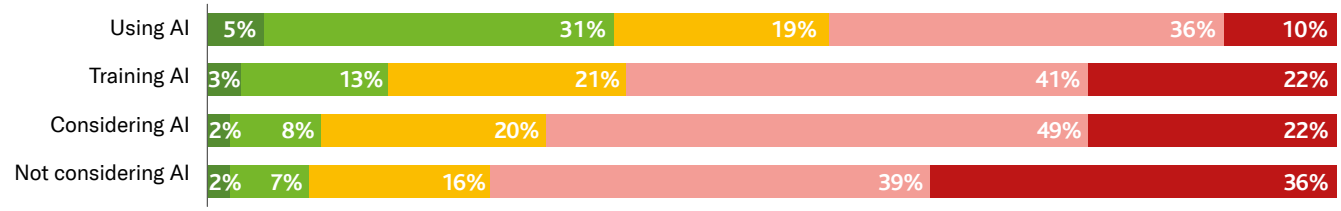
The question then becomes, are early adopters of AI able to do so because they have better internal data, or are they using AI for the purpose of improving their data?

It is clear a data-maturity gap exists between those companies already using AI and the rest of the field.

36% of those already using AI rate their internal data as high-quality or superior, compared with only 9% of those not considering AI.

At the other end of the scale, 75% of those not considering AI think their data is inconsistent or fragmented, compared with a still far-from-perfect 46% of existing users.

Which of the following statements best describes your organization's data maturity in the context of compliance?



Base: Total (n=550), Using AI (n=42), Trialing AI (n=95), Considering AI (n=225), Not Considering AI (n=83)

With 55% of those using AI rating their data as "clean" or better, there appears to be a powerful link between high-quality internal data and early adoption of AI.

SECTION FOUR

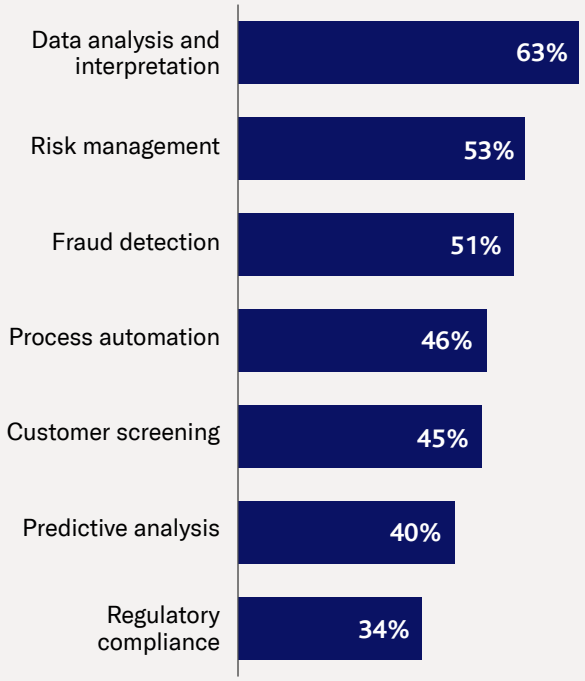
Voices from the vanguard: insights from early AI adopters

PUTTING AI TO WORK

Understanding where AI is being implemented today is key to seeing how it will impact risk and compliance tomorrow.

Unsurprisingly, as teams are forced to deal with ever-increasing levels of information, 63% of companies actively using or in a trial phase with AI are using it for data analysis and interpretation.

Areas in which AI is being used (existing users / trialists only)



Base: Using/ Trialing AI (n=144)

Risk management and fraud protection, particularly in banking, come next on the list. Other priorities like automation, screening, and regulatory compliance are being applied and will likely grow as more AI technologies become commonplace.

The different AI models an organization uses provide insights into a range of areas like the level of its data maturity, the specialized nature of tools it has developed, and the specific intelligence it requires.

We wanted to understand which of the following types of AI models were being used:

Statistical or stochastic models are primarily based on statistical methods and often used for forecasting, pattern recognition, or anomaly

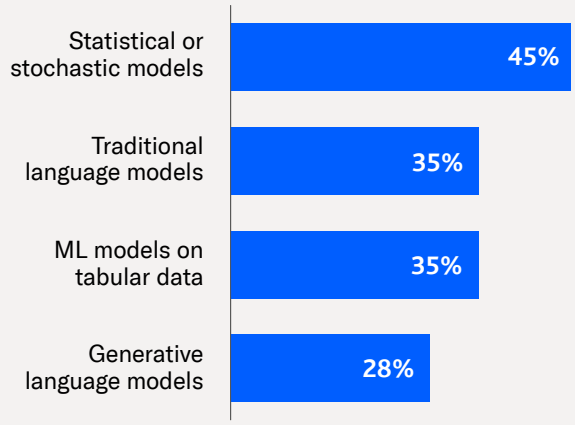
Traditional language models are designed for tasks like text classification, sentiment analysis, and named entity recognition.

ML models on tabular data are designed for structured data, such as those used in finance, healthcare, and retail for tasks like prediction and clustering.

Generative language models generate coherent and contextually relevant text over extended passages.

Our research identified that, on average, those using or trialing AI were using an average of 1.8 different models, reinforcing the idea that AI is a multi-faceted technology.

AI model types being used / trialed:



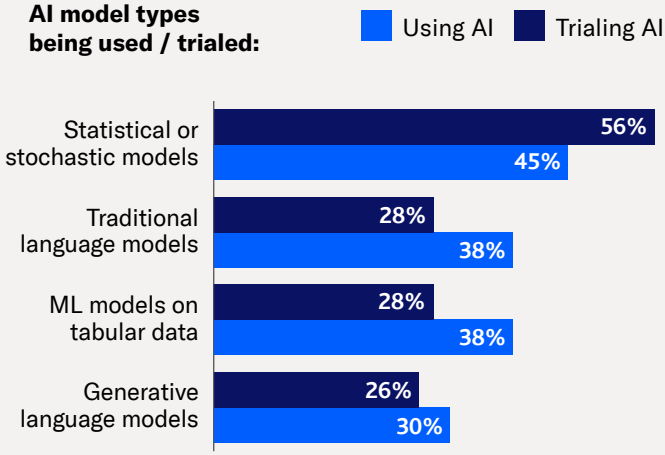
Base: Using/ Trialing AI (n=144)

The prominence of statistical or stochastic models reflects both the breadth of demand for pattern recognition and anomaly detection, as well as the fact such models are more established forms of AI.

However, when comparing current users of AI with those trialing AI, we see the latter are more likely to be trying out traditional language models, ML models, and generative language models.

This is most likely due to the recent advancements in LLMs, like ChatGPT, which have shifted awareness and become more accessible, versus the complexity and more specialized nature of stochastic models, which were a feature of early-mover investment.

AI model types being used / trialed:



Base: Using/ Trialing AI (n=144)

CHARTING INTENT VS. OUTCOME

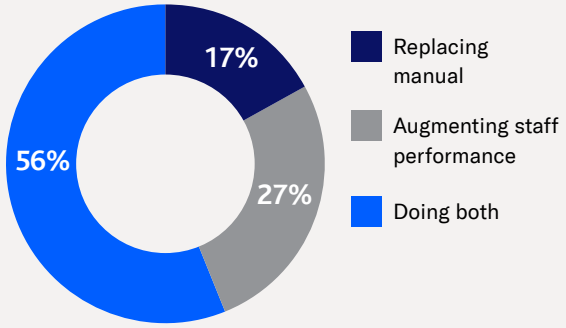
Meeting desired outcomes and successful implementation of AI today will shape the role it can play in risk and compliance in years to come.

When implementing AI, what is the primary intent for organizations? What has the impact of AI been to date? We posed these questions to early adopters to understand what their initial aims were and whether they were currently being met.

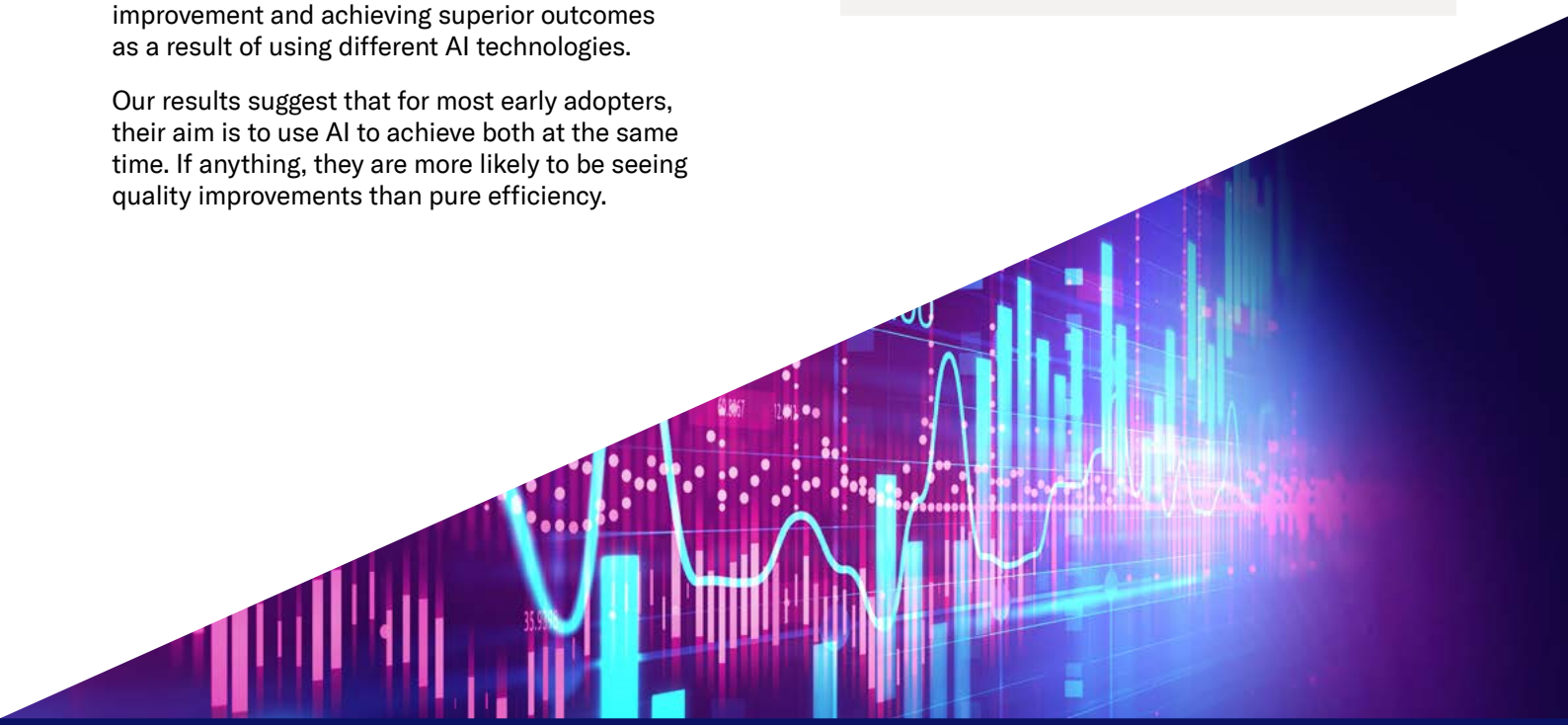
Replacing manual processes can be considered akin to seeking efficiency, i.e. doing the same tasks more quickly and at lower cost, and potentially using fewer staff. By contrast, augmenting staff performance speaks to a desire for qualitative improvement and achieving superior outcomes as a result of using different AI technologies.

Our results suggest that for most early adopters, their aim is to use AI to achieve both at the same time. If anything, they are more likely to be seeing quality improvements than pure efficiency.

What has been your primary intent in implementing AI?



Base: Using AI (n=43)



MOODY'S

When it comes to the impact of AI, early adopters are highly positive. 91% of respondents feel AI has had significant or moderate impact on risk and compliance, compared with 9% who claim it has had minimal or no impact.

What has been AI's impact to date?

32%	**Significant impact** Major improvements in efficiency or outcomes
59%	**Moderate impact** Noticeable improvements in some areas
7%	**Minimal impact** Slight improvements but less than expected
2%	**No impact** No significant change in efficiency or outcomes

Base: Using AI (n=43)

Drilling deeper, the early adopters of AI identify benefits across five key areas:

1) **Efficiency gains**
   Automation of repetitive tasks like anti-money laundering (AML) reduces workloads, allowing them to focus on what's important.

2) **Enhanced risk identification**
   Improved transaction AML reporting and monitoring. More timely identification of risks informing better decisions.

3) **Tighter fraud detection**
   Reducing fraud, including impersonation fraud, and enhancing threat detection in cybersecurity.

4) **Cost saving and error reduction**
   Minimizing errors and irregularities to reduce full time employees (FTEs) and infrastructure upkeep.

5) **Data processing and quality gains**
   Improving how data is collected, organized and analyzed, allowing for deep and extensive insights.

> "With a small compliance team, we are leveraging AI to operate best-in-class transaction reporting monitoring for money laundering, market abuse, and best execution."

SECTION FIVE

The balancing act: how risk and compliance professionals view AI

Looking beyond early adopters to the wider audience, we see a story of cautious optimism. A balancing act.

Minds are still being made up around the best policies to adopt on AI tools such as LLMs. But, while most firms are yet to implement the technology, there is broad agreement AI will deliver advantages for risk and compliance teams in the long run.

When it comes specifically to LLMs like ChatGPT, only around 1 in 4 firms (28%) take a positive stance, and 25% are "actively discouraging" or "prohibiting" its use. However, the fact the largest group (46%) has yet to adopt a policy speaks to the relative newness of the technology.

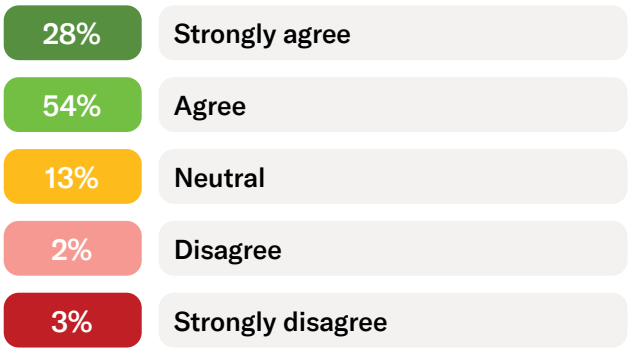
Digging into the detail, fintechs, perhaps expectedly, are the most open to LLMs with 54% taking a positive stance. This contrasts with banks, potentially more mindful of reputational risk and data privacy, with 25% taking a negative stance.

Here again we identified a difference by company size. Whereas 70% of firms with more than 10,000 FTEs have devised a policy, only 43% of firms with fewer than 1,000 FTEs have done so. The policies devised by large firms are as likely to impose a negative stance as a positive one, 35% in both cases.

There is clear interest among firms of all sizes in developing "co-pilot" LLMs trained specifically on their proprietary data, and as such avoiding data privacy and security pitfalls.

Despite cautiousness and reticence, the overall outlook for AI in the broader spectrum is optimistic. 82% of respondents either agreed or strongly agreed that AI will deliver significant advantages within the risk and compliance function. Only 5% demurred.

Overall, do you agree there are significant advantages of using AI within risk and compliance functions?



Base: Total (n=550)

This sentiment is consistent across all types of organizations, both financial and non-financial, and in those who were using AI and those who weren't considering it at all.

EXTRA CREDIT

Awareness of the benefits of AI are well recognized across both those considering and those not considering its use.

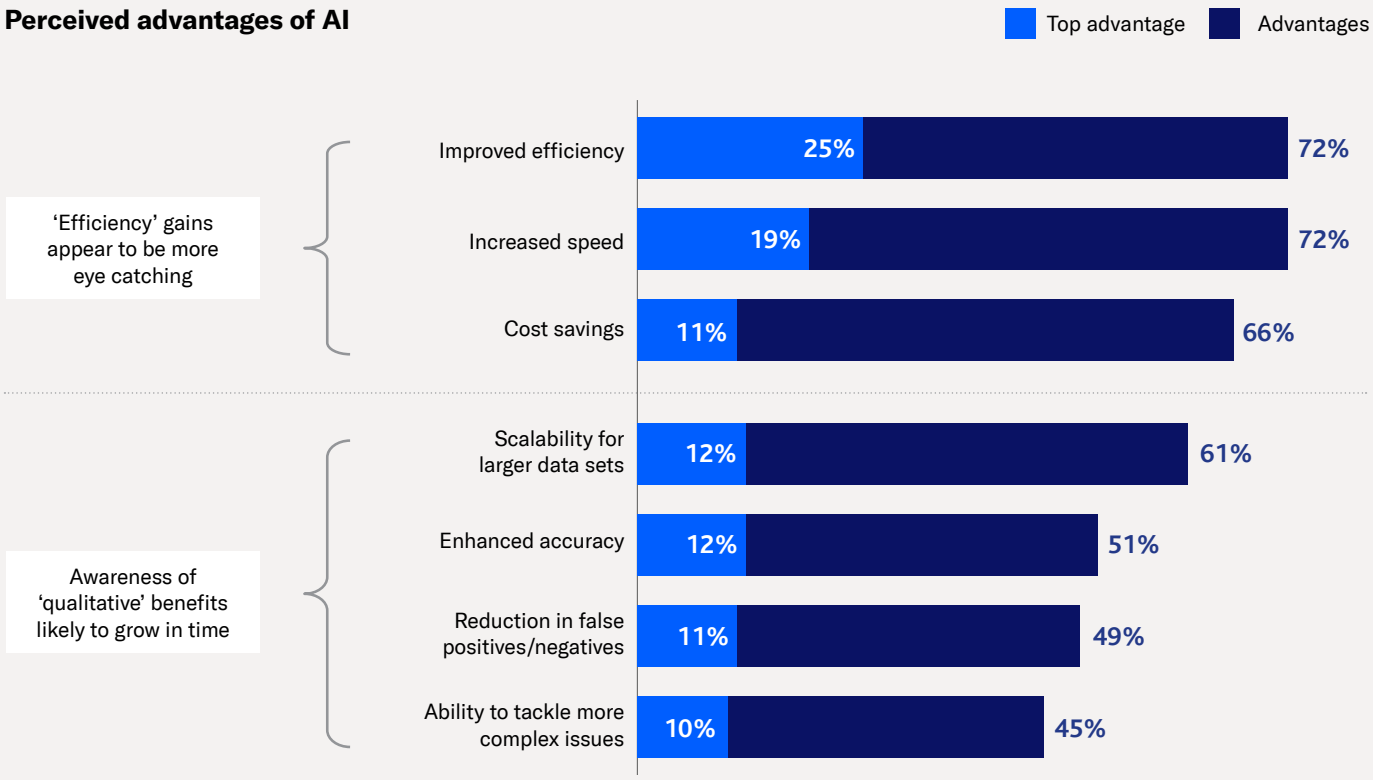
We therefore asked respondents to identify the key benefits of AI in risk and compliance in their view, and to specify one single key benefit.

Among the benefits listed, efficiency and speed were most cited, in both cases by 72% of respondents.

When asked to home in on one main benefit of AI, 25% chose efficiency while 19% opted for speed.

More "qualitative" benefits, like the reduction of false positives or enhanced accuracy, are less widely perceived at present, though these are likely to grow as awareness of AI's potential improves and technologies become more embedded in risk and compliance processes.

Perceived advantages of AI



Base: Total (n=550)

RIGHT PLACE, RIGHT TIME

AI appears to be well placed to address the growing challenges faced by many risk and compliance teams.

In a world where efficiency is paramount and teams are being continually streamlined, many feel they are creaking under the weight of exponentially growing datasets and ever-evolving regulatory requirements.

AI presents the opportunity to solve the conundrum of being asked to do more with less.

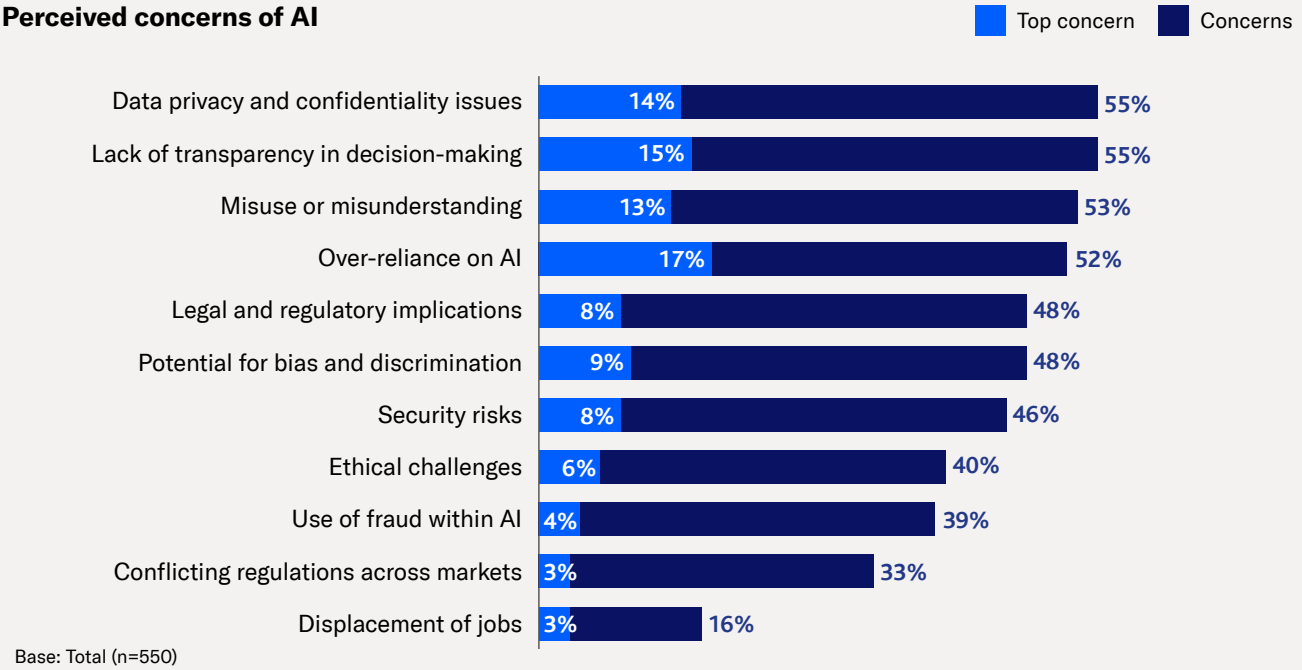
> I think at the moment we spend too much time on repetitive, non-complex issues that could be outsourced to an AI tool.

> As a relatively small financial institution, compared to the big banks, we are usually behind in innovation and automation. AI is a chance to close that gap to some extent, leading to more "best-in-class" processes, especially in terms of speed.

RAISING CONCERNS

If the benefits of AI are widely understood, so too are its risks. We asked respondents which concerns they had over the use of AI in risk and compliance, and to state which one they considered the biggest concern.

Perceived concerns of AI



Base: Total (n=550)

Data privacy fears and the lack of transparency in AI-driven decision-making are the most frequently stated concerns, being cited by 55% of respondents.

> Industrial espionage risk is high and it's difficult to know how AI could expose the company

> The black box nature of the decision making is very unsettling as it will not lead to consistent nor explainable outcomes.

At the other end of the scale, people are less worried about AI displacing jobs or navigating different regulatory environments.

The next most common concern is the misuse or misunderstanding of AI, cited by 53% of respondents overall.

> AI is only as good as the person building it and employing it.
> It will not serve as a replacement for individuals that are weak or uninformed regarding AML, compliance or fraud issues.

MOODY'S

Over-reliance on AI ranks fourth overall, being named by 52% of respondents. However, this is the factor most likely to be named as the single main worry, for 17% of respondents, meaning its significance should not be underestimated.

This reflects two separate but connected concerns. On one hand lies a fear that companies will entrust so much decision making to AI that human judgement no longer reigns supreme. On the other, there is a sense that AI's role could make it difficult for the
next generation of professionals to develop the intuition and nuanced reasoning needed to make difficult calls in the future.

The telling nature of these concerns is that they are not just the voice of those reluctant or unwilling to take up AI. In many cases they are live concerns for people using or trialing AI technologies.

Clearly additional reassurance is needed to ensure risk and compliance professionals as a whole can have faith in processes and decisions powered by AI.

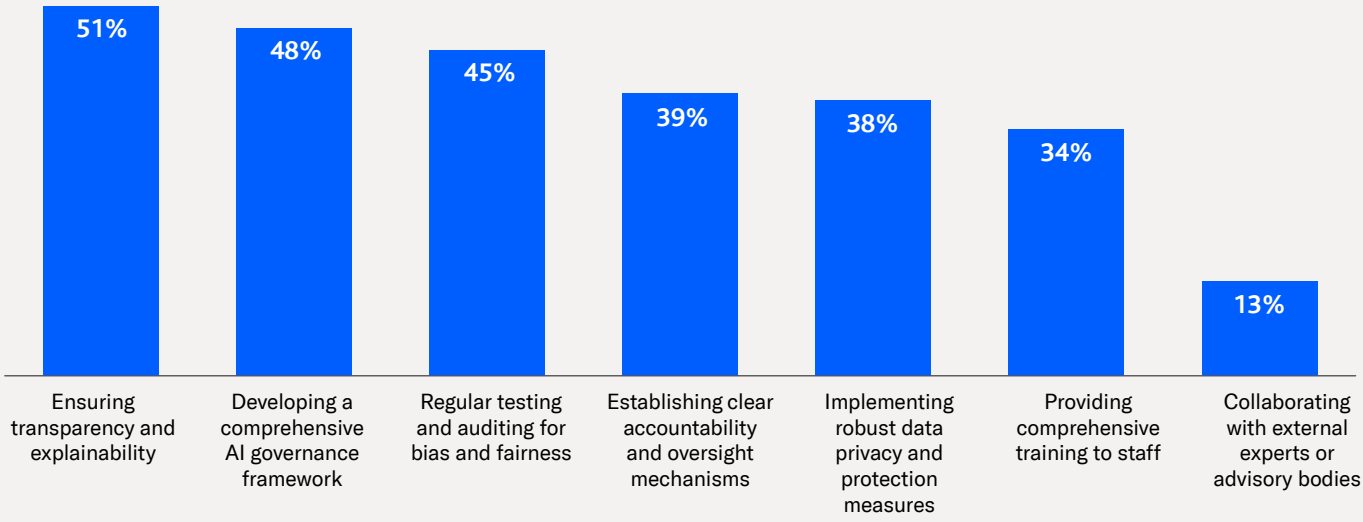
> Relying too much on AI could lead to a decrease in awareness that the final decision should always be taken by a human being. AI should only be a tool, not a decision-maker.

LET'S BE CLEAR

So, what can be done to allay existing fears? What safeguards can be put in place to ensure the reasonable and responsible introduction of AI technologies within risk management and compliance operations?

Most cited, 51%, was ensuring transparency in AI decision making. Developing a comprehensive AI governance framework and regular AI testing were also seen as key to providing confidence in new technologies at 48% and 45% respectively.

Which safeguards are required around AI in risk and compliance?



Base: Total (n=550)

SECTION SIX

Walking the tightrope: regulatory perceptions

While AI continues its march into the world of risk and compliance, what regulation has been developed or is needed to support safe entry? And how aware were our survey participants of the evolving regulatory conditions related to AI in their sector?

Only 15% of respondents claimed to be well aware or fully aware of current regulations, and one third admitted to not knowing anything.

How aware are you of the current AI-related regulations in your sector?

5%	I am fully aware
10%	I am well aware with some gaps
21%	I am somewhat familiar
34%	I know a little
32%	I don't know anything

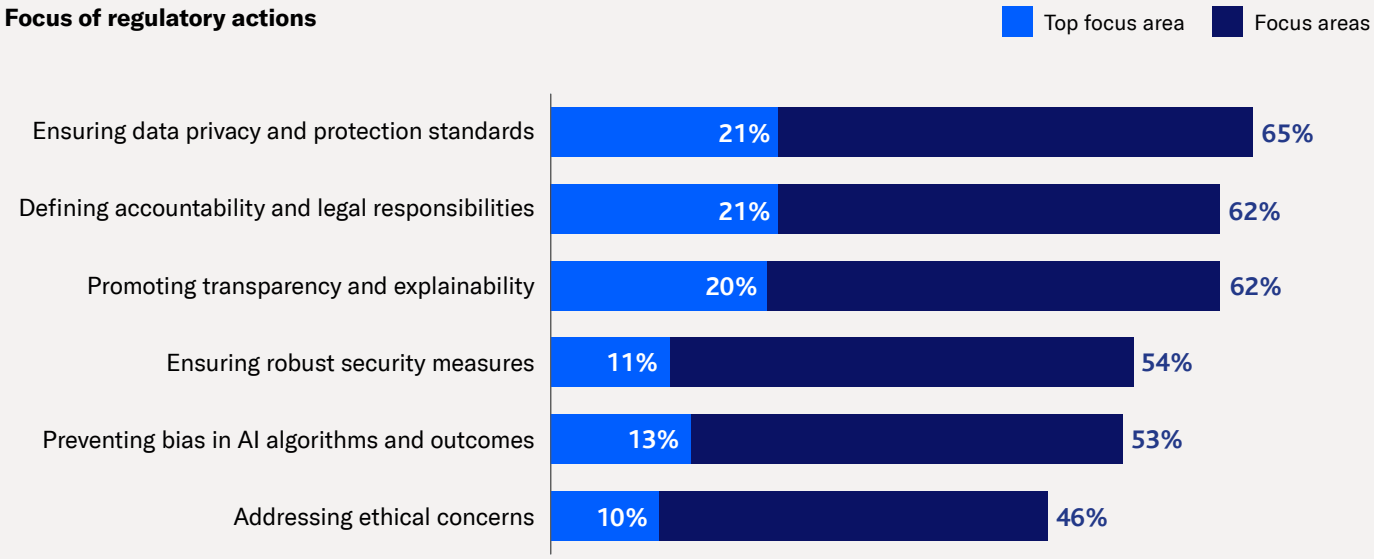
Base: Total (n=550)

Even when looking at different segments, regulatory awareness needs work. Among early adopters and those trialing AI, only a quarter of respondents claim to have good awareness of regulation.

These findings contrast with the perceived importance of regulations in this space. With 79% of respondents agreeing regulation of AI is important, there is clearly a desire for authorities to act. This view is reflected across all sectors and almost as much by those not using AI (75%) as those already using it (83%).

The concerns most survey participants shared in the previous section mirror the priorities people believed regulators should address first.

Focus of regulatory actions



Base: Total (n=550)

MOODY'S

CREATING A FRAMEWORK FOR SUCCESS

Professionals clearly want regulators to implement globally consistent, forward-looking rules, that enshrine human accountability in the use of AI. Some of the topics that consistently came up include:

Standardization and global collaboration to create a consistent and standardized regulatory framework, avoiding piecemeal country- or state-level versions.

Transparency, accountability, and human oversight to ensure decision-making is clear. Individuals should be held accountable for outcomes. And there should be involvement of humans in AI-driven decisions at all times.

Ethical deployment and data privacy are paramount, especially regarding potential bias in AI. Regulations should protect data privacy, given AI's use of vast datasets.

Regulators need to grow understanding through education, with precise terminology and by educating the public to foster trust and address skepticism around AI.

Legislation needs to be flexible and adaptable, recognizing the rapid advancement of AI. While there's a need for rules, a principle-based approach might serve better than being overly prescriptive as AI matures.

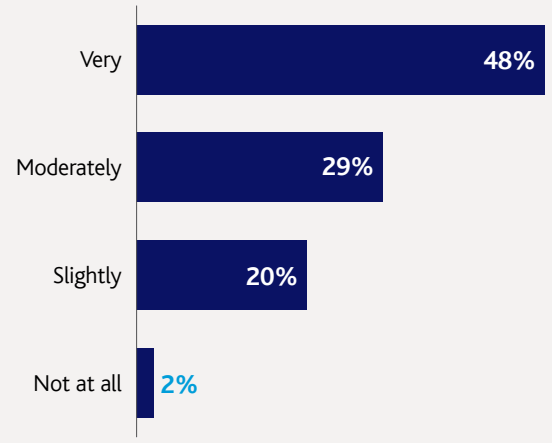
SECTION SEVEN

In the spotlight: the solution vendors shaping the AI landscape

If the rapid development of AI is putting pressure on regulators, our survey found that another group facing growing expectations is solution vendors.

When asked about their interest in vendors introducing AI tools into their risk and compliance offerings, the results were unequivocal. 97% of respondents are interested to some degree – 48% being very interested – with a high degree of consensus across industries, regions, and risk and

How interested are you in vendors introducing AI tools into risk and compliance offerings?



Base: Total (n=550)

However, vendors will need to reassure customers by demonstrating any AI-powered tools meet high standards and can be relied on in the high-stakes realms of risk and compliance.

Specifically, our study found that technology partners must prioritize demonstrating how their offerings address key areas including:

Transparency

Understanding how AI-driven outcomes are achieved and providing insights into the decision-making processes of AI systems. Stakeholders need to understand their partners can explain how systems work with confidence and clarity. Transparency helps prevent "black-box" scenarios where users question the reasoning behind decisions.

Accuracy and reliability

AI models will need to deliver consistent results with high accuracy, robustness, and reliability. Mistakes or inconsistencies have significant repercussions, particularly in the field of risk management and compliance, ranging from financial penalties to reputational damage.

Bias control and ethical use

Overcoming inherent bias in AI models was cited by many respondents, highlighting a need for technology partners to prioritize bias audits, address disparities, and ensure the ethical use of AI.

Data security and protection

It's paramount that AI solutions guarantee the protection of sensitive data and information associated with risk and compliance. Many express concerns about ensuring confidentiality and security of company, customer, and staff data, especially in external platforms.

Efficiency and optimization

Cost and speed are important, but these shouldn't be achieved at the expense of accuracy or transparency.

IN-HOUSE OR OUTSOURCE?

We next asked respondents whether they lean towards building AI solutions in-house or purchasing pre-built tools.

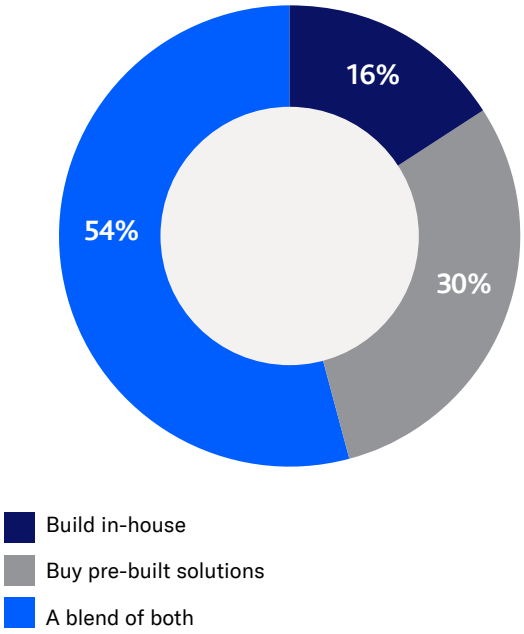
Overall, a blended approach was most preferred (54%), with 30% buying pre-built solutions and only 16% building in-house.

However, digging into the results provides additional insight. Pre-built solutions are most favored by smaller firms with fewer than 1,000 FTEs, not least because these companies are less likely to have the technical skills needed.

By contrast, those who adopted AI early are more likely to prefer systems built in-house, while later adopters are often using pre-built and off-the-shelf solutions.

These findings hint at the changing face of AI – that more bespoke and specialized AI solutions, like statistical and stochastic models, were developed by first movers in-house, whereas evolving technologies like LLMs are becoming increasingly widespread, democratized, and outsourced. There's clearly an increasing role for third-party partners to create AI-led solutions for risk and compliance functions if they get the

Do you lean towards building in-house or buying pre-built AI solutions?



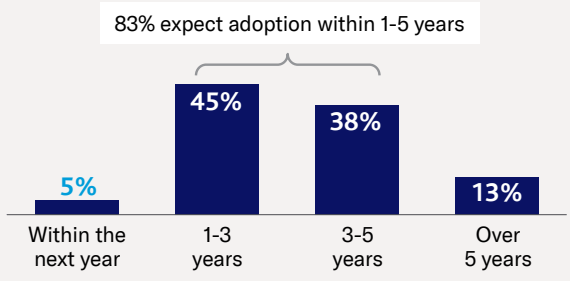
Base: Total (n=550)

SECTION EIGHT

Looking ahead: predictions and projections from the frontlines

While AI is deepening its reach into everyday risk and compliance tasks, the transition won't happen overnight. Very few predict widespread adoption of AI in risk and compliance within the next 12 months. Most people we spoke to – 83% – see a more realistic timeline being over the next 1-5 years.

Expected timeline for the widespread adoption of AI usage within the risk and compliance field?

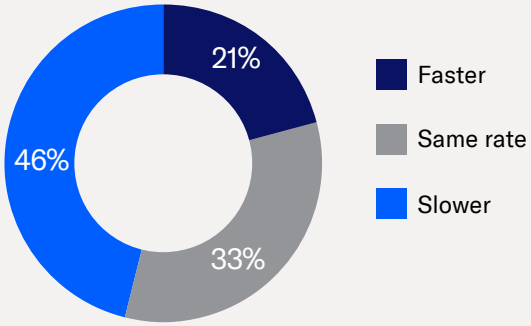


Base: Total (n=550)

So, did risk and compliance professionals expect AI to be adopted at a different rate within their function as compared to other business functions?

In fact, nearly half of respondents anticipate a slower adoption in risk and compliance than other business areas, with a much smaller proportion expecting the reverse. What lies behind this expectation?

Do you expect AI adoption in risk management and compliance to occur faster or slower than other business functions?



Base: Total (n=550)

PERCEPTION OR REALITY?

Our respondents highlighted a mix of practical, cultural, and regulatory challenges that are expected to slow adoption of AI technologies in risk and compliance compared to other areas.

- Budget allocation tends to go to revenue-generating units first, with risk and compliance functions viewed as cost-centers
- Compliance and risk management are also heavily regulated areas so the speed of regulation could dictate the pace of uptake
- The complexity and requirement for nuance in many risk and compliance decisions makes it less open to the use of AI, as a high level of human judgement is often required
- Risk and compliance people, by their nature, are generally more risk-averse, which may mean they are slower to change, and more resistant to adopting new technologies than other business areas
- Technical and practical issues feature too, with some feeling current AI systems won't understand the intricacies of interpreting and analyzing risk and compliance data, particularly when the stakes are high

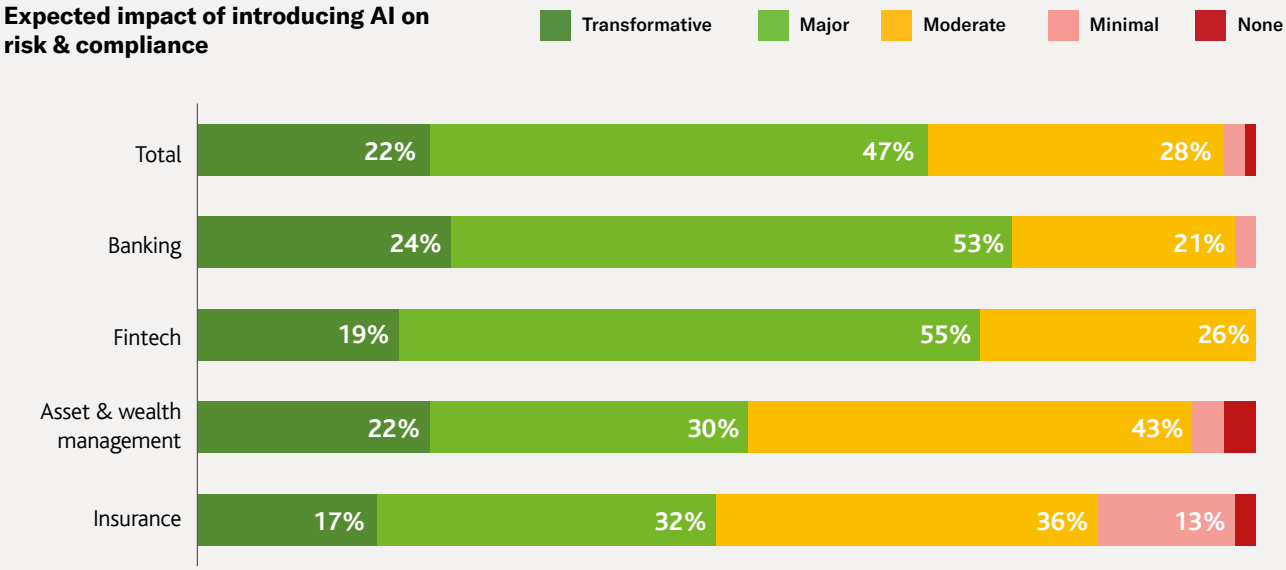
> Leaders do not see compliance and risk as a contributor to profit and performance. They will likely prefer to invest in functions that are seen to enhance competitive edge and growth.

> Risk management is about judgement, which AI is not particularly good at.

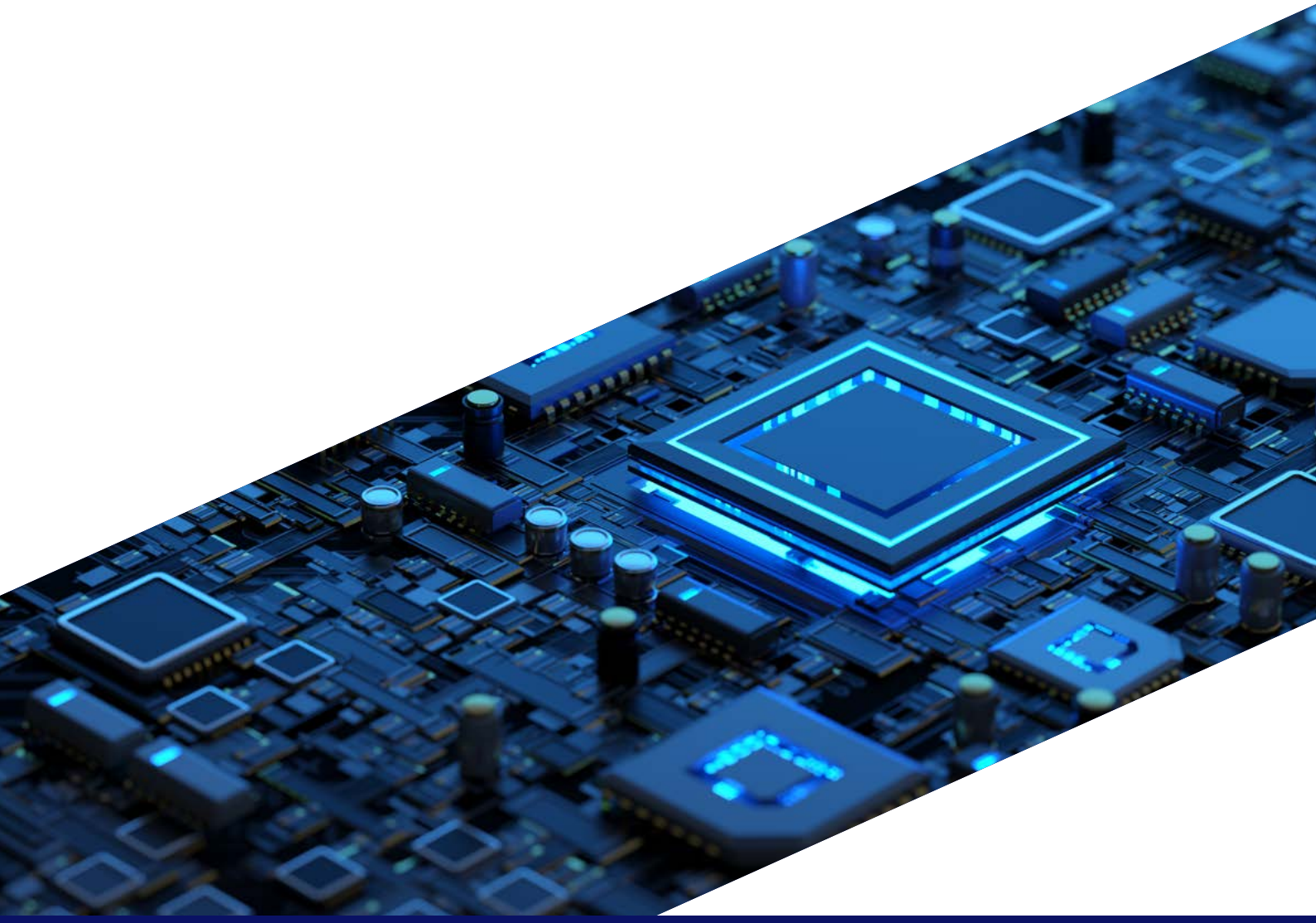
> Risk and compliance are inherently change adverse and will need to consider privacy and other considerations.

But despite reservations, almost 70% of firms expect AI will exert a transformative or major impact on risk and compliance in future, which rises to 77% in banking and 74% in fintech.

Expected impact of introducing AI on risk & compliance



Base: Total (n=550), Banking (n=219), Fintech (n=43), Asset & WM (n=40), Insurance (n=48)



SECTION NINE

Wrapping things up: six key takeaways

While it is still early days for the impact of AI technology to be felt across risk and compliance, one thing is certain: change is coming. In what shape and what ways remains to be seen, but those who are most alive to the risks and opportunities now will be those most able to adapt, avoid pitfalls, and take advantage of the benefits it promises.

These six takeaways should help anyone working in risk and compliance get a better understanding of the AI landscape today, and how it could change tomorrow:

1. 9 in 10 early adopters of AI report that it is having a positive impact on risk and compliance, delivering an impressive range of benefits

2. Outside of the early adopters, most firms have yet to embrace use of LLMs, but there is broad agreement: AI technologies, including GenAI, will deliver advantages for risk and compliance

3. With two thirds of respondents describing their data as fragmented or containing inconsistencies, the poor quality of internal data could be a barrier to AI implementation if firms can't get a firmer handle on it

4. There is a stark gap between the lack of awareness of AI-related regulation and the common agreement that new legislation is needed; therefore, those in the industry need to engage in dialogue with regulators

5. As the clamor for AI-augmented solutions grows, vendors need to communicate how they ensure data security, explainability, and quality of outputs

6. Widespread adoption of AI is predicted in the medium term, though perhaps less quickly than in other business areas, so risk and compliance leaders who perceive there to be speed and efficiency gains to be had from use of AI need to build their business case based on evidence from early adopters

Whether you are in the vanguard of change or reluctant to adopt AI, it pays to understand what is happening in the field. It will undoubtedly be a key driver of progress and could influence competitive advantage. It does create entirely new opportunities and challenges for risk and compliance professionals – whether leading change or resisting it – for the foreseeable future, so developing understanding, continuing to participate in the conversation, and beginning to navigate the AI landscape are essential.

GET IN TOUCH

Contact information

To find out how Moody's can help you unlock the potential of AI in your world of compliance and risk management, please visit moodys.com/kyc/ai-study or get in touch.

AMERICAS
+1.212.553.1653
clientservices@moodys.com

EUROPE
+44.20.7772.5454
clientservices.emea@moodys.com

ASIA (EXCLUDING JAPAN)
+852.3551.3077
clientservices.asia@moodys.com

JAPAN
+81.3.5408.4100
clientservices.japan@moodys.com

MOODY'S