Thought Leadership

Research partner

IBM

AI in RegTech: a quiet upheaval

How advanced technologies are changing the way that financial risk, financial crime risk and GRC are managed

Chartis

Independent. Insightful. Actionable.

About Chartis

Chartis Research is the leading provider of research and analysis on the global market for risk technology. It is part of Infopro Digital, which owns market-leading brands such as Risk and WatersTechnology. Chartis' goal is to support enterprises as they drive business performance through improved risk management, corporate governance and compliance, and to help clients make informed technology and business decisions by providing in-depth analysis and actionable advice on virtually all aspects of risk technology. Areas of expertise include:

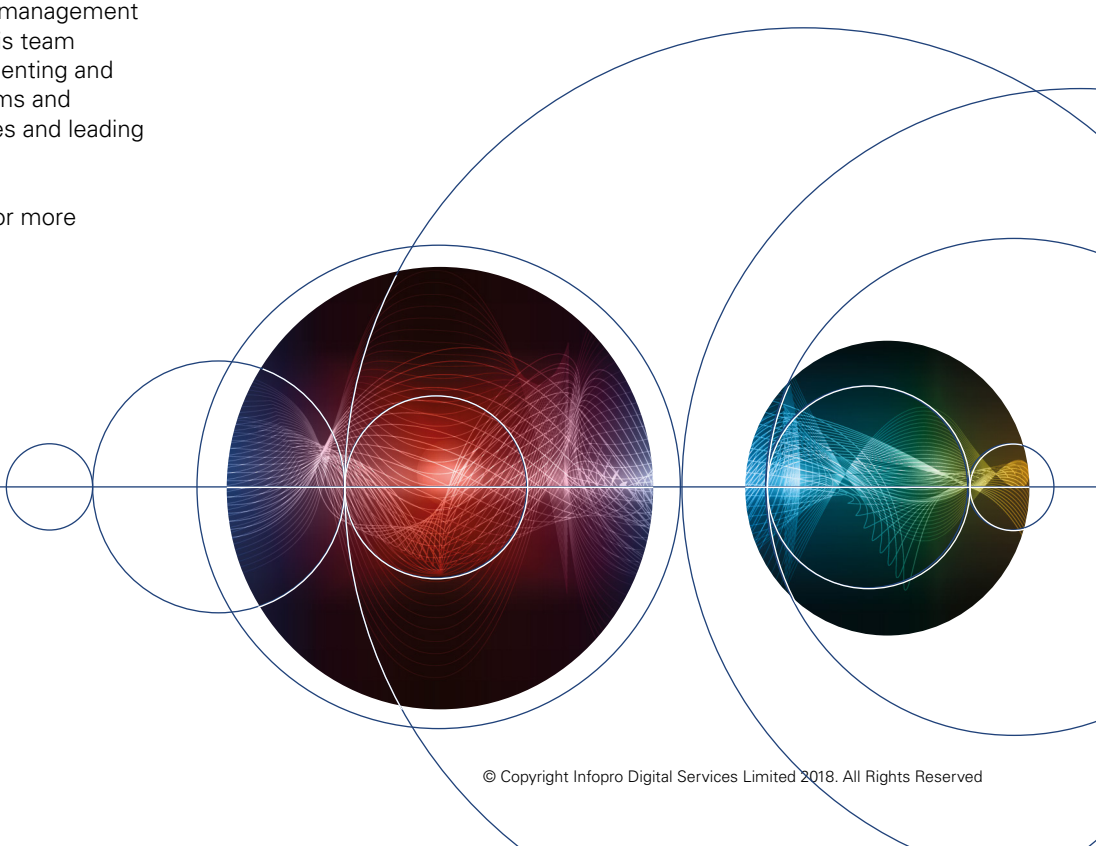
- Credit risk.
- Operational risk and governance, risk and compliance (GRC).
- Market risk.
- Asset and liability management (ALM) and liquidity risk.
- Energy and commodity trading risk.
- Financial crime including trader surveillance, anti-fraud and anti-money laundering.
- Cyber risk management.
- Insurance risk.
- Regulatory requirements including Basel 2 and 3, Dodd-Frank, MiFID II and Solvency II.

Chartis is solely focused on risk and compliance technology, which gives it a significant advantage over generic market analysts.

The firm has brought together a leading team of analysts and advisors from the risk management and financial services industries. This team has hands-on experience of implementing and developing risk management systems and programs for Fortune 500 companies and leading consulting houses.

Visit **www.chartis-research.com** for more information.

Join our global online community at **www.risktech-forum.com**.



About our research partner

IBM is working with organizations across the financial services industry to use IBM Cloud, cognitive, big data, RegTech and blockchain technology to address their business challenges. Watson Financial Services merges the cognitive capabilities of Watson and the expertise of Promontory Financial Group to help risk and compliance professionals make better informed decisions to manage risk and compliance processes. These processes range from regulatory change management to specific compliance processes, such as anti-money laundering, know your customer, conduct surveillance and stress testing.

To learn more about IBM risk and regulatory compliance solutions, visit **ibm.biz/RiskAndCompliance** and follow us on Twitter **@IBMFintech**

Table of contents

List of figures and tables

1. Executive summary

Research by Chartis and IBM highlights new emerging themes in how Artificial Intelligence (AI) is used in regulatory technology to help financial institutions address risk management and regulatory compliance. In the specific areas of Financial Risk, Financial Crime Risk Management and Governance, Risk management and Compliance (GRC), most risk professionals are adopting specific tools and statistical techniques to streamline and upgrade their processes, augmenting human capabilities through better visualizations, better analysis and better methods. In some areas – notably financial risk and GRC – AI could have a transformative impact, but only if users properly familiarize themselves with how it works. Based on our conclusions, risk professionals across the RegTech landscape can now clearly assess the promise of AI, gain a true picture of where it is within their organizations, and assess where they themselves sit in its broader evolution.

Artificial Intelligence (AI) technologies – or, more accurately, the array of specific statistical and quantitative tools of which AI is just one – are everywhere in the finance industry. In particular, statistical tools are making their presence felt in vendors' Regulatory Technology (RegTech) offerings, as Financial Institutions (FIs) develop ever more complex systems and processes to address their evolving risk and compliance requirements.

In April 2018, Chartis and IBM published *Demystifying Artificial Intelligence in Risk and Compliance: A Step-by-Step Guide*. This collaborative piece of research aimed to dig beneath the hype surrounding AI tools to a deeper understanding of the statistical roots of these technologies, examining how AI techniques can effectively be applied to the areas of risk and compliance.

Since that report we have been considering more detailed questions: as RegTech tools and techniques become more prevalent in the landscape, how are FIs adopting and using AI tools and techniques in their *specific* risk and compliance operations? Are there any differences in the way that professionals from different areas of risk and compliance view AI and what it can do for them?

To examine these questions, we carried out surveys and interviews with more than 100 relevant risk and technology professionals, including CROs, CTOs, CIOs and CCOs, in three key areas of risk and compliance where evolving RegTech technologies are making an impact: Financial Risk – which includes market, credit and balance sheet risk – Financial Crime Risk Management (FCRM) and Governance, Risk management and Compliance (GRC).

The results were illuminating, providing a more nuanced view of AI use in the RegTech sphere. As our research shows, risk professionals are making extensive use of AI in their risk and compliance operations – just not in the way we might expect.

Research highlights

Some of our key findings, analyses and conclusions include:

- **There is fairly even use of AI in RegTech solutions, across Financial Risk, FCRM and GRC**, and most institutions are cautious but strong adopters. About 70% of respondents in each area were using AI in risk and compliance. Only 4% were from institutions with reservations about AI. The most heavily used techniques are Machine Learning (ML) and Natural Language Processing (NLP); for 11% of institutions NLP has become a core component in many applications.

- **Efficiency and accuracy are the driving forces behind most implementations**. Alongside compliance requirements (64%), the main reasons to implement AI in RegTech solutions were cost reduction (56%) and greater accuracy of process and analysis (44%). For most FIs, AI is about achieving better visualization, analysis and methods to generate ideas, automation and efficiency.

- **A lack of skills and data is a persistent challenge**. This was cited as a significant issue across all three risk areas, highlighting the growing disparity between those who know how to use AI effectively, and those who don't.

- **FCRM professionals have the broadest adoption of AI (closely followed by Financial Risk)** – at least two-thirds of risk professionals in FCRM (74%) were already using AI tools, with a notable focus on anti-fraud and Anti-Money Laundering (AML) applications. Use of AI in FCRM has hit a plateau as risk professionals move on from their initial implementations. A deeper understanding of the real strengths and weaknesses of AI is crucial to new developments in this area – as highlighted by our interviewees, who suggested that the use of AI in financial crime has hit a boundary. As in Financial Risk, there seems to be a greater focus on data preprocessing, behavorial analysis, client segmentation and the use of NLP techniques such as sophisticated lexical analysis, and less of a focus on core decision making. Different areas of financial crime (such as sanctions screening and trade surveillance) have different ideas of what an 'optimal' algorithm is, while AI for fraud analytics is an equally complex area that depends largely on context.

- **For GRC professionals, it's about using efficiency to increase engagement with exasperating systems**. Almost three-quarters of respondents (71%) cited time savings as a main benefit of using AI. According to 42% of respondents, the big impact of AI will be on data validation for regulatory reporting. As GRC analytics take off, Operational Risk (OpRisk) quantification looks like becoming a growth area in this sector. Interviewees suggested that cyber risk (within the universe of OpRisk) is the area in which quantification and modeling are furthest ahead, as advanced AI (involving ML and other approaches) rapidly gains prominence.

- **Financial Risk professionals, already acquainted with statistical techniques, take a pragmatic view** – 62% view AI as a viable alternative to established statistical models. But AI tools will have to prove themselves against other, more familiar statistical techniques that may not be perfect, but which are more explainable. Our interviewees suggested that most quantitative professionals are becoming rapidly acquainted with languages such as R, Matlab and Julia, and with other data science tools, in order to build quickly and easily configurable applications using a variety of techniques in surrounding ecosystems (of which the Python ecosystem is the most advanced).

- **Within Financial Risk, ML and NLP are increasingly being applied to a broad range of problems within the areas of market risk, credit risk and portfolio management**. Clustering techniques such as topological data analysis and unsupervised neural networks are also being used widely as potential alternatives to Principal Component Analysis (PCA) techniques. The tools being used – many of which are GPU-friendly – are inspired by a broad range of underlying methods, including evolutionary programming and Tabu Search.

- **Traditional 'quant' techniques are increasingly being used in hybrid approaches with AI**, notably in stress testing and curve construction and validation. Combinations are occurring elsewhere too, with Monte Carlo simulation techniques coupled with ML and data tagging.

- **In effect, research and strategy teams are the largest users of AI**. AI is already playing a significant role in data preprocessing, segmentation and modeling, although existing quant methods will continue to dominate in the 'last mile' (such as sensitivity analysis and P&L analysis).

Not only do these results and our accompanying analysis provide a more nuanced view of AI use in key areas of RegTech, they also offer other risk professionals a useful guide to their own adoption of these technologies. By accessing the depth of analysis in our main report, risk professionals everywhere can determine where they stand on AI, and where they want to move to in the future.

2. Introduction: building on past research

This report details recent research conducted by Chartis and IBM into the use of AI in risk and compliance in the finance industry. It follows *Demystifying Artificial Intelligence in Risk and Compliance: A Step-by-Step Guide*, a collaborative piece of research published by Chartis and IBM in April 2018. That research took a broader approach, getting behind the hype around AI to a more practical view. In this wave of research, we wanted to dig deeper into three specific areas of risk and compliance – Financial Risk, FCRM and GRC – to identify different and equivalent trends in the adoption and use of AI tools and techniques.

Our aim was to get a view of AI 'on-the-ground': a sense of how risk and compliance professionals today view and approach these emerging and evolving technologies. We also wanted to answer some key questions:

- Where in these three key areas of risk and compliance are AI tools and techniques being used?
- How far have they penetrated financial organizations?
- What patterns of adoption have we seen across the three areas?
- Are risk professionals early adopters on the whole, or fast followers?

Finally, and most importantly, we ask what the implications of these findings are for the wider risk and compliance community, both now and into the future. As we made clear in our previous research, AI is not magic or weird science, but a set of practical tools that can be used now to improve processes and save costs. But as we will see, there is still some uncertainty around the use of AI and exactly what these tools and techniques entail for risk professionals – and this uncertainty is likely to continue to shape how these users implement AI tools for some time. For risk professionals, knowing where they sit in this environment, in relation to their peers, can be a useful benchmark by which to calibrate their own attitudes and approaches, so that they can assess, or even reassess, their own unique approach to AI.

To explore these themes and ideas, we conducted the following[1]:

- A quantitative survey of 73 relevant market participants, including CROs, CTOs, CIOs, CCOs and senior risk decision-makers.
- A total of 20 qualitative interviews with a total of 28 risk-focused professionals across a variety of relevant institutions.

The findings revealed some interesting results, both at the overall level and within each risk and compliance category.

[1] *A more detailed breakdown of the respondents is given in Appendix A. Note that rounding factors mean that some charts may not add to exactly 100%.*

3. The main story

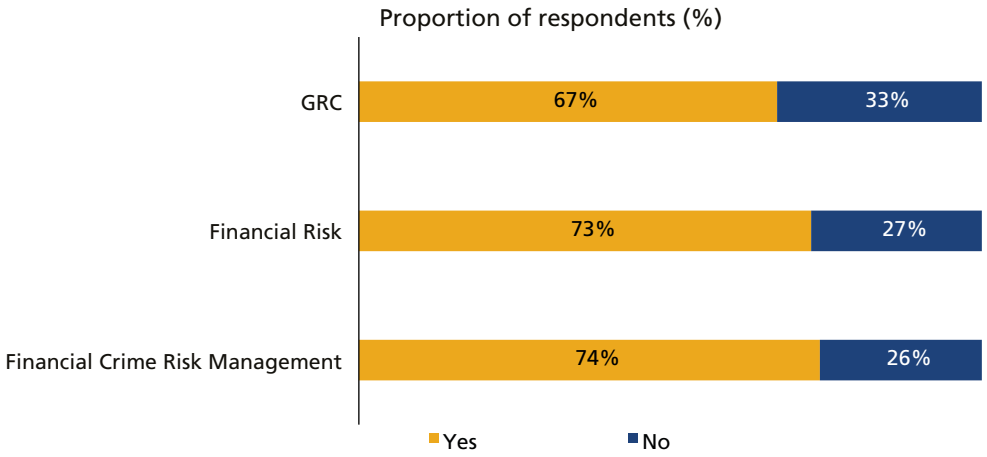
Firstly, we consider our overall findings, before looking at the individual areas in the next section.

Broad but cautious adoption

AI is enjoying broad adoption across risk and compliance, and across the landscape it is already embedded in a wide variety of use cases – between two-thirds and three-quarters of respondents are already using AI in some application (see Figure 1). Although adoption is broad, however, it is also cautious – driven by fast followers rather than cutting-edge innovators (see Figure 2).

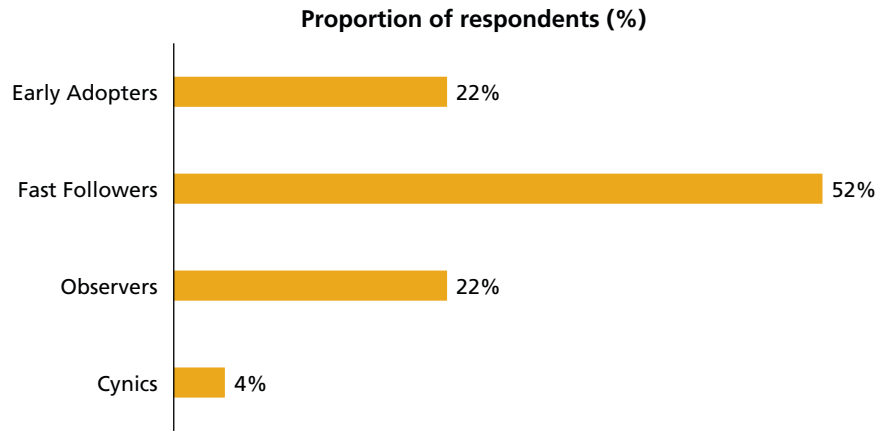
Rather than being seen as an 'exotic' or even 'strange' technology in business, AI is increasingly being viewed as a standard statistical toolkit for analysts. Many quants (who tend to have most experience with analytical tools) have embraced a more hybrid approach in which they supplement their standard statistical toolkit with AI techniques when faced with high-dimensional problems or multivariable contexts. Many have also become familiar with toolkits and ecosystems (such as the Python ecosystem) that allow them to rapidly add sophisticated data management capabilities to their core analytics. However, these new tools may themselves create organizational challenges that are much larger and more complex than the spreadsheet environments many FIs may be used to.

Figure 1: Use of AI tools in risk and compliance management, by area



Q: In which of the following areas of risk and compliance management are you using AI tools? (Yes/No)
N = 73
Source: Chartis Research

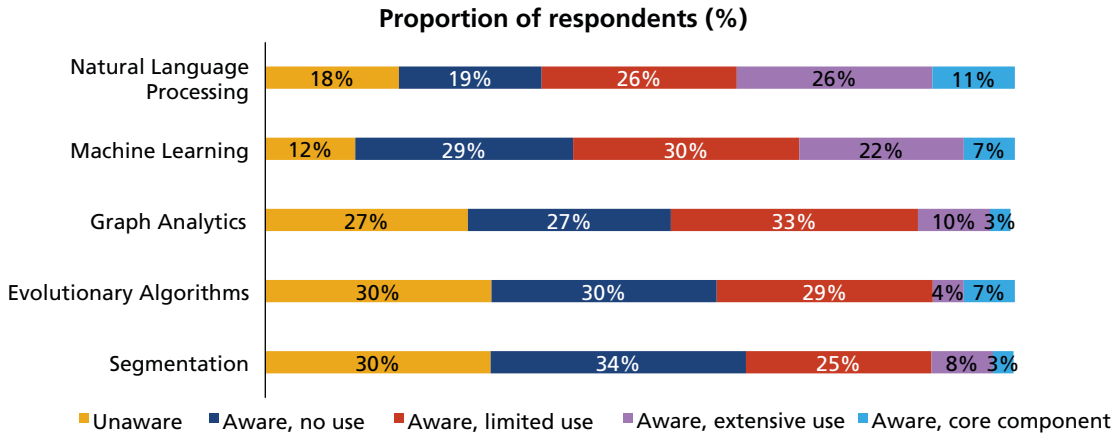
Figure 2: Institutional approach to AI adoption



Q: Which of the following statements best describes your institution's approach to AI adoption? (Select one answer)
N = 73
Source: Chartis Research

Among types of AI tools, NLP and ML are currently gaining the highest levels of traction among respondents (see Figure 3). NLP in particular – in many ways the 'workhorse' of AI techniques – has rapidly become a core element of data management systems, providing a powerful mechanism for industrializing the conversion of unstructured data into structured data.

Figure 3: Level of awareness of specific AI tools



Q: To what extent are you engaging with the following AI tools to support compliance activities? (Select one answer for each tool)
N = 73
Source: Chartis Research

Many of the hundreds of valuable NLP use cases (such as converting and mapping load documents, analyzing term sheets, or converting and auto-tagging fixed-income term sheets) have a long history, although they have become more standardized, stable and industrialized in the last few years.

Drivers of AI use: efficiency and accuracy

While compliance looms large in the reasoning behind AI implementations, in practical terms AI is being used to improve organizations' efficiency (see Figure 4). The main focus of AI projects tends to be streamlining processes, saving time, improving data management and controlling costs. Cost

savings come in a variety of guises, from the better utilization of data and infrastructure to the more efficient use of people's time. Considerable additional savings can also be gleaned from the shrinking costs of compute hardware, as well as the next step in general office automation – the automation of straightforward documentation-related tasks such as data quality checking and document scanning, all of which can be achieved using software.

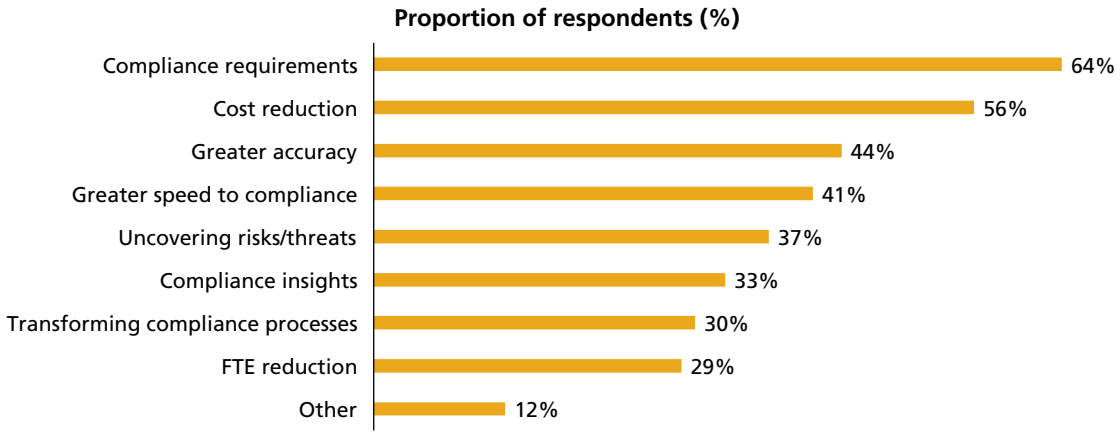
In the survey, the focus on efficiency was supported and expanded on by the interviewees. Their expectation tended to align with the notion of 'augmented intelligence', with many interviewees feeling that the increased use of AI would enable their staff to become more productive, by effectively removing repetitive drudge work from many of their day-to-day operations.

However, interviewees also identified a flipside to efficiency: many of the gains introduced by automation could be eaten away by the requirement for more expensive resources such as specific software skills. This is especially true of some automation projects, not least because of the money involved in hiring the right people to run them – effectively undermining any cost savings acquired through greater efficiency. Knowing when something is broken can also be a challenge – if the AI tool embedded in data management systems has incorrect parameters, for example.

Increasingly, institutions feel that they need people with the right expertise to manage many statistically or AI-intensive applications, creating new cost and management challenges for the organization. Risk professionals now find themselves having to balance the efficiency gains of AI projects with the costs of recruiting the right staff.

Alongside efficiency, being able to better analyze information is also a key driver of many AI implementations. In our survey, accurate analysis was deemed as important as saving time. In essence, FIs' goal in using AI techniques seems to be driving efficiency and improving their analytical accuracy, as they move beyond straightforward compliance toward a new operational era in which streamlined, more efficient, augmented human processes are supplemented with more accurate data and analysis.

Figure 4: Purpose of AI deployment



Q: For which purposes is your institution deploying AI tools in a risk and compliance context? (Select all that apply – note total responses are > 100%)
N = 73
Source: Chartis Research

Other considerations: efficiency and regulation

For most institutions, AI is helping risk and compliance teams keep pace with regulation and be more proactive. The employment doomsday scenario predicted by some commentators appears to be more myth than reality so far. Any drop in compliance staff numbers in the immediate future will likely be the

result of natural fluctuations in regulatory-driven recruitment that happens regardless of the underlying technology.

Finally, while compliance issues are an important consideration in AI projects, and AI is often used in a compliance context (to make reporting processes more efficient, for example), the threat of regulation is not a material barrier to organizations adopting AI. Financial Risk professionals were most concerned about regulatory sign-off for their AI projects, but the 36% that cited it were well behind the group that cited data availability (58%) and insufficiently knowledgeable staff (49%). In both the FCRM and GRC groups, the proportion citing regulatory sign-off as a challenge struggled to rise above 20%. This relative lack of concern around regulation suggests that there are significant areas of finance and banking where AI techniques can be used far more than they are today within the current regulatory environment.

The interviews provided support for this view, and an intriguing corollary. CROs and modelers encounter much confusion in terminology around the issue of data regulation, and while data regulations often indirectly impact AI methods, some interviewees felt that they rarely affect them specifically (i.e., red-lining rules affected all statistical tools). Two individuals with global responsibility for model methodology in their firms also revealed that compliance professionals' inability to prove the quality of their results was often attributed directly to regulatory issues (in other words, regulators could be made convenient scapegoats for troubled implementations).

In financial crime and compliance departments many institutions are reluctant to implement aggressive resource roll-back projects, recognizing the need to gain more demonstrable results from applying AI systems to decision-making processes. Again, however, these issues apply to all statistical approaches, not just AI. Arguably, in many supporting areas (such as client segmentation, behavioral analytics and entity resolution) there is simply no problem at all.

4. Digging deeper: AI adoption and use in Financial Risk, FCRM and GRC

Having considered the broader findings, what did the research have to say about each of the individual areas?

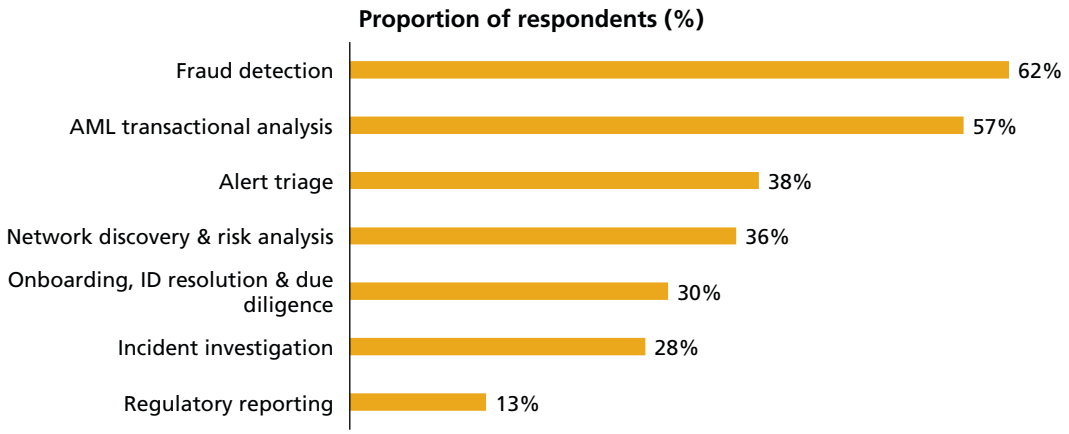
FCRM

Professionals working in FCRM were among the earliest adopters of AI tools and techniques, and the use of AI is widespread in the sector, particularly in the areas of anti-fraud and AML (see Figure 5). AI tends to be applied in the areas of segmentation, data analysis and scenario generation, and efficiency and accuracy are seen as the main benefits of implementations (see Figure 6). FCRM is one area where reducing headcount has often been touted as a goal of automation systems – yet only 17% of FCRM respondents in our survey cited FTE reduction as a benefit of AI implementation.

FCRM teams seem content to automate some of their processes and organize and structure their data using AI tools – perhaps in the hope that this will lead to FTE reduction directly or indirectly. For now, however, reducing the repetitive drudge work inherent in many FCRM processes is a priority, alongside understanding what's going on in AI tools (an increasingly important consideration elsewhere in the organization).

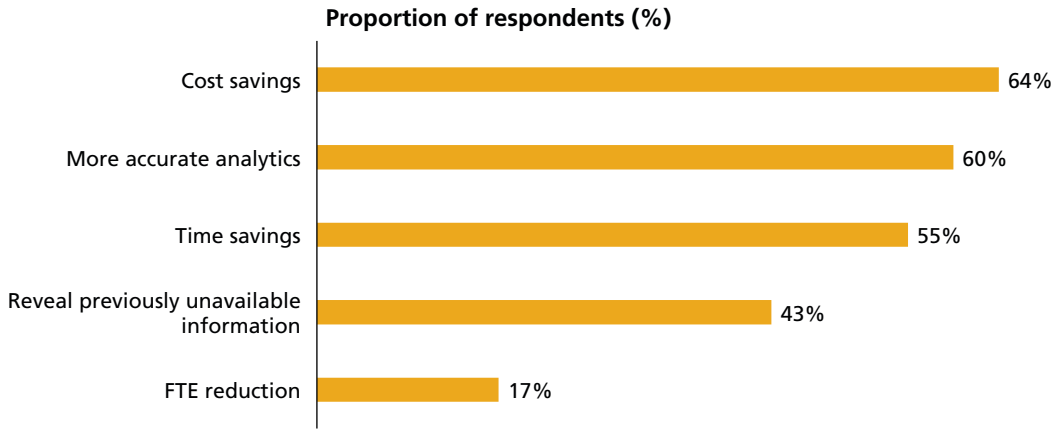
In the more complex areas of FCRM, such as investigations or key decision-making, AI tools have struggled to make headway. Decision-making is a vital part of the FCRM process, and judgements can have serious consequences. In that specific area of FCRM AI is being used to augment decision-making, not replace it. Understanding and explainability are also becoming increasingly important in the area of FCRM, partly to satisfy regulators, but also to convince boards that the technology can bring genuine results.

Figure 5: Where is AI most effective in an FCRM context?



Source: Q: For which areas of the FCRM process do you see AI being the most effective? (Select all that apply – note total responses are > 100%)
N = 47
Source: Chartis Research

Figure 6: Main benefits of implementing AI for FCRM

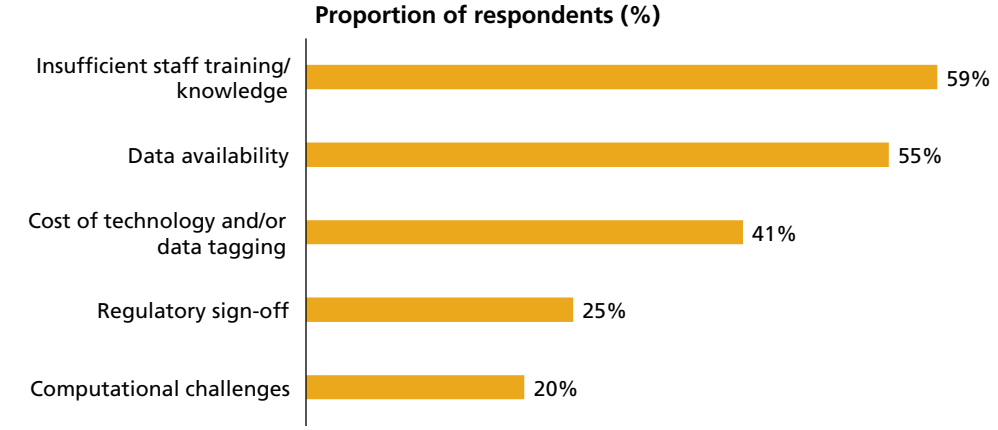


Q: Which of the following factors do you consider to be the key opportunities or benefits of implementing AI tools for FCRM? (Select all that apply – note total responses are > 100%)
N = 47
Source: Chartis Research

Challenges: now and in future – accuracy and understanding

For most FCRM respondents in our survey, the biggest challenges facing them when *implementing* their AI systems was the lack of experienced staff able to take on the task, followed by the perennial problem facing many AI projects – a simple lack of available and suitable data (see Figure 7).

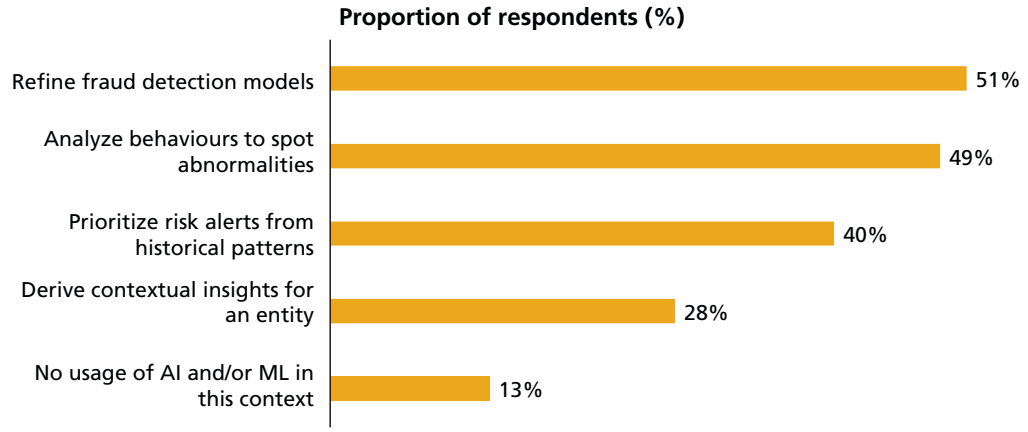
Figure 7: Main challenges to implementing AI for FCRM



Q: Which of the following factors do you consider to be the key challenges in the implementation of AI tools for FCRM? (Select all that apply – note total responses are > 100%)
N = 47
Source: Chartis Research

As highlighted by the interviews, one of the biggest constraints with the ongoing *running and success* of FRCM projects is the modest quality of results – which run a spectrum from being no use whatsoever to being very tough to prove. One of the applications of AI identified by our survey respondents is to lessen the impact of false positives, using a variety of specialist techniques (see Figure 8).

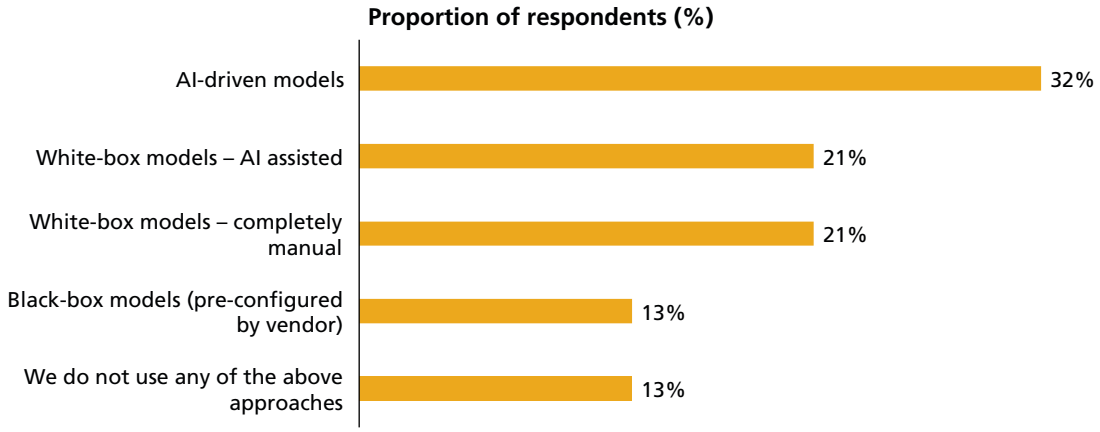
Figure 8: Impact of AI on reducing false positives



Q: How are you employing AI and/or machine learning to reduce the impact of false positives? (Select all that apply – note total responses are > 100%)
N = 47
Source: Chartis Research

Alongside the knowledge of the staff implementing AI projects, the general 'explainability' of AI tools is of growing relevance and importance. Risk professionals must be able to understand AI models as a whole, not just the underlying algorithms. So-called 'white box' and AI-assisted frameworks are considered more important than models that can't be inspected or explained (see Figure 9). Ideally, FCRM teams want a 'wrapper' around an AI tool to help them understand the results of the process in an intuitive way – in easy-to-manage terms that enable them to explain their results to someone else.

Figure 9: The nature of existing financial crime detection models



Q: Among the following, which option best describes the nature of your current financial crime detection models? (Select one answer)
N=47
Source: Chartis Research

The evolution of AI in FCRM

The results of this survey highlight some key trends in the three main themes in managing financial crime risk: *modeling, detection* and *investigation*, supporting our wider research into this important area of AI use. In this research, financial crime and compliance professionals felt very strongly that there were specific areas where AI applied well, and others where more traditional analytical tools would be better suited. Supporting roles such as data preparation, model testing and back-testing (including scenario generation and creating stress tests) were seen as areas with strong possible applications.

- **Modeling**. As shown in Figure 8, FCRM respondents were looking to use AI in improving their internal analytics, specifically improving and refining their internal models, as well as focusing on customers' behavioral analytics. Within this context, what we are likely to see in the modeling space is a move from what we might term 'commodity' (or supervised) ML techniques that rely on past historical data to techniques such as cluster analysis, which employ unsupervised ML that focuses on true customer risk and behavior.

- **Detection**. Most of the FCRM respondents are comfortable with the use of AI in early warning and detection systems such as fraud detection and AML transactional analyses. This comfort – a crucial factor in AI adoption – is likely to spur calls for more adoption of AI tools in the areas of detection and triaging alerts, to enable systems to mature and become more effective.

- Investigation. In contrast to both modeling and detection, faith in AI systems was much lower for second-order activities such as investigations: fewer than one-third of respondents felt that AI would be effective in that setting. The crucial consideration here is one of *knowledge transfer* and *education*. The work done by these early adopters is crucial in this regard, if vendors and FIs are to develop a more standardized, and ultimately effective, approach to using AI to enhance investigations.

Forthcoming research from IBM and Chartis' sister brand *Risk.net*, due in early 2019, will explore these themes and trends in more detail.

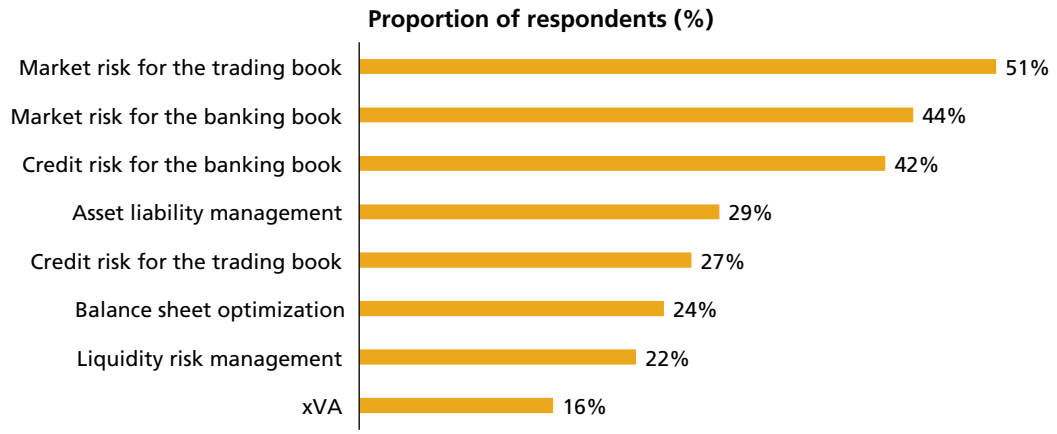
Financial Risk

A great many use cases

In the area of Financial Risk there is broad adoption of AI across market and credit risk (see Figure 10). Professionals in this particular area of risk and compliance are already familiar with statistical techniques, and many view AI as simply another statistical tool among many. In fact, as we shall explore later, this relative experience with statistical tools points to some important qualitative differences between risk professionals in Financial Risk and those in the other areas.

These differences sit on both sides of the adoption issue. According to the Financial Risk professionals we interviewed, AI offers very few new structural challenges (many of those we interviewed had used AI techniques in the past, notably various types of neural networks and evolutionary programming). There was a general view that as computational techniques and computing power continued to increase, AI (and specifically ML) could eventually become mainstream tools. In fact, AI techniques are becoming ubiquitous in the sector because of the relative benefits they offer in terms of cost, ease of access and speed of performance.

Figure 10: Use of AI tools in financial risk



Q: In which areas is your firm using AI tools to help you manage financial risk? (Select all that apply – note total responses are > 100%)
N = 45
Source: Chartis Research

Within Financial Risk, ML and NLP are increasingly being applied to a broad range of problems within the areas of market risk, credit risk and portfolio management. ML is increasingly seen as a powerful tool in areas such as scenario generation and stress testing, as well as curve construction and validation (for yield curves, for example, or smile curves). ML tools are also being used heavily in conjunction with NLP in data preprocessing, such as in converting unstructured data into structured data (bond terms and conditions into transactable and analyzable time series, for example).

Equally, clustering techniques such as topological data analysis and unsupervised neural networks are being used widely to help set up factor analysis, which offers potential alternatives to PCA techniques. Heuristic combinatorial analysis, traditionally used for portfolio optimization, is starting to make a significant comeback – albeit a slow one. The tools being used – many of which are GPU-friendly – are inspired by a broad range of underlying techniques, including evolutionary programming and Tabu Search.

Traditional 'quant' techniques are also increasingly being used in hybrid tools alongside AI. A good example of this in the context of financial risk is the use of AI techniques in constructing stress tests, and the use of ML in curve construction and validation. In other areas, several approaches have married Monte Carlo simulation techniques (to generate use-case paths and data inputs) with ML and data tagging to more efficiently generate automated maps, validation routines and portfolio strategies.

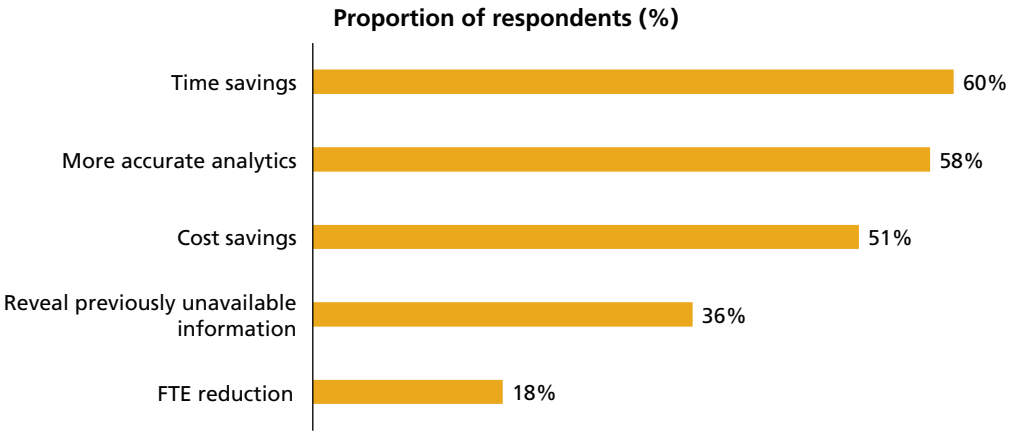
Within Financial Risk, research and strategy teams are the largest users of AI. AI is already playing a significant role within banks' and FIs' operations, in the areas of data preprocessing, segmentation and modeling. Nevertheless, existing quant methods still dominate in the 'last mile' (such as sensitivity analysis and P&L analysis), and the interviewees we spoke to did not expect this to change.

Despite this wide adoption, however, AI tools are still seldom used in core models in Financial Risk. Two quant managers we spoke to saw little real use for AI techniques, although they agreed that many of their existing algorithms resembled ML in any case. Neither felt they would be venturing down the ML path any time soon, since they each felt that their existing models achieved the same outcomes and – crucially – were more explainable. Their existing algorithms have evolved over many years of use, are optimized for specific contexts, and used specially configured hardware (and indeed software). Their analysts and mathematicians had developed a deep understanding of much of the parametrization process. However, they believed that if different hardware had been available (if high-performance programmable GPUs had preceded custom FPGAs, for example) then they might have pursued a different path, though some details of ML frameworks posed methodological challenges.

Benefits and challenges

Even within the statistical context that distinguishes Financial Risk, accuracy and efficiency (in the form of time and cost savings) were again seen as the main benefits of AI (see Figure 11). As highlighted by the interviews, there tends to be a focus in Financial Risk on supplementing research with data preparation and data sciences, particularly in the areas of credit, commodities and equities – in fact, use of both techniques is fairly widespread in the sector.

Figure 11: Main benefits of implementing AI for financial risk



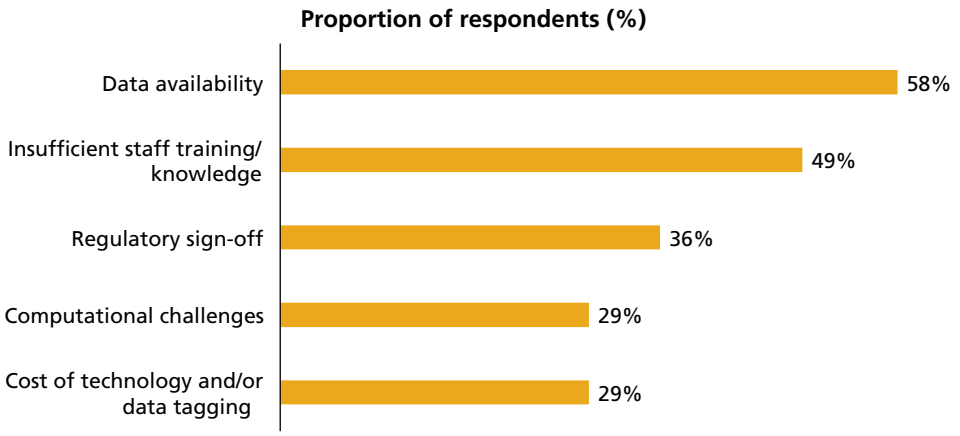
Q: Which of the following factors do you consider to be the key opportunities or benefits of implementing AI tools for financial risk? (Select all that apply – note total responses are > 100%)
N = 45
Source: Chartis Research

Data sciences are also enjoying fairly widespread use across asset classes. The consumption of AI-supplemented data is another avenue that is often explored – users buy data from third parties that use AI to map and organize it. There are a large number of specific AI use cases in Financial Risk, across both market risk and credit risk, including interest rate calculations, constructing curves and identifying gaps in curves, mapping equities, and constructing equities portfolios, as well as mapping balance sheets to equity and credit models and using non-financial data in credit models.

There are also several examples in the Financial Risk sector of areas in which AI is improving existing analytics, particularly curve construction, identifying gaps in curves, and pinpointing anomalies in data. In market risk specifically, AI tools are being used extensively in stress testing, in creating scenarios, and in behavioral and regression-style models. FIs are also already widely using ML for fairly straightforward benefits, often as an alternative to PCA models.

The biggest challenges to implementing AI are the availability of data and suitably knowledgeable staff (see Figure 12). Regulatory sign-off also featured fairly strongly, reflecting the particular scrutiny that Financial Risk systems are under.

Figure 12: Main challenges to implementing AI for financial risk



Q: Which of the following factors do you consider to be the key challenges in the implementation of AI tools for financial risk? (Select all that apply – note total responses are > 100%)
N = 45
Source: Chartis Research

When asked about regulatory restrictions in a general context, 36% suggested it was a key challenge. Even so, attitudes to regulation varied. When the question focused on specific analytical and operational activity (such as credit activity and credit risk analytics), only 20% agreed that regulation was seen as a serious restriction.

So while regulations are clearly seen as a critical challenge, there are many operational and analytical areas in which they are not perceived to be a significant hurdle. Specifically, the results suggest that regulations are a stronger constraint in more structured areas (such as regulatory reporting and enterprise risk). As a corollary, analytics developed to run the business are subject to fewer regulatory challenges than analytics developed and deployed for regulatory reporting and enterprise analysis.

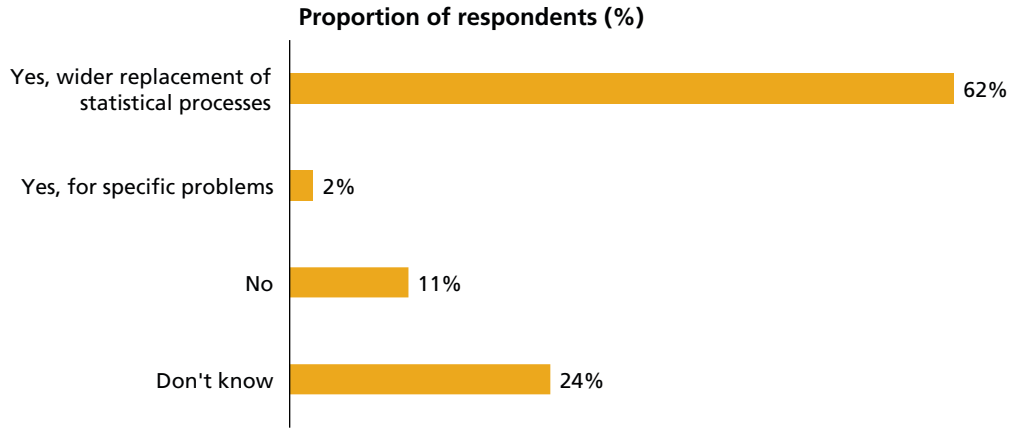
Qualitatively different

Financial Risk professionals' general acquaintance with statistical methods means that they approach AI in a different way to those in the other sectors. Two key factors are at play here: the toolbox factor, and the familiarity factor.

One tool among many

Many (about 60%) of those involved in Financial Risk regard ML as a potential alternative to existing statistical techniques (see Figure 13) – as another process that will have to compete with those already in place. This suggests that in Financial Risk, AI – and in particular ML – is seen as a complex non-linear statistical process, and as such is a natural fit with a business that is probably highly statistical and quantitative in any case.

Figure 13: AI as a viable alternative to established statistical models



Q: Do you consider deep learning/machine learning models a viable alternative to existing statistical models (e.g. GARCH Structural Credit Risk Model)? (Select one answer)
N = 45
Source: Chartis Research

There are plenty of examples of areas where AI tools – and ML in particular – are being used in Financial Risk analytics. These include curve construction; using ML to build interest rate curves, e-curves and similar curve models; and trying to find gaps and anomalies in data. ML also works well in frameworks based around cluster analysis, which in statistical terms can be very difficult to explain – and very slow to operate. The overlapping areas of PCA, factor analysis and cluster analysis are also good candidates for replacement with ML. Scenario generation, because of its multivariable nature, also suits ML tools well.

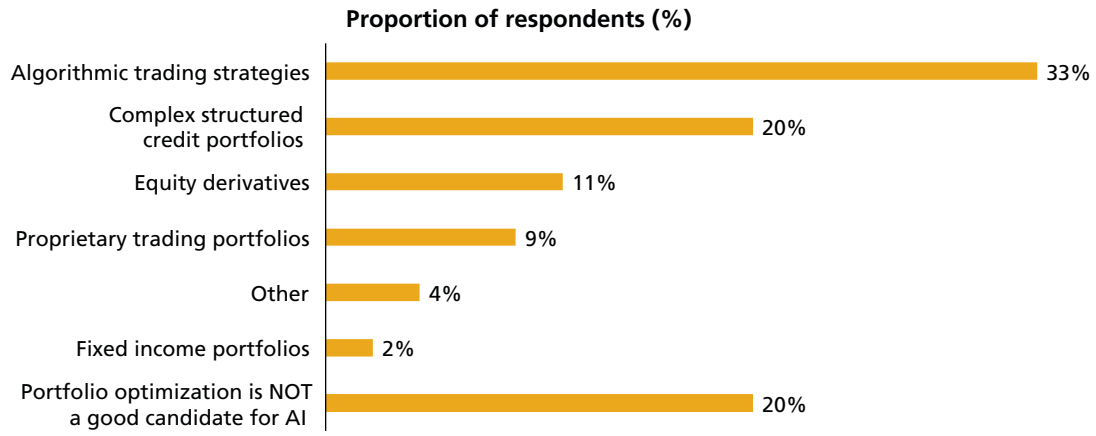
Time-series models, on the other hand, are not good candidates for ML substitution. Financial risk professionals already use well-established time series systems with very efficient schemas; what's more, their users understand how they change over time, and in reality ML hasn't proved itself in this area – on the whole it simply can't compete with more established models.

Perhaps unexpectedly, Financial Risk professionals have considerable confidence in AI as an algorithmic trading tool (see Figure 14). One-third of Financial Risk respondents believe that AI has proved successful in algorithmic trading and real-time portfolio management. This is a possible point of departure and divergence from interviewees: while survey respondents were clear on the suitability of AI for algorithmic trading, interviewees suggested that the tools they were using were similar to ML but not exactly the same.

The use of AI in algorithmic trading is restricted, because the process involves rapid decision-making that requires more straightforward software tools, and even relying on GPUs ML is not the ideal algorithm in that setting. In the area of preparing data for the algorithmic system itself, however, AI and ML have a definite role to play.

In short, while AI and ML may replace some existing algorithms, for the most part they are components of a wider toolbox available to users. AI may replace algorithms only when it's efficient and practicable to do so. Ultimately, while AI is introducing a change to the Financial Risk area, it does not constitute a complete overhaul. Crucially, for AI tools to be adopted, first their users have to *understand* how they work.

Figure 14: For which portfolio optimization problems is AI a good candidate?



Q: Portfolio optimization models in non-linear financial instruments are cited as an optimal use case for AI. In this context, where do you consider AI adoption to be highest? (Select one answer)
N=45
Source: Chartis Research

Familiarity

This leads us to the second main theme in Financial Risk – an important one when we come to consider the wider adoption of AI across the risk and compliance space – namely *familiarity*, alongside *explainability*, *knowledge* and *comfort*. While our findings show that the priority for financial risk professionals is efficiency and accuracy, understanding and comfort levels around this new technology are absolutely central to adoption.

Few risk professionals are wholly familiar with AI algorithms, even in the area of Financial Risk, which is already highly statistically aware. Knowledge of and familiarity with algorithms in any organization is a process of osmosis, involving a steady diffusion of skills and knowledge throughout the organization. Staff and users have to adjust to new mental models, which can be a challenge if they are already familiar with other ones. Some people may simply refuse to change, exacerbating the problem.

From our wider research, and confirmed by the interviewees in this study, in certain sectors – notably asset management – many professionals don't even use the latest tools that are already available, largely because explaining these tools to their end users, some of whom are less technically and mathematically inclined than they are, can be a real challenge. In sectors like asset management it is not acceptable to simply tell the end user that a tool exists – they need to know how it works. Many users may modify existing models to make them more understandable – even if they contain errors. The issue here is one of *comfort* – risk professionals and their end users are unlikely to adopt a new tool unless both parties are comfortable using it, leading to an inevitable trade-off in the tool itself between being right and being explainable.

For a large section of the industry, including asset management, this is not a trivial issue – being able to explain how a model works is part of some FIs' legal contract with their end users. This explains the continued use of techniques (such as certain models used in performance attribution) that have theoretical problems – because they are relatively easy to explain. And, if fund managers can't understand a model, they are less likely to provide funding.

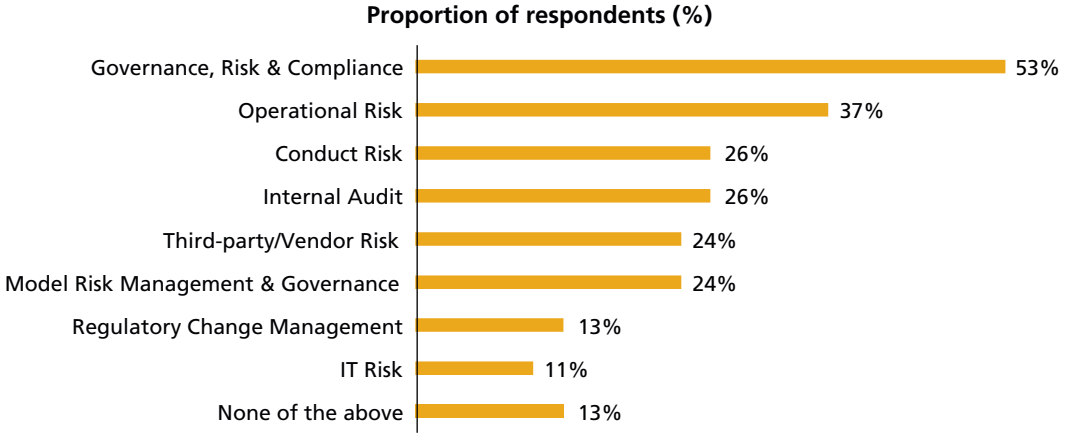
Comfort is greater in areas such as data preparation because users don't have to explain to their clients how they created their data. When reporting, by contrast, users are much more likely to feel uncomfortable using AI and ML models. This is especially true for credit scenarios, for example: from the end user's perspective, once a scenario has been constructed, so long as its parameters are clear, the way in which it was constructed is less of an issue. In fact, the real issue is not one of a conflict between

AI and existing statistical mechanisms, but often a conflict between the existing statistical methods themselves and the tools that are currently used in the industry.

GRC

Use of AI in GRC is growing – more than half of respondents are using AI tools for enterprise GRC, with OpRisk the largest segment (see Figure 15). The theme of efficiency as a key driver of AI adoption was particularly evident in this sector.

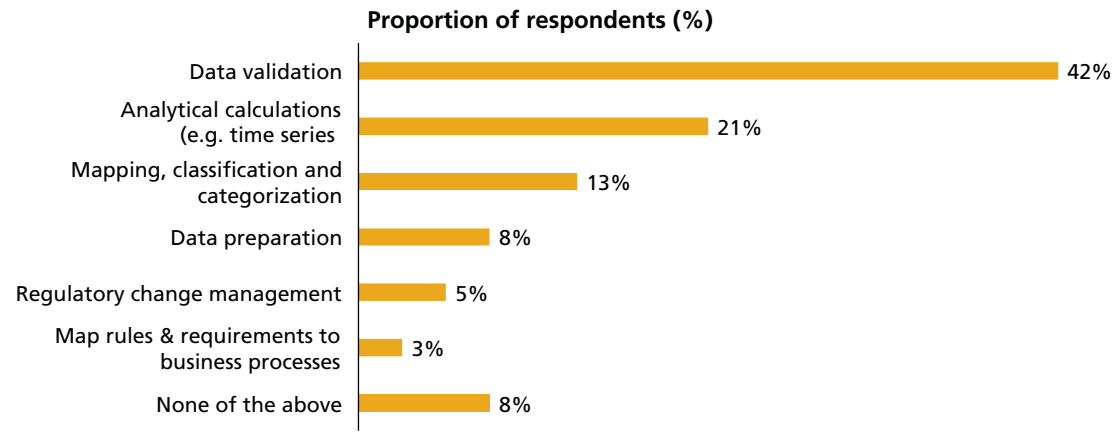
Figure 15: Use of AI tools in GRC



Q: Which, if any of the following AI tools are you using for GRC compliance? (Select all that apply – note total responses are > 100%)
N = 38
Source: Chartis Research

For those involved with GRC systems, AI offers most value in automation and data validation, cleaning and speeding up the time-consuming elements that can ultimately stymie GRC systems (see Figure 16). The problem that many risk professionals encounter with GRC systems is tedium: users have so many issues, Key Performance Indicators (KPIs) and rules to feed into the system that they simply give up. Automating much of that process, as well as elements of data validation and control, is seen as a vital next step to keep GRC systems valid. Another area generating interest is the use of NLP to help users with categorization and mapping (such as mapping obligations to existing controls, policies and procedures).

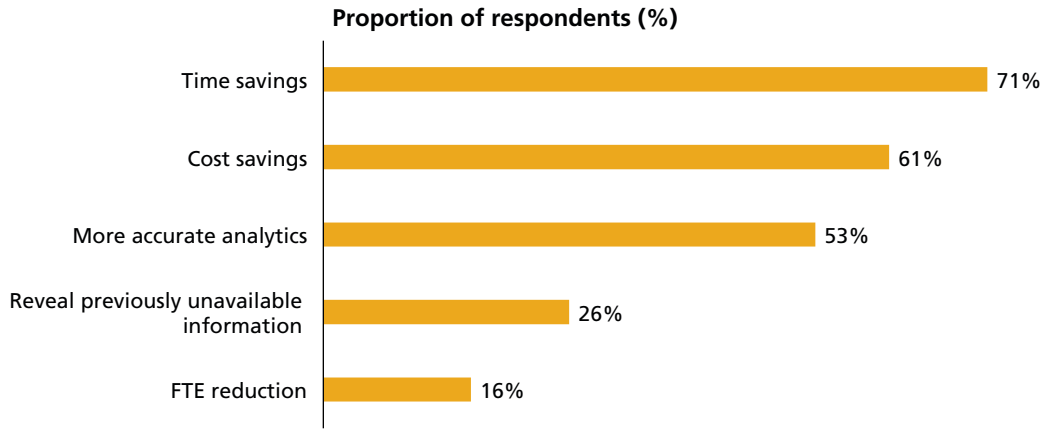
Figure 16: Impact of AI on the regulatory reporting value chain



Q: Where in the regulatory reporting value chain do you see AI playing the greatest role? (Select one answer)
N = 38
Source: Chartis Research

Time saving in particular stands out as a benefit among a large majority of respondents (see Figure 17). By focusing on cleaning and organizing data and automating workflow processes – which take up a lot of time – FIs can make their GRC applications more usable, and more likely to provide outputs that key decision-makers can rely on.

Figure 17: Main benefits of implementing AI for GRC

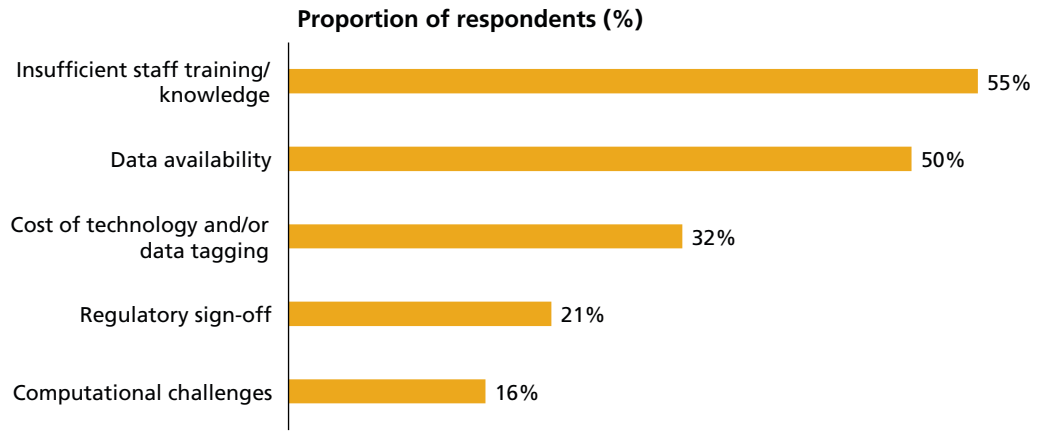


Q: Which of the following factors do you consider to be the key opportunities or benefits of implementing AI tools for GRC? (Select all that apply – note total responses are > 100%)
N = 38
Source: Chartis Research

Challenges

As in the other areas of risk and compliance, staff knowhow and a lack of available data are the two main challenges to implementing AI in GRC (see Figure 18).

Figure 18: Main challenges to implementing AI for GRC



Q: Which of the following factors do you consider to be the key challenges in the implementation of AI tools for GRC? (Select all that apply – note total responses are > 100%)
N = 38
Source: Chartis Research

Two key themes: engagement and quantification

Adoption of AI tools and techniques in the GRC sector tends to be more complex and nuanced. In a parallel to financial risk, there is a bifurcation in attitudes to and use of AI within the area of GRC. While the two strands of adoption may seem quite different, they both offer an insight into the real potential of AI in risk and compliance.

The first is *engagement*. The key factor to consider in GRC is that the implementation of GRC systems is, for many risk professionals, largely a box-ticking exercise. Most GRC systems are seldom used – largely because of the amount of repetitive work they require to keep them operational: users are more likely to refuse to use them than embrace them wholeheartedly. In GRC the biggest gains in terms of efficiency are likely to be in persuading people to use the system in the first place. Here AI can play an important role, albeit a more nuanced one than it takes in FCRM and Financial Risk, providing a user experience and interface to improve performance and boost adoption.

The focus of AI tools in GRC is data preparation and using automation to reduce the burden on end users, as risk professionals in this area attempt to make their GRC systems more useable and user-friendly by removing much of the tedious work that underpins such systems. If anything, the use of AI to streamline systems might increase the possibility that the system will be used.

5. Implications and analysis

Our intention in carrying out this research was partly to reveal some of the detail around how risk and compliance professionals dealing with financial, FinCrime and governance issues approach and use AI tools. In doing so, we have revealed several important themes in each category, and across all three.

- FCRM users were among the first to adopt AI tools, largely because the tools they already had lacked the sophistication they needed to tackle the complexities of financial crime, and there was a belief that new systems would prove a robust defense against criminals. But despite the best efforts of those involved, AI does not work effectively across the board, and its use in FCRM has hit a plateau. Not only has it largely failed to live up to its initial promise, users are also still trying to determine how to make it work effectively, not least to reduce the number of false positives that can throw an investigation off track. And the pressure on AI to succeed is heightened because the consequences of a wrong decision can be catastrophic – while an AI tool may identify a potential criminal, it's not enough to simply 'flag and run'; the burden of proof still has to be achieved if the system is to be wholly effective.

- In Financial Risk the key themes are understanding and comfort. Financial risk presents a different case to the other two sectors, in that users in that area employ statistical tools all the time. The relationship of users to technology is more mature, making explainability the key, for sound financial reasons. Users in this area view AI as one tool among many, and until it can achieve the status and explainability of the established methods it is effectively competing against, its spread across the sector is likely to remain relatively muted. A definite shift is needed in this area – from the comfort and understanding around established methods to the understanding, knowledge and comfort AI tools need to thrive.

- In GRC, the use of AI tools seems to be mostly around streamlining unwieldy systems and making them easier to use. But GRC is a wide area, and there's a growing industry around GRC analytics, including cyber risk quantification. ML fits neatly into some areas – such as process risk – largely because analytical methods are a relatively new development in this field, so AI tools are viewed as a benefit.

Two key challenges with AI, across the board, are the availability of suitable data, and the knowledge and expertise of the people using these systems and informing others about them. The overarching theme linking the results across the sectors we analyzed supports that outlined in our previous published research. AI, while enjoying broad adoption and use across risk and compliance, is not an overarching fix-all system controlling and shaping operational processes across the risk function. Like most tools and processes, its success depends on how people use, understand and interact with it within the wider structural and cultural context of the organization in which they work.

6. Conclusion

The results of our survey and interview research show that what we are seeing is widespread adoption of AI, but not a wholesale transformation. Risk professionals across Financial Risk, FCRM and GRC are adopting AI across their organizations – but in quite specific areas and for specific purposes. AI adoption is seeping into all areas of risk and compliance, but people's attitudes to it vary, partly due to their experience with statistical tools – clearly in some areas that experience is more relevant and important than in others. And the type of adoption depends – as we highlighted in our previous research – on the specific use case concerned, and the organizational context in which it sits.

One very powerful theme emerges: familiarity. Simply put, as AI use grows across the broader risk and compliance sector, to get meaningful results people must understand it. The lack of explainability in many AI tools may itself explain why adoption (outside FCRM) has been driven by fast followers rather than early adopters. People still aren't absolutely clear about what AI can and cannot do. If there is going to be a continued gap anywhere as adoption spreads, it is likely to be in getting everyone up to speed.

Looking ahead, it seems to be transparency that is important, especially in FCRM. FIs need more explanation – more ways to visualize, display and discuss AI techniques through their results. It's simply not enough to have NLP or ML – FIs need to be able to explain it and report on it, especially to supervisors. The idea of an explanatory 'wrapper' around AI tools, which helps everyone involved understand the technology and interpret its results in an intuitive way, is an appealing one. And, we believe, it is in that explanatory space that the next wave of developments in AI will happen.

Our results and analysis should hopefully provide other risk professionals with a rough benchmark with which they can assess their own attitudes and approach to these new technologies. What does this mean for your own attitudes to and adoption of AI tools and methods, in core and peripheral processes? Are you approaching AI with the same attitude as your peers? It may even be time for a reality check if you think these tools are going to achieve more than perhaps they actually can. Why do you need AI, and where it can be most effective? What are your main considerations, and what next steps should you take? Perhaps, based on this research, it is time to reassess and recalibrate your attitude to AI in risk and compliance.

7. Appendix A: Details of survey respondents

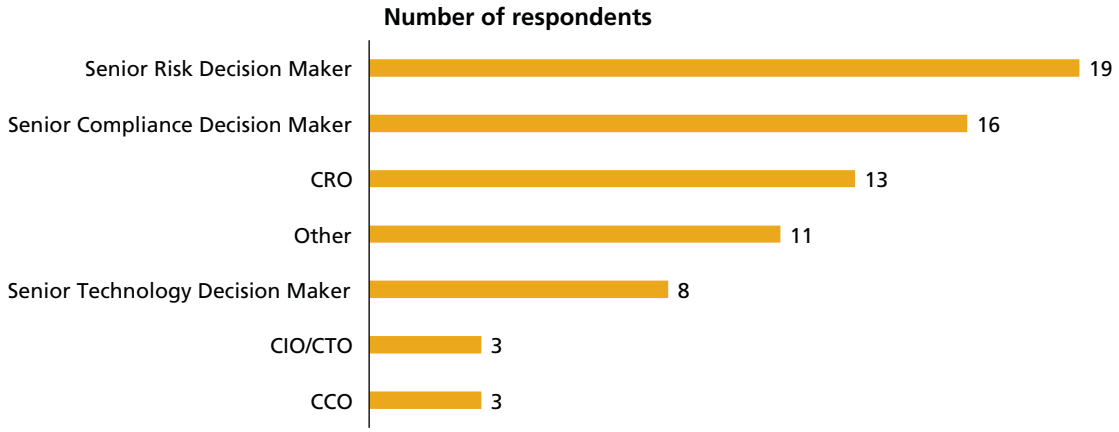
For this research we canvassed over 100 relevant market participants for their views on AI in risk and compliance:

- 73 survey respondents.
- 28 interviewees across 20 financial institutions.

Note that respondents to the survey did not belong exclusively to one risk and compliance department, but tended to answer across all three. This reflects the fluid nature of much of risk and compliance: wholly siloed behavior and thinking are rare in FIs.

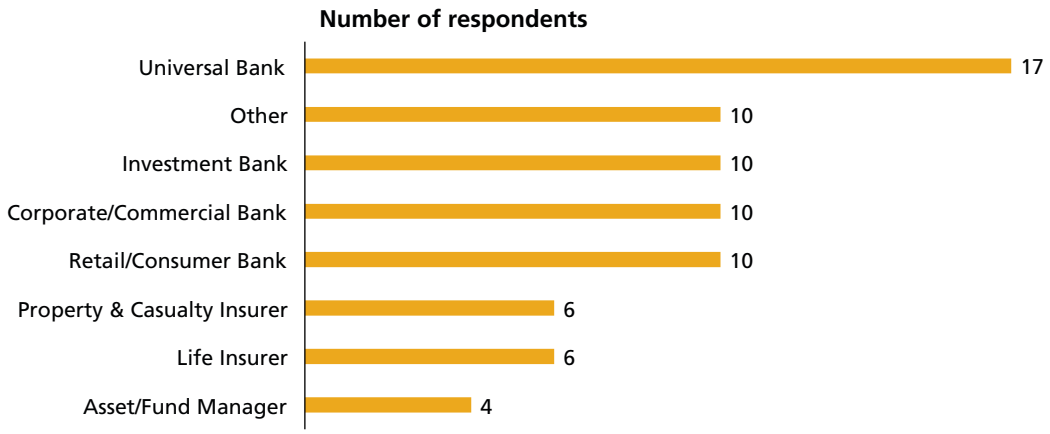
Figures 19 to 23 give details of the survey respondents by job title, organization type and size, and geography.

Figure 19: Respondents by job title



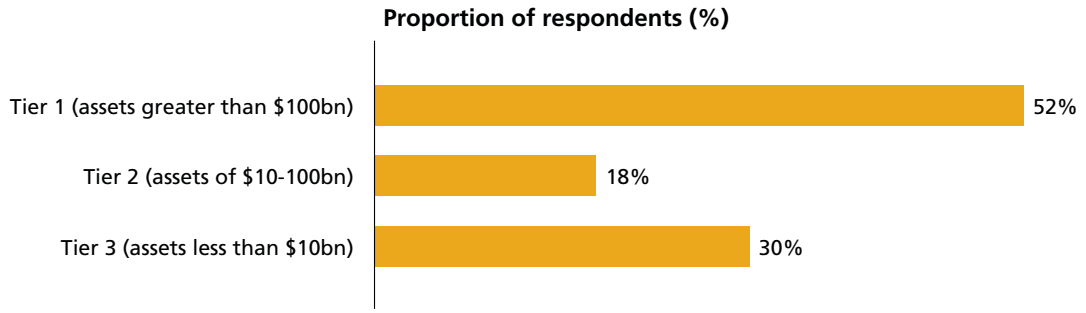
Q: Which of the following best describes your job role? (Select one answer)
N = 73
Source: Chartis Research

Figure 20: Respondents by organization type



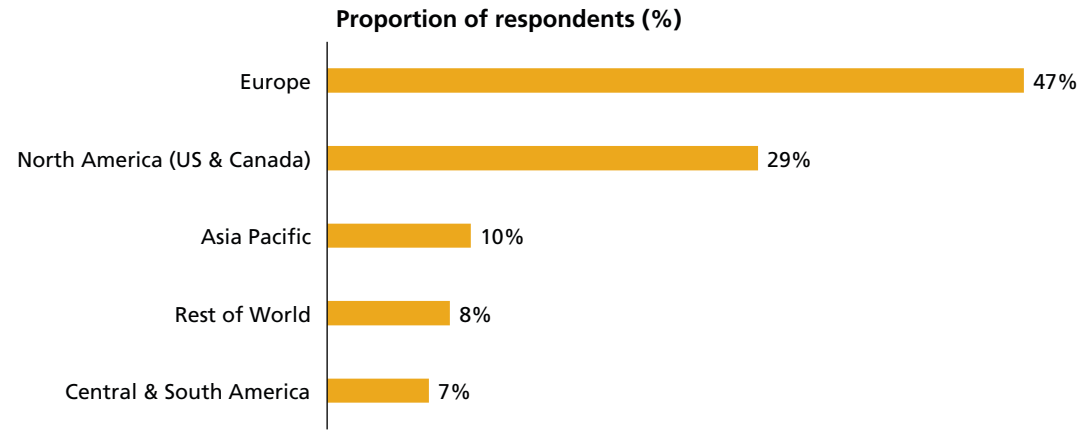
Q: Which of the following best describes your organization? (Select one answer)
N = 73
Source: Chartis Research

Figure 21: Respondents by size of organization's assets



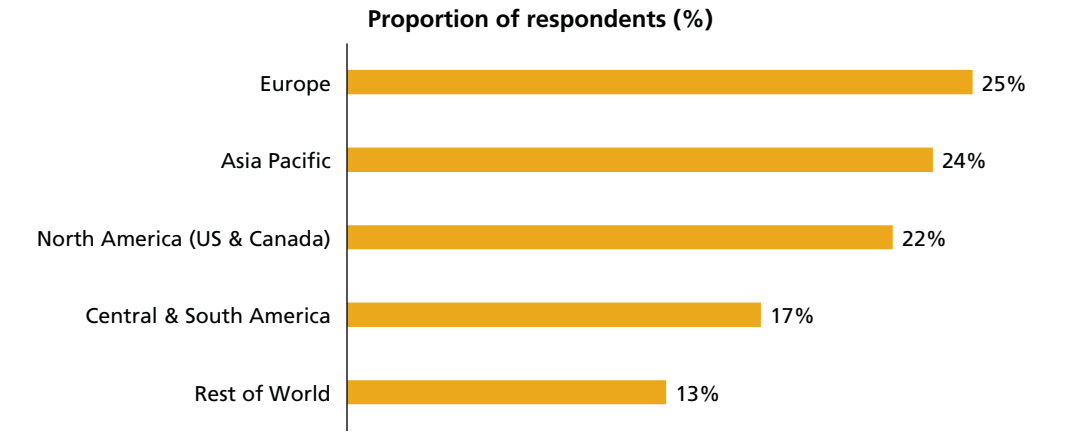
Q: What is the size of your organization by total assets? (Select one answer)
N = 73
Source: Chartis Research

Figure 22: Respondents by location of headquarters



Q: In which regions does your business operate? (We are HQ'd here; Select one answer)
N = 73
Source: Chartis Research

Figure 23: Respondents by region of operation



Q: In which regions does your business operate? (We operate here; Select one answer)
N = 73
Source: Chartis Research

8. How to use research and services from Chartis

In addition to our flagship industry reports, Chartis offers customized information and consulting services. Our in-depth knowledge of the risk technology market and best practice allows us to provide high-quality and cost-effective advice to our clients. If you found this report informative and useful, you may be interested in the following services from Chartis.

For risk technology buyers

If you are purchasing risk management software, Chartis's vendor selection service is designed to help you find the most appropriate risk technology solution for your needs.

We monitor the market to identify the strengths and weaknesses of the different risk technology solutions, and track the post-sales performance of companies selling and implementing these systems. Our market intelligence includes key decision criteria such as TCO (total cost of ownership) comparisons and customer satisfaction ratings.

Our research and advisory services cover a range of risk and compliance management topics such as credit risk, market risk, operational risk, GRC, financial crime, liquidity risk, asset and liability management, collateral management, regulatory compliance, risk data aggregation, risk analytics and risk BI.

Our vendor selection services include:

- Buy vs. build decision support
- Business and functional requirements gathering
- Identification of suitable risk and compliance implementation partners
- Review of vendor proposals
- Assessment of vendor presentations and demonstrations
- Definition and execution of Proof-of-Concept (PoC) projects
- Due diligence activities.

For risk technology vendors

Strategy

Chartis can provide specific strategy advice for risk technology vendors and innovators, with a special focus on growth strategy, product direction, go-to-market plans, and more. Some of our specific offerings include:

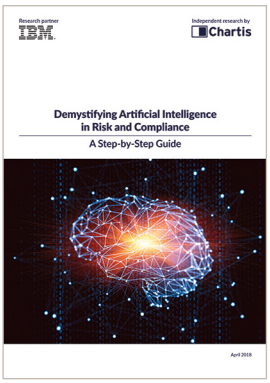
- Market analysis, including market segmentation, market demands, buyer needs, and competitive forces
- Strategy sessions focused on aligning product and company direction based upon analyst data, research, and market intelligence
- Advice on go-to-market positioning, messaging, and lead generation
- Advice on pricing strategy, alliance strategy, and licensing/pricing models

Thought leadership

Risk technology vendors can also engage Chartis to provide thought leadership on industry trends in the form of in-person speeches and webinars, as well as custom research and thought-leadership reports. Target audiences and objectives range from internal teams to customer and user conferences. Some recent examples include:

- Participation on a 'Panel of Experts' at a global user conference for a leading Global ERM (Enterprise Risk Management) software vendor
- Custom research and thought-leadership paper on Basel 3 and implications for risk technology.
- Webinar on Financial Crime Risk Management
- Internal education of sales team on key regulatory and business trends and engaging C-level decision makers

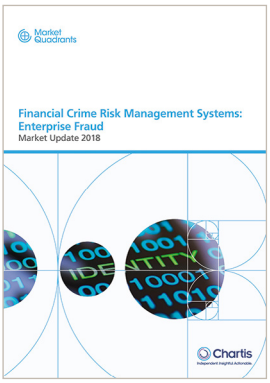
9. Further reading



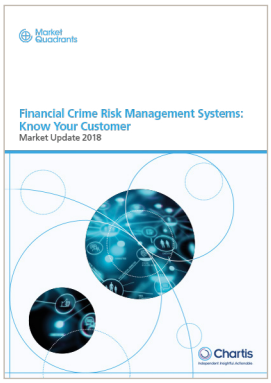
Demystifying Artificial Intelligence in Risk and Compliance: A Step-by-Step Guide

Spotlight: Artificial Intelligence in finance – A primer

Data Integrity and Control in Financial Services; Market Update 2018



Financial Crime Risk Management Systems: Enterprise Fraud; Market Update 2018



Financial Crime Risk Management Systems: Know Your Customer; Market Update 2018

RiskTech100 2019

For all these reports, see **www.chartis-research.com**