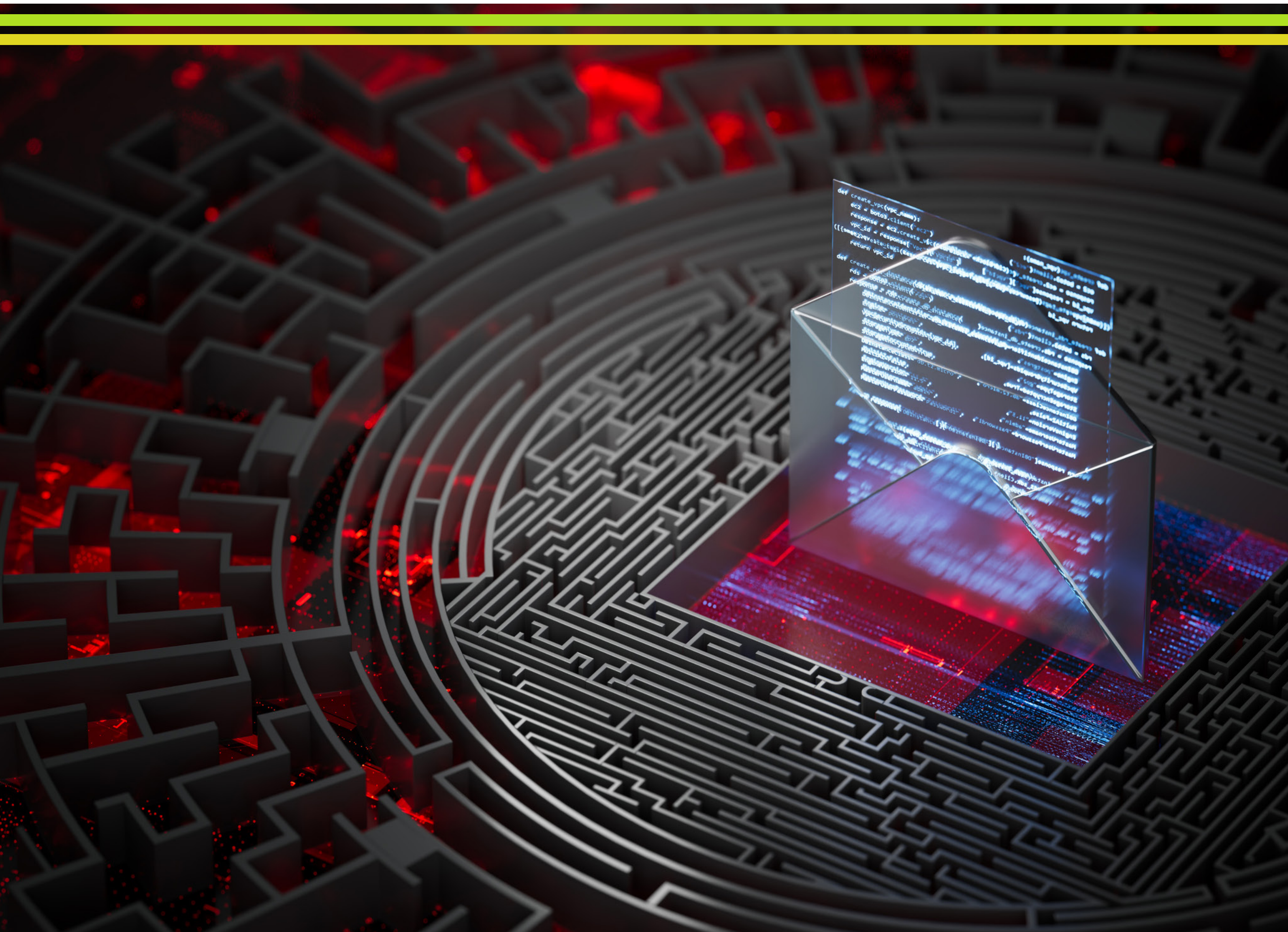
Market Insight

The role of RiskTech in effectively managing emerging risks and driving competitive edge



Contents

1. Revolution, evolution, and key findings

An influx of regulations and changing operational practices means that emerging risks must progress from their historical roots under audit and organizational control, evolving to encompass a wider set of concepts and procedures and perform a core role for banking, financial services, and insurance (BFSI) institutions. Their functions and sub-categories have expanded dramatically and are now widely linked to both the risk function and the technology function. In addition, the control function now has a broader and more strategic role, focused on business optimization and tightly coupled with frontline operations.

BFSI firms are grappling with increasingly dynamic and continuously evolving risks. Newer areas of the risk landscape, such as cyber, operational resilience, supply chain, climate and environmental, social, and governance (ESG), are pushing risk departments even further. Institutions are continuously updating their models, methodologies and operational and organizational structures to adjust to what often seems like a nebulous cloud of regulations and emerging risks. The rapid pace of change and advancement in technology means that despite progress, the RiskTech sector can still be described as relatively immature.

One of the biggest hurdles to overcome is the wide variety of quantitative techniques, alternative risk measures and frameworks for emerging risks. Increasing diversity and lack of regulatory focus on specific risk measures mean that organizations are struggling to incorporate emerging risks into their standard quantification methods. While institutions employ many different approaches, individual institutions may measure these risks in different ways. Quantification techniques have therefore not yet been fully and comprehensively incorporated into CROs' quantification toolkits.

There is a broad diversity of methodologies and analytics from a growing array of vendors providing ratings, incident probabilities, and risk scores in areas such as IT and cyber risk quantification and management. Similarly, supply chain and climate risk are witnessing an explosion of methodologies and lack of clarity in quantitative methods. These core methodologies range from expert judgement models to complicated blends of machine learning (ML), neural network models with standard statistical regression models, and significant use of graph theoretic frameworks.

The data foundations of risk management are rapidly evolving and are, in some ways, a double-edged sword. Within network management and analytics, while the ability to gather data on the state of networks has dramatically improved and there have been significant developments in the theoretical foundations of network and graph analysis, the techniques that organizations use remain diverse and at an early stage.

Just as VAR became the standard framework for risk measurement in the market and credit risk spaces, the industry needs a similar standardization of computational approaches in each of the major emerging risk verticals to complement the traditional qualitative/judgement-based approaches here.

About the research

This report reveals the results of research jointly conducted by Chartis and Tata Consultancy Services (TCS) into the views of banking, financial services, and insurance (BFSI) organizations on emerging risk types and the role of RiskTech. We surveyed 152 BFSI firms, predominantly large and mid-sized, with a diverse institutional mix across the BFSI spectrum. Our interview respondents included CEOs, board members, chief risk officers (CROs), heads of IT risk and a range of other risk and regulatory leads.

To support our quantitative survey, we also conducted more in-depth qualitative interviews of 54 institutions spread across banking, capital markets, and insurance. These institutions are distributed across Europe, North America, and Asia.

Key findings

- Regulations and business shifts are driving overall change. In some ways this is a truism. However, our survey and interviews suggest that institutions were responding to the interactions of a shifting business/technological environment and increasingly prescriptive regulations.
- The impact of digital transformation on the banking sector and the extent to which IT and cyber risks are increasingly intertwined with operational resilience and third-party risk was clearly confirmed in our interviews. Our interviewees felt that there would be increasing focus on the prescriptive definition of the boundaries of IT and operational risk. Of all the sectors, banking was at a higher risk of increasingly prescriptive regulations. Most participants felt that all financial sectors and many non-financial sectors would increasingly be regulated from an operational and IT risk perspective.
- IT and cyber risks are the most significant emerging risks faced by organizations.
- Technological and regulatory challenges are significant roadblocks to addressing emerging risks.
- The RiskTech market is mid-maturity with relatively high levels of adoption.
- Adoption levels are patchy across different emerging risk types and there is a clear divide between ‘mature’ and ‘early stage’ RiskTech adopters.
- Pilots or add-ons should not be conflated with technology that forms an integral part of the operating environment.
- RiskTech adoption will continue to mature, and investments will increase as companies look to harness continuous advances in technology and gain or maintain a competitive edge.

Key questions for institutions to answer include how ‘early stage’ adopters can catch up with their mature counterparts and how the market can progress towards maturity. The challenge for institutions lies in transitioning from perceiving RiskTech as an emerging sector to one where it is effectively leveraged across the whole of their organizations, thereby creating a more stable and robust technology and architectural landscape. Institutions need to overcome significant organizational barriers for these RiskTech investments to continue their path to maturity.

It is perhaps unsurprising that regulatory compliance, data security, and privacy are the biggest barriers to RiskTech adoption; 58% and 51% of institutions, respectively, view these as high barriers. Companies are also struggling with issues such as resistance to change, difficulties in integrating with existing systems, and infrastructure limitations.

Overall, mature RiskTech adopters perceive these issues to be far less significant barriers to adoption than organizations at an earlier stage, highlighting their greater comfort with RiskTech. Our in-depth qualitative interviews revealed that while regulatory requirements drive a considerable amount of spending, an even larger proportion is driven by the desire of companies to control, monitor, and understand the risks of their own operational infrastructure that is increasingly, and often totally, digital. Spending is being focused on automation, controls, and technological frameworks to ensure operational resilience, including operational infrastructure and process mapping and analysis, automatic aggregation and management of event data.

Cyber risk management is the single largest area of spending, with the fastest growing area being the technology layer required to analyze, control, and mitigate cyber risk. There is a strong focus on quantification, risk posture analysis, technology infrastructure analysis and mapping.

Spending on other emerging risk areas is also increasing. For example, in recent years there has been a veritable explosion of new supply chain risk management tools and a vast range of alternative data designed to allow a closer and more analytical examination of an organization’s supply chain dynamics.

2. The evolving risk landscape

Our surveys, both quantitative and qualitative, highlight a rapidly changing and evolving landscape. Our effort found that BFSI firms are rapidly increasing their investment in a range of non-financial risk management tools, but also revealed major roadblocks and deep structural challenges. As institutions (most specifically banks) have transformed their digital environments, in some instances, a whole set of new challenges have emerged.

Regulators' reaction to the evolving risk landscape has thus far been inconsistent regionally and has operated in fits and starts. This defines the industry response to the evolving technology landscape. Similarly, the industry response to the demands of cyber risk management has been in bursts and continues to be ad hoc.

Digital transformation

IT and cyber risks are the most significant emerging risks faced by organizations; over 80% of survey respondents view these risks as highly significant, particularly in terms of operational resilience and data privacy.

Digitalization is transforming every element of an institutions' business, creating a new operating environment and bringing in its wake a range of new and escalating IT and cybersecurity challenges. With cyber-attacks growing in both volume and sophistication, these risks pose significant threats to the integrity of financial systems, impacting customer data security, privacy and trust. These risks are further amplified by the interconnectedness of financial services with third-party providers.

As a result of the challenges caused by digitalization and the connected transformation in business practices, many firms globally and across industries have been struggling to maintain governance and business continuity. Firms are now placing a strong focus on digital resilience, which is becoming increasingly synonymous with overall business resilience.

Generative artificial intelligence (GenAI) also presents a range of emerging risks. In addition to cyber and fraud, there are concerns around data privacy, security, and bias in decision making. The rapid pace of artificial intelligence (AI) advancement poses challenges in regulatory compliance and ethical standards. There is an increasing recognition that GenAI tools are fundamentally probabilistic. Identifying and managing risks and establishing strong guardrails and structures is a complicated challenge.

Strategic risk

Strategic risks, including industry, technology, and business model disruption, are also a significant issue. Institutions are navigating the challenges posed by fintech start-ups, blockchain technologies, and changing consumer behaviors, requiring more personalized, digital-first experiences. Adapting to these changes requires not only investment in new technologies but also a reevaluation of traditional business models to stay relevant and competitive.

Supply chain and climate risks

The global nature of BFSI firms' supply chains, including third-party vendors and service providers, exposes firms to a wide range of risks. These include geopolitical tensions, regulatory changes, and operational vulnerabilities. In addition to physical and transition risks, institutions are also facing increasing regulatory and reporting requirements in ESG.

Emerging risks associated with the crypto market

A large minority (40%) of the institutions rate cryptocurrency as a significant emerging risk. Issues including regulatory uncertainty, market volatility and the risks associated with the custody and security of digital assets are prevalent. Moreover, the potential for cryptocurrencies to be used for money laundering and other illicit activities poses significant compliance and reputational risks.

Industry- and geography-specific risk trends

The regulatory environment in the European Union (EU) for non-financial risks is far more prescriptive. The Digital Operational Resilience Act (DORA) regulation on operational resilience, for example, is more well defined. Equally, the arrival of AI regulations has created a considerable amount of confusion as it is going to be a horizontal regulatory layer that cuts across industries and affects all institutions. This is in variance with other geographies where many of the regulatory issues around AI and GenAI are more likely to be tackled through the end models and the business line itself. In retail banking, for example, considering fair lending practices when leveraging AI tools in the lending context, considering investment advisory rules when using AI in an investment advisory context. In the EU, it remains to be seen whether AI will be considered as a separate class of modeling and technology altogether, or within the financial services space, there will be more business specific regulations first, with AI being pulled in. The current EU AI regulation suggests the first, i.e., AI as a block of separate regulations, which creates challenges for firms in the EU as well as those that happen to operate within the EU.

Looking across financial services, the banking and capital markets industries have undergone broad structural change, with digitalization, deep regulatory transformation, regionalization, and an increasing focus on integration with external platforms. As operationally intensive platforms, the need for banks and capital markets firms to quantify and analyze their operational risks, including cyber, IT, and third-party risk has become central.

Within insurance, the modelling environment is changing rapidly as risk analytics are increasingly converging with other financial sectors, such as banking, capital markets and asset management. This rapid convergence has created significant gaps in the insurance risk ecosystem. Even standard actuarial models are being upended and insurance fraud analytics are increasingly data-centric.

3. Roadblocks to addressing emerging risks

When it comes to addressing these emerging risks, institutions must overcome several issues:

Strong technological challenges. 71% of survey respondents identified technology as a top three challenge, and 27% perceive it to be their biggest obstacle. Institutions cited issues with upgrading and replacing their legacy technology infrastructure in the face of rapid technological changes, the vulnerabilities of their systems and controls to AI risks and cyber threats, and their continual struggles with data privacy and security. The data management infrastructure of an organization is another obstacle when it comes to GenAI.

Data: a central challenge and opportunity. Integral to the challenges are the issues surrounding data and data management. Alongside the cyber risks threatening data privacy and security, and the issues of regulatory and legal compliance, institutions are struggling with profound data challenges. These include the exponentially increasing volumes of data, the complexity of data environments (with fragmented data in siloed systems) and issues such as data quality, accessibility, costs, reporting and governance.

While digitalization has added to and created new vulnerabilities, it has also allowed organizations to dive deep into operational routines. The emergence and development of new digital tools and the capability to monitor and manage new platforms at a granular level is giving firms a new ability to control, survey, and analyze assets, employees, operations, and business processes in ways that would previously have been impossible. This continuous and granular data availability is transforming approaches to emerging risks, enabling institutions to identify, assess, measure, analyze, report, track, and model risk.

Expanded case management capabilities also allow for more detailed audit trails, all of which add to data volume and the associated challenges of data management. The technology required to organize and store data in the most appropriate format for both statistical and GenAI requirements is another huge structural challenge. As institutions move AI applications into production, they are increasingly realizing that data management is a far deeper issue than they had anticipated, requiring a significant amount of effort.

Along with the internal data challenges, companies in areas such as supply chain and climate risk are struggling with diverse data sets and processes and a lack of sufficiently detailed information. Integrating these diverse data sets requires sophisticated data management capabilities, the development of complex data models, and data transformation tools. For example, within supply chain risk management, while entity data is more easily available commercially, enrichment can be more complex, requiring integration of data from several sources into a single view. Both the interviews and survey data suggest that the data infrastructure is a central element of building out emerging risk areas. Most emerging risk areas (climate, IT, cyber, etc.) require management of large elements of data with complex structures and leveraging the broad selection of available data tools including graph and vector databases.

Managing climate risk frameworks is a good example of the centrality of the data challenges. The challenge of data management in emerging risk management is exemplified by the issues in handling climate risk.

Despite the challenges, however, the huge increase in commercial data and supporting technologies can enable institutions to perform more complex analytics and take multidimensional perspectives on a variety of risk areas. We have seen growth in all areas of data (such as credit, entity, climate, physical and product data), and in detailed operational data in a range of domains (including retail, property, general credit, energy, commodities and logistics). Moreover, the emergence of a well-defined commercial market in areas such as entity data in many (if not most) jurisdictions has allowed financial institutions to leverage these data sets, while highly detailed and enriched spatial data has enabled firms to overlay risks such as credit risk and physical/climate risk (from events such as wildfires, floods and hurricanes). The market for property data is a good example of how increased digitization and new technology have enabled more detailed analytics in emerging risk areas. This market is growing rapidly, and is composed of two distinct consumer groups: the PropTech market and the financial data services market. In both, the US is the most mature region, providing a global benchmark, although the UK, Europe and Japan are developing rapidly in a similar direction.

A lack of regulatory clarity. 20% of institutions cited this as the biggest challenge to address emerging risks, and 63% cited it as a top three challenge. In addition to a lack of regulatory clarity over the roles and responsibilities of institutions tackling these emerging risks, the frequency and pace of regulatory change and compliance requirements are also proving difficult to manage.

4. The state of technology adoption

The rapid evolution of technology brings new choices to institutions when addressing emerging risks. RiskTech adoption is therefore widespread; well over 90% of the companies we surveyed have adopted each of the major frameworks outlined below for at least one emerging risk. High-performance computing (HPC), ML, and AI, and GenAI/large language models (LLMs) are the most widely used technologies, having been deployed in some form by 97% of the institutions we surveyed.

When it comes to the level of adoption of these technologies, our research reveals that the RiskTech sector is mid-maturity. It is no longer about emerging frameworks or nascent technologies. Significant computational infrastructure is in place, with almost 60% of institutions reporting high levels of adoption of HPC for risk modelling. In addition, around four in ten institutions are reporting high levels of adoption of each of the remaining major technologies.

However, despite relatively high overall RiskTech usage, the deployment of these technologies is fragmented across risk types. As the most significant emerging risks, IT and cyber risks generally see high usage of RiskTech. However, only 'ML and AI' and 'Biometrics and Behavioral Analytics' are being used by more than half the institutions to address these risks.

In fact, across all risk types, there are only a handful of cases where more than 50% of institutions are using RiskTech to tackle a particular emerging risk. These technologies are therefore a long way from universal adoption.

It is also important to note that what constitutes 'high' levels of adoption is open to interpretation. Our in-depth discussions with organizations show that while 80-90% of institutions have piloted GenAI systems, very few organizations have made it a part of their operating environment, with only 10% claiming significant adoption. This contrasts with the quantitative survey, where 40% claim high levels of adoption.

In our experience, the focus on managing GenAI risks has ensured that while there have been a vast number of pilots, there have been far fewer projects. These have been typically restricted to lower risk areas that do not have overarching enterprise consequences, indicating that firms have some way to travel before the sector can be deemed mature.

Many GenAI projects are focused on consumer-type or individual-centric approaches, such as leveraging GenAI as a search engine or a document management capability. Adoption in these cases will only increase, albeit within certain guardrails and boundaries that firms will need to determine depending on their risk profile.

There is a much broader potential application of GenAI within operations and enterprise technologies. However, this is far more complicated, and adoption will be much slower. There are structural hurdles to overcome, including data privacy, security, accuracy, and confidence in results. It is more of a challenge to implement guardrails that reduce these risks to acceptable limits.

These two streams are therefore moving at different speeds and have very different technological, regulatory and organizational structure impacts and consequences. One is largely a technological issue, involving individual data and individual data management. The other has strong business process and risk tolerance dynamics, requiring institutions to determine how much probabilistic risk they can accept.

Our survey respondents have been segmented into 'Mature' and 'Early stage' RiskTech adopters to examine the characteristics of these firms and to identify the different types of challenges faced by these institutions as the RiskTech landscape continues to evolve.

- As firms continue to grapple with emerging risks and challenges, RiskTech adoption will continue to mature. Investment in RiskTech has already been substantial, and these levels of investment seem set to continue – 54% of institutions predict an increase in spending on emerging technologies over the next year and 39% expect annual budgets to remain the same. Only 6% plan to reduce spending.

- It is not simply a case of smaller institutions playing catch up with their larger counterparts. In fact, RiskTech spending will increase further among the largest institutions. 61% of those with assets of $100-500 billion and 57% of those with over $500 billion plan to increase RiskTech spend, compared to 50% of those with less than $100 billion in assets.

- The level of RiskTech adoption maturity also has no bearing on future investment plans; 55% of mature RiskTech adopters plan to increase their budget next year, compared to 53% of early-stage institutions. None of the mature firms plan to reduce spending next year, compared to almost one in ten of the early-stage institutions.

- RiskTech investments will continue to increase in response to rapid digitalization, the drive for efficiency and growth, and the need to strengthen cybersecurity. Spending is being driven by the imperative of upgrading existing solutions and a desire to harness continuous technological advances in an increasingly diverse and complicated risk landscape. While keeping pace with innovation demands, there is also a strong sense of needing to invest to keep up with, or stay ahead of, the competition.

- A central facet of spending will be consulting around the technological infrastructure that underpins risk management and analytics in different risk domains. According to our survey, half the institutions use external inputs from consultancy firms and market experts when making strategic decisions in the areas of risk management, RegTech, and RiskTech. Institutions are seeking external expertise, validation, and strategies for capabilities that they may not have in-house.

To conclude, emerging risk is rapidly evolving in the BFSI industry, with growing but still immature quantitative foundations and frameworks. The regulatory environment and significant management focus in most institutions has not yet led to convergence in methodologies, tools or techniques. In some segments, emerging risks are indeed business risk (i.e. the insurance sector). Therefore, emerging risk areas show signs of maturity (adoption, high importance and focus by senior executives) on one hand and signs of immaturity/evolution in their modeling/tools and techniques on the other.

Market Insight