Market Insight

TATA CONSULTANCY SERVICES

Chartis

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

Contents

1. Executive summary

Chartis and Tata Consultancy Services (TCS) conducted research to explore the views of banking, financial services, and insurance (BFSI) organizations on emerging risks and the role of RiskTech in mitigating them. Our report, *The role of RiskTech in effectively managing emerging risks and driving competitive edge*, has a detailed analysis of the research.

This report delves deeper into the capital markets results, exploring the experience and adoption levels of RiskTech among broker dealers and other capital markets institutions. It examines the particular challenges they face, and the actions needed to effectively manage emerging risks and gain a competitive edge.

About our research

We conducted a global survey of 152 BFSI firms in 2023, of which 56 were capital markets institutions. Interview respondents included CEOs, board members, chief risk officers (CROs), heads of IT risk and a range of other risk and regulatory leads, predominantly in large and mid-sized firms. The survey covered a diverse range of capital markets organizations, including broker dealers, asset managers, investment banks, and mutual funds.

To support our quantitative survey, we also conducted more in-depth qualitative interviews across Europe, North America, and Asia. This included interviews with 10 capital markets firms.

All BFSI firms, including capital markets firms, are grappling with increasingly dynamic and continually evolving risks. A tsunami of regulatory requirements and operational shifts have comprehensively reshaped the risk landscape. The operational resilience of capital markets firms is heavily reliant on third-party infrastructures, exposing firms to a wide range of risks and increasing the complexities of analyzing and understanding IT, cyber, and operational risk exposure.

Capital markets firms have undoubtedly come a long way in their response to these emerging risks through widespread RiskTech adoption. However, this remains patchy across emerging risk types, and the rapid pace of change, along with advances in technology mean that, despite progress, the RiskTech sector can still be described as relatively immature.

The challenge for firms lies in transitioning from a position where RiskTech is treated as an emerging sector to one where it is effectively leveraged across the organization, thereby creating a more stable and robust technology and architectural landscape.

As broker dealers and other capital markets firms progress towards effectively managing emerging risks, they must look at some key aspects, which include:

- Tackling the wide variety of quantitative techniques, alternative risk measures and frameworks to quantify and analyze their operational and emerging risks.
- Understanding the post-quantification steps, including building second order models; ensuring actionable steps based on risk quantification; and organizing security portfolios.
- Harnessing the wealth of granular data to weave cyber risk into the organizational risk fabric.
- Leveraging insurance analytic approaches to construct non-financial and analytics environments for the future.

Key survey findings: capital markets

- **IT and cyber risks are more pressing emerging risks for capital markets firms**: 86% of capital markets firms view IT and cyber as highly significant emerging risks (vs 77% for banks). Capital markets institutions, specifically broker dealers, are overly dependent on their technological platform and the technology ecosystem they operate in. They are heavily interconnected with third-party vendors, that often provide platforms for clients. These platforms require 24/7 operations.

- **Capital markets firms are struggling with technology and operating model challenges more than other financial services sectors when tackling emerging risks**: over a third of firms (34%) identified technology challenges as the top obstacle to addressing emerging risks (vs. 23% banks). Operating model challenges ranked as the second biggest obstacle overall (capital markets: 23% = top obstacle and 55% = top 3 obstacle; banks: 12% = top obstacle and 41% = top 3 obstacle).

- **The operational resilience of capital markets firms is heavily reliant on third-party infrastructures**: half of capital markets firms view supply chain as a significant emerging risk, the highest of the financial services sectors we surveyed. This risk dimension is the central issue from broker /dealers and capital markets institutions in general. Most of the business process are run on third-party solutions and supply chain risks are thus central to the risk framework of capital markets organizations.

- **RiskTech adoption is patchy across emerging risk types**. Capital markets firms are also lagging banking in their use of machine learning (ML) and artificial intelligence (AI) (54% vs 57% for banks) and generative artificial intelligence (GenAI) (36% vs 50% for banks) for IT and cyber risk. Broadly it is clear that use of ML is the highest in retail banking.

- **More capital markets firms are planning to increase spend on emerging technologies than other financial services sectors**: 57% of capital markets firms are predicting an increase in spends on emerging technologies over the next year and 38% expect annual budgets to remain the same. Only 5% plan to reduce spends. This however comes from a relatively lower base.

- **Capital markets firms are struggling more with their infrastructure than banks**: 36% of capital markets firms view their infrastructure limitations as a high barrier vs 21% of banks. 36% view the integration of RiskTech with their existing systems as a high barrier vs 26% of banks (when high and medium barriers are combined these figures are 73% vs 45% for banks, and 68% vs 51% for banks respectively). This is simply the function of the fact that technology infrastructure for capital markets is more central and often externalized.

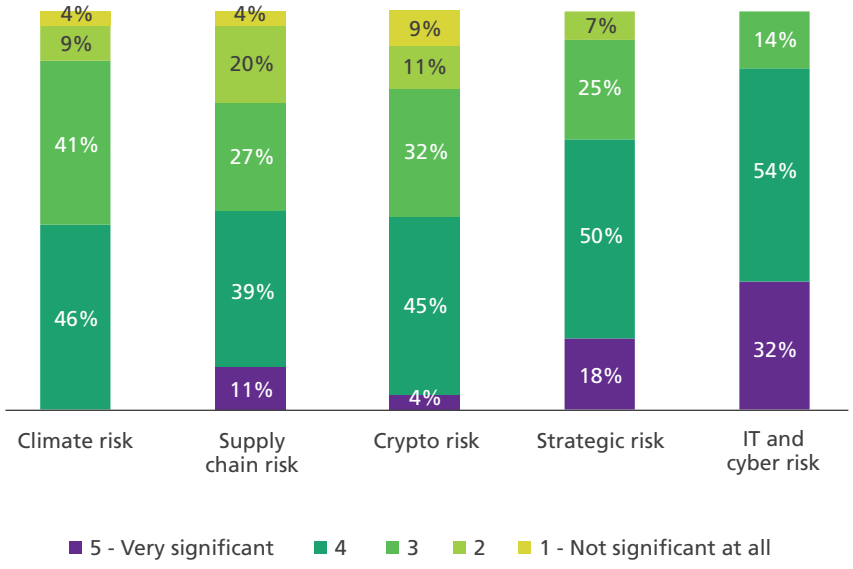
- **Capital markets firms should focus on increasing RiskTech KPIs**: Capital markets firms are lagging banks in data quality and integration KPIs (64% vs 70% in banks, another natural consequence of externalization of the platform.

2. Findings in detail

The evolving risk landscape: capital markets

Capital markets firms are grappling with increasingly dynamic and continually evolving risks. Our survey examines their views on the different types of emerging risks.

Q5 State the significance of emerging risks within your organization.



IT and cyber risks are inextricably linked with third-party risk

Among our survey respondents, broker dealers and other capital markets institutions had the strongest response to IT and cyber risks; 86% of capital markets firms view these risks as highly significant.

Like banks, capital markets firms have been transformed by a wave of digitalization that is affecting every element of their business, creating a new operating environment along with a range of new and escalating IT and cybersecurity challenges.

Capital markets business models are different to banks; their overarching technical architectures are generally simpler. However, broker dealers, particularly, are often part of broader networks, integrated into exchange systems, clearing houses, and transaction management networks. In addition to these market infrastructures, significant outsourcing of operating infrastructure means that capital markets firms rely on third parties far more than banks.

Financial institutions are now placing a strong focus on digital resilience, which is increasingly synonymous with overall business resilience. For capital markets firms, as a considerable portion of their operational resilience relies on third-party infrastructures, the operational resilience, IT and cyber risks of the networks in which they operate often outweigh the concerns surrounding their own internal IT risk and resilience. Concerns about their internal systems often focus on the middleware and messaging infrastructure that connects them to these mutualized operating infrastructures and market tools.

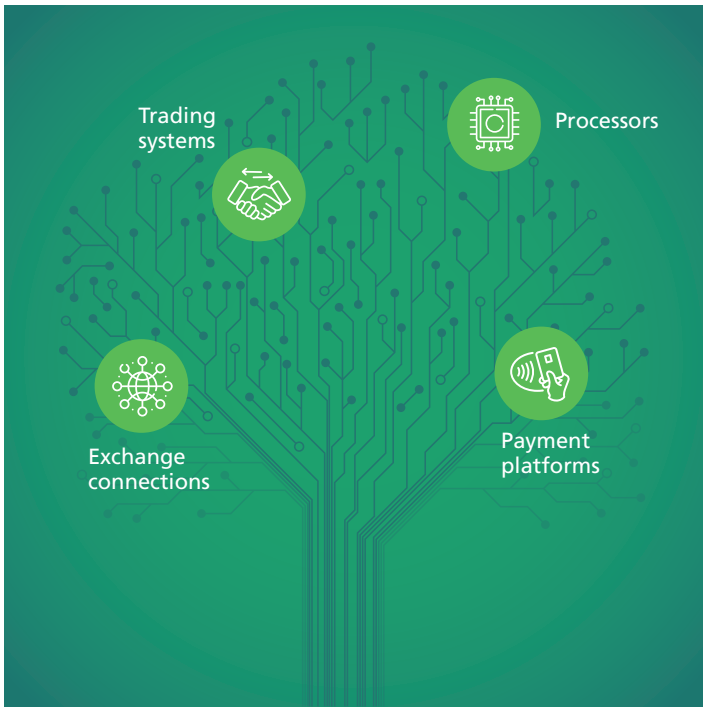
This interconnectedness with third-party providers and the global nature of financial institutions' supply chains exposes firms to a wide range of risks. Half of capital markets firms view supply chain as a highly significant emerging risk, highest among the financial services sectors we surveyed.

From a capital markets perspective, most supply chain risk comes from software and IT infrastructure and service providers along with other network elements such as exchanges and trading networks. In this respect, third-party risks are somewhat more concentrated compared to manufacturers, energy providers or healthcare service providers. However, the complexities of analyzing software and IT infrastructure risks are far greater, as these organizations may have fourth- or fifth-party components which are almost invisible from the outset and require close cooperation with suppliers to enable clear understanding of those risks.

These third-, fourth-, and fifth-party challenges are enormously complex, particularly for broker dealers. Our qualitative interviews reveal that many view tackling these challenges as more akin to magic, than an art or science. The move to the cloud and to managed services has 'meta-sized' this problem, dramatically transforming the difficult into the impossible, as software vendors move to cloud, SaaS, and managed services.

As seen with the European Union's (EU) Digital Operational Resilience Act (DORA), regulators are becoming increasingly prescriptive about the challenges of supply chain risks. There is increased regulatory focus on the third-party risk in software, which includes security aspects as well as legal and control risks in open-source software.

Third-party and fourth-party risks, extension beyond organizational risks



Other emerging risks

While IT and cyber risks are often seen as central and existential from a capital markets perspective, other emerging risk areas are also significant and salient:

- Strategic risk, including industry, technology, and business model disruption, is a hugely significant issue; 68% of capital markets firms viewed strategic risks as significant.

- Almost half (49%) of capital markets institutions rate cryptocurrency as a significant emerging risk.

Climate risk is another increasingly pressing emerging risk identified by capital markets firms, while this does not resonate as strongly as it does for banks, just under half (46%) rate it as a significant issue. Asset managers have sold significant sustainability-linked products which exposes them to the dynamics of sustainability compliance.

The regulatory environment around climate risk is also lacking in clarity. Regulators are encouraging financial institutions to take climate risk into account in their decision-making. However, there is no single, clear, prescriptive model for how climate risks should be incorporated into credit analysis – or, for that matter, to assess their impact on any part of the capital structure of the associated institution. Whether we look at corporate bonds or focus on equity instruments, the translation is complex and uncertain at best. There is also no clarity on which data sets to use or how to use them. All of this leaves capital markets firms in an uncertain position, particularly with the increasingly complicated politics surrounding climate risk.

Roadblocks to addressing emerging risks: capital markets

When it comes to addressing these emerging risks, capital markets firms seem to be struggling more with **technological challenges** than other financial services sectors; 34% perceive it to be their biggest obstacle (compared to 23% of banks) and overall 73% identify technology to be a top three challenge, compared to 68% of banks. Issues with upgrading and replacing their legacy technology infrastructure in the face of rapid technological changes seem to be a significant issue for capital markets firms.

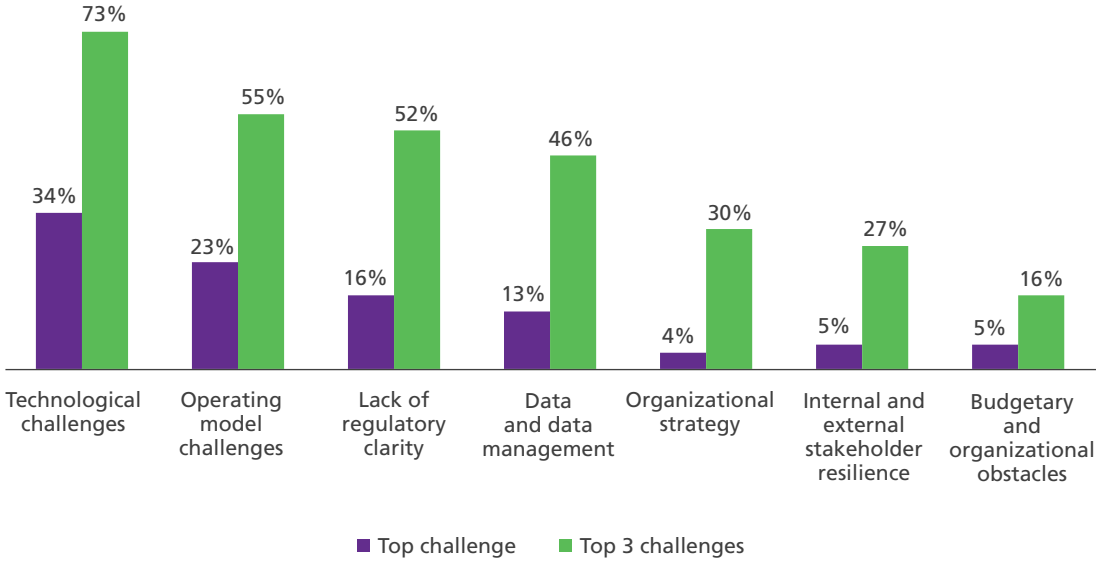
Operating model challenges are the second biggest obstacle for capital markets firms, with 23% citing it as the top challenge, compared to only 12% of banks, and 55% viewing it as one of their top three challenges, compared to 41% of banks. In addition to the mutualized operating infrastructure challenges outlined above, operating model issues such as operating inefficiencies, lack of integration between risk functions and operations, and insufficient agility, clarity, alignment, ownership or accountability within different functions are affecting the industry.

Data: a central challenge and opportunity

For broker dealers and other capital markets firms, the issues surrounding data and data management are another significant challenge; 46% of capital markets firms cited it as a top three challenge. Alongside cyber risks threatening data privacy and security, and the issues of regulatory and legal compliance, capital markets institutions, like all financial 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, cost, reporting and governance.

In addition to internal data challenges, capital markets firms must contend with diverse emerging risk data sets and processes, along with 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.

Q6 What are the top 3 key challenges your organization faces while addressing the emerging risks?



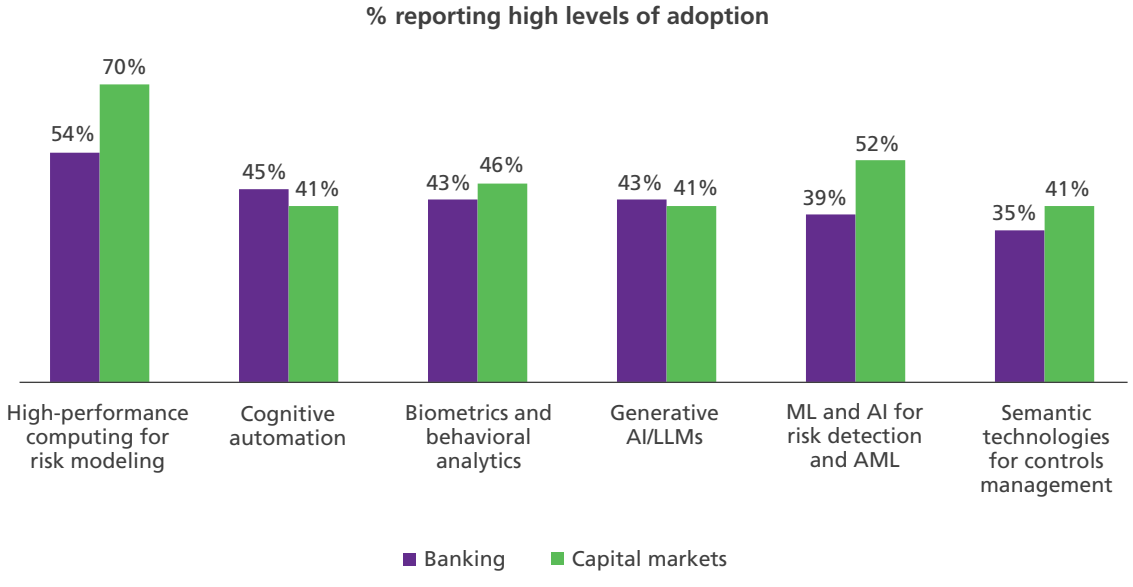
The adoption of RiskTech: capital markets

In many respects, capital markets firms are leading the financial services sector in their use of RiskTech. All the capital markets firms in our survey are using the major emerging technologies in some form, except for the 2% not using biometrics and behavioral analytics.

When it comes to the level of adoption of these technologies, significant computational infrastructure is in place, with 70% of capital markets institutions reporting high levels of adoption for high-performance computing (HPC) for risk modeling. In addition, over half are reporting high levels of adoption for ML and AI, and around four in ten institutions are reporting high levels of adoption of each of the remaining major technologies.

Q10: State the level of adoption of the following RiskTech and RegTech frameworks by your organization.

	High	Medium	Low	N/A
High-performance computing for risk modeling	70%	16%	14%	0%
ML and AI for risk detection and AML	52%	25%	23%	0%
Biometrics and behavioral analytics	46%	41%	11%	2%
Generative AI/LLMs	41%	43%	16%	0%
Cognitive automation	41%	43%	16%	0%
Semantic technologies for controls management	41%	39%	20%	0%



Deployment

However, despite relatively high overall RiskTech usage, only just over a third (36%) of broker dealers and other capital markets firms in our survey are classified as 'mature' adopters (defined as those ranking their levels of adoption as high (4,5) across more than three technologies).

The deployment of these technologies is also fragmented across risk types. As the most significant emerging risk, RiskTech usage is generally highest for addressing IT and cyber risks. Yet only 'ML and AI' and 'Biometrics and Behavioral Analytics' are being used by more than half of institutions to address these risks.

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

It is also worth noting that within IT and cyber risk, capital markets firms are falling behind banking in their use of ML and AI (54% vs 57% for banks) and generative artificial intelligence (GenAI) (36% vs 50% for banks). However, this should be considered within the context of our qualitative research findings, which reveals that pilots and add-ons to existing technologies are far more common than full adoption.

In terms of strategic risk, use cases would include risk associated with areas such as tech replacement/ investment, M&As, reputation, ESG, geopolitical issues, etc.

Q7 Which of these technologies has your organization adopted to address each of these risks?

	Climate risk	Supply chain risk	Crypto risk	Strategic risk	IT and cyber risk
High-performance computing for risk modeling	41%	52%	66%	61%	41%
Cognitive automation	48%	48%	46%	36%	46%
Biometrics and behavioral analytics	45%	27%	32%	29%	64%
Generative AI/LLMs	18%	21%	18%	21%	36%
ML and AI for risk detection and AML	29%	27%	21%	39%	54%
Semantic technologies for controls management	29%	21%	20%	16%	46%

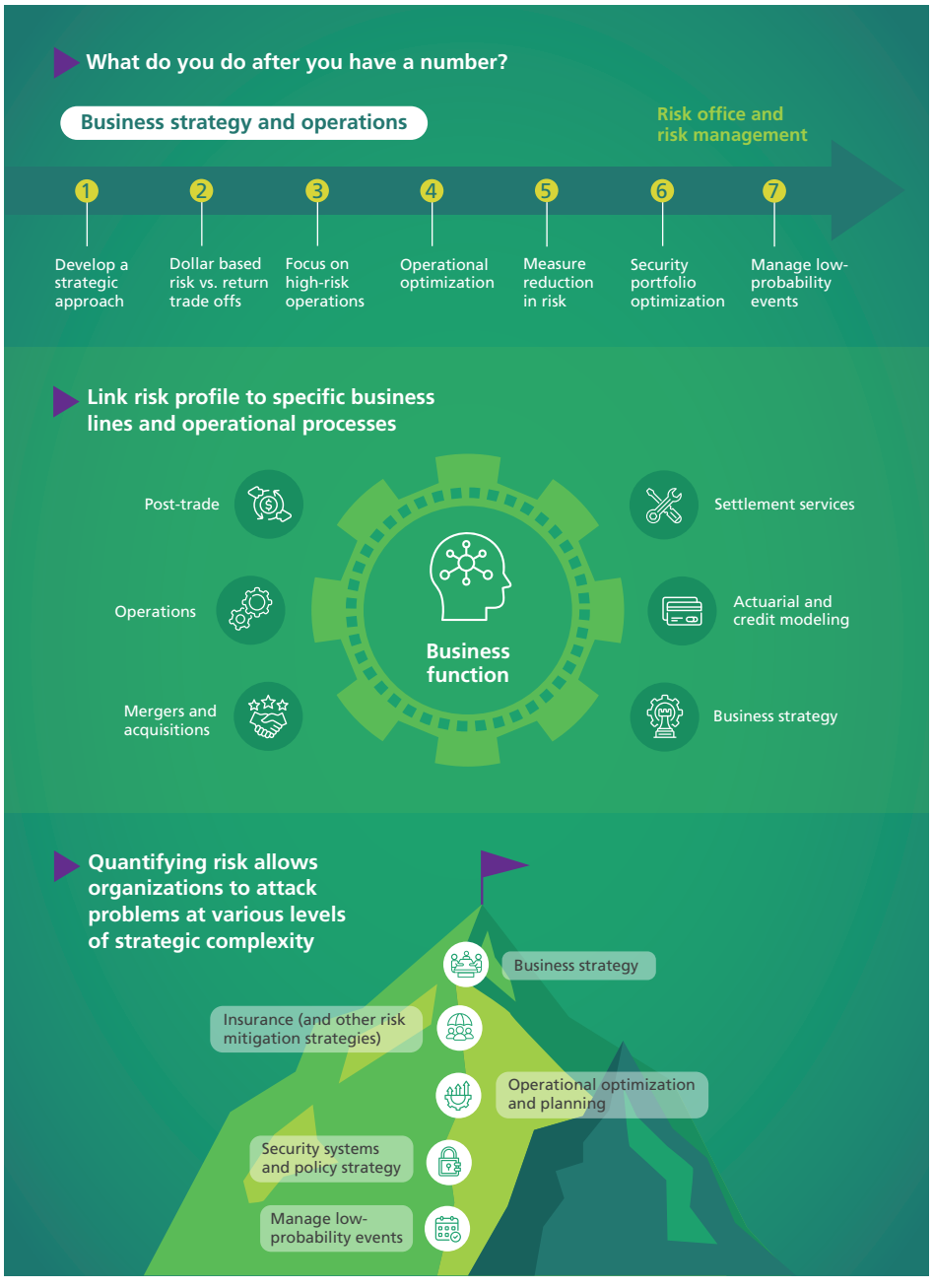
Note: Colour coding shows comparison vs capital markets (PURPLE = behind, GREEN = equal to or higher)

Emerging risks: from historical roots to a core role

An influx of regulations and changing operational practices mean 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 performing a core role for successful capital markets firms. Its functions and sub-categories have expanded dramatically and are now widely linked to the risk function on one side and the technology function on the other. The control function now has a broader and more strategic role, focused on business optimization and tightly coupled with frontline operations.

In addition to the steps outlined in our overarching BFSI report, we list the following key conclusions for capital markets firms.

Post-quantification, capital markets firms need to tackle next steps



The overwhelming majority of capital markets firms are still struggling with major methodological challenges. One of the biggest hurdles to overcome is the wide variety of quantitative techniques, alternative risk measures, and frameworks for emerging risk.

The increasing diversity of methodologies and vendors, along with lack of regulatory focus or clarity on specific risk measures, mean that organizations are struggling to incorporate emerging risks into their standard quantification methods and face difficulties in adding these data points into actual operational activities.

Quantifying risk allows organizations to attack problems at various levels of strategic complexity. However, for most capital markets firms there is a further clear challenge around the steps to take once that quantification has taken place. In particular:

- How to build second order models.
- How to ensure actionable steps can be taken based on risk quantification.
- How to organize security portfolios.

Similarly, capital markets firms need to tackle central questions around the appropriate nature of quantification at different levels of the organization, and at what point in the organization they may be focusing on risk appetite calculations.

CRITICAL TECHNOLOGIES

- Vector databases for high-performance analytics – including ML.
- Messaging and lightweight data management infrastructure.
- Broker dealers are major consumers of third-party services and risk-as-a-service.
- Third-party risk is a significant challenge.

Harnessing the wealth of granular data to weave cyber risk into the organizational risk fabric

With the proliferation of systems, along with vast and ever-increasing amounts of data, capital markets firms need strong data management and governance. They also need to understand the measures and metrics to use in determining what constitutes good cyber security. Huge volumes of data are available in internal networks, but the key challenge for capital markets firms is to make sensible decisions based on this data.

Analyzing the data and distributing actionable insights to different parts of the organization with appropriate risk analysis is a key challenge. Almost 80% of our qualitative interviewees feel they have not yet woven the technical analysis of this data into the overarching framework of their organization, and they certainly have not yet woven it into commercial decision making or operational analysis.

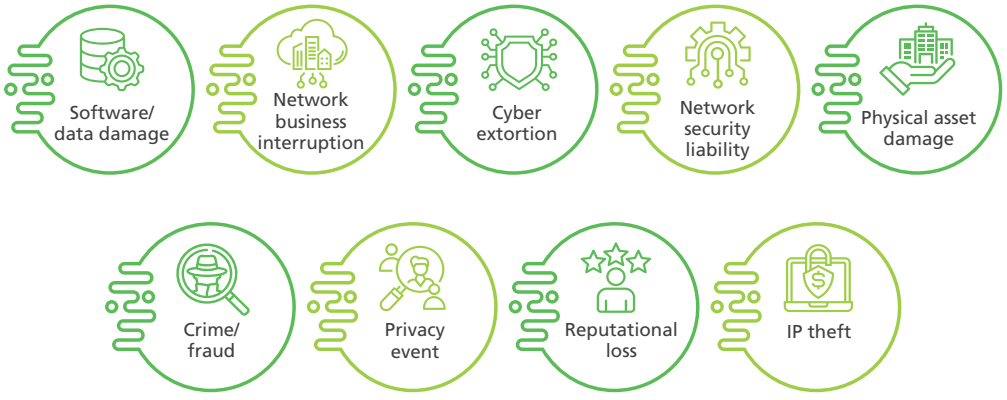
Insurance analytics provide a model for integrating cyber risks into business strategy

For capital markets firms, there is an increasing consensus that the mechanisms of insurance underwriting and actuarial practices can play a significant role in the development of analytical frameworks in the near future.

The analytics approach developed within financial markets, such as market risk and credit risk models, are not always entirely appropriate to addressing emerging risks. They often do not factor in some of the key structural issues that are central to non-financial risk modelling. There is an increasing consensus that capital markets firms can leverage more traditional insurance approaches to help in the construction of non-financial risk and analytics environments for the future.

With the evolution of non-financial risk, we expect the emergence of a convergent framework that incorporates significant elements and approaches from traditional financial modelling, such as risk management measures (for example, VaR and expected shortfall) but marries these with actuarial measures. This converged risk framework is the long-term approach that holds significant promise for modeling cyber and other emerging risks.

A variety of cyber and IT risks impact capital markets institutions

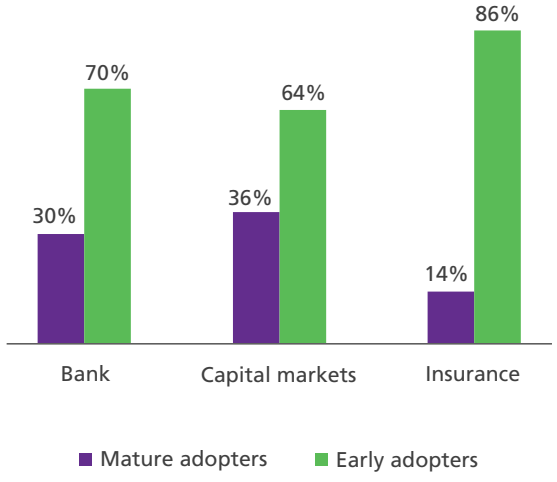


Conclusion

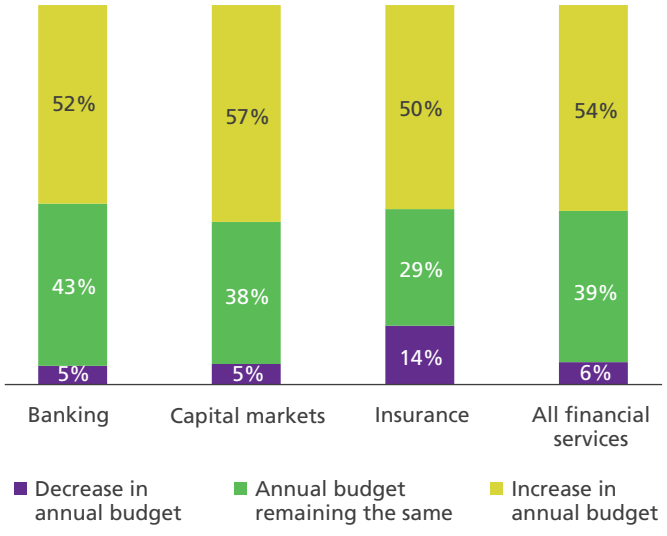
Capital markets institutions are struggling to comply with varied types of emerging risks along with the compliance required for the tsunami of regulatory requirements. The impact on capital market players is somewhat uncertain, because they operate in a complex ecosystem and the regulatory incidence across the entire value chain is not necessarily well-defined. And while the notion of responsilibility is also uncertain, some segments (such as asset management) have seen far more impact, given that they have a large set of products that are directly impacted by ESG/environmental issues.

3. Appendix: Capital markets graphics/data for reference

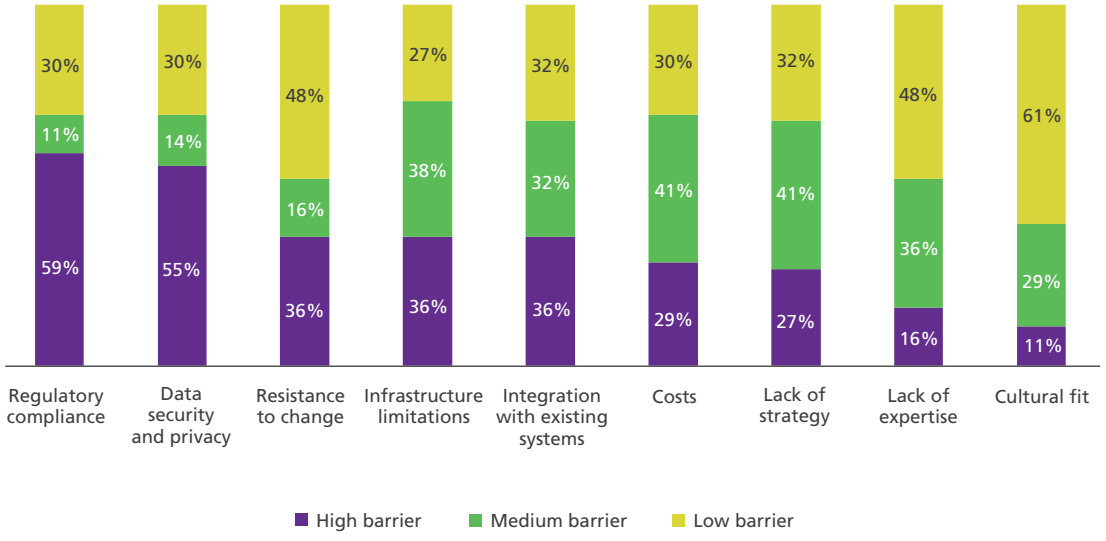
RiskTech/RegTech technologies: mature vs early adopters



Q9 How do you expect spending on emerging technologies to change over the next year?



Q11: Rate the relevant organizational barriers blocking institutions like yours from adopting RiskTech and RegTech technologies.



Q10: What are the KPIs for RiskTech and RegTech frameworks your institution uses?

	Primary institution type			
	Broker dealers and other capital market institutions	Insurance company	Banks	TOTAL
Base: All respondents	**56**	**14**	**82**	**152**
Regulatory compliance	73%	86%	71%	73%
Data quality and integration	64%	64%	70%	67%
Real-time/actionable insights	57%	50%	48%	51%
Efficiency and cost saving	50%	57%	35%	43%
System performance	41%	64%	37%	41%
Better customer experience	29%	50%	35%	34%
We do not use KPIs for RiskTech and RegTech	–	–	4%	2%
Other	–	7%	–	1%

Market Insight

TATA CONSULTANCY SERVICES

Chartis