Market Insight

TATA CONSULTANCY SERVICES

Chartis

Banking: 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) 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 banking results, exploring the experience and adoption levels of RiskTech among banks and financial institutions. It examines the particular challenges faced and the actions needed to effectively manage emerging risks and gain a competitive edge.

About the research

We conducted a global survey of 152 BFSI firms in 2023, of which 82 were banks. 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 banking organizations, including retail, corporate, private, and universal banks.

To support our quantitative survey, we also conducted more in-depth qualitative interviews across Europe, North America, and Asia. This included interviews with 32 banks.

All BFSI firms, including banks, are grappling with increasingly dynamic and continually evolving risks. The banking industry has undergone broad structural change, marked by digitalization, deep regulatory transformation, regionalization, and increasing focus on integration with external platforms. This has comprehensively reshaped the risk landscape. In response, banks and financial institutions have undoubtedly come a long way with widespread RiskTech adoption.

However, adoption remains patchy across emerging risk types. 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 banks 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. In the context of cybersecurity and risk management, organizing security portfolios involves structuring and aligning security initiatives, tools, and investments to safeguard firms from threats and vulnerabilities. This process usually includes risk assessment, prioritization of assets, selection of appropriate controls, and continuous monitoring of security performance.
- Harnessing the wealth of granular data to weave cyber risk into the organizational risk fabric
- Leveraging approaches to construct non-financial and analytics environments for the future.

Market Insight

Key survey findings: banking

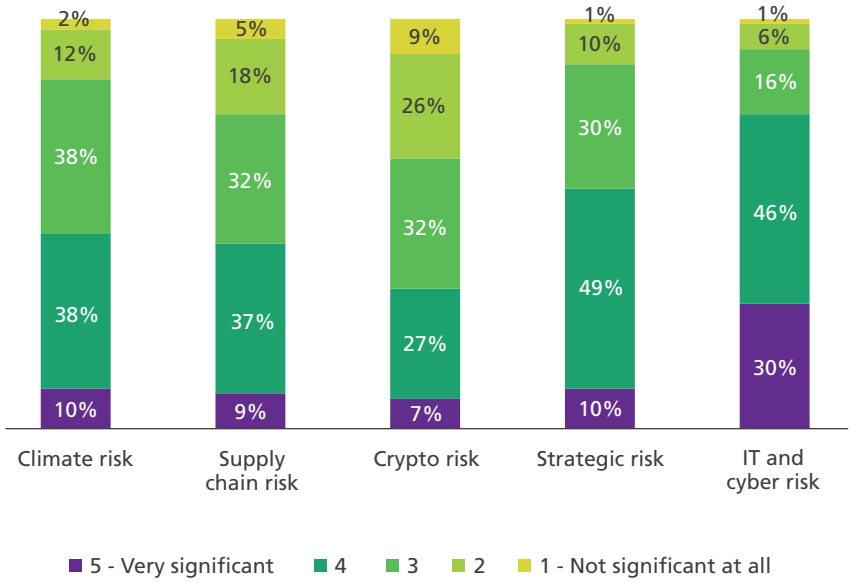
- **Banks view IT and cyber as the most significant emerging risks**: 77% of banks view IT and cyber as highly significant. Digital transformation has created a raft of new vulnerabilities and placed a new lens on operational resilience.
- **Banking supply chain risks are under increased focus from regulators** and are closely linked to IT, cyber, and operational risk.
- **Climate risk is an increasingly pressing emerging risk**: Banks believe that today's methodologies and data are not yet robust nor widely available enough to enable efficient credit-based decisions for most asset classes based on climate risk indicators. While risk analytics for climate events (such as floods or wildfires) are widely available, translating these into specific physical damage is a challenge. Harder still is moving the results further up the value chain to determine credit or market risk. While event data can often be well-defined for the short term (one to three years), assets are exposed to these risks for a much longer period. Determining how this will affect a corporate entity's capital structure adds further complexity. Banks would prefer a standardized methodology and far more detailed physical and organizational data to effectively analyze the impact of climate risk on their clients' financials.
- **While technological challenges are a significant roadblock to addressing emerging risks, banks are struggling with a lack of regulatory clarity more than other financial services sectors**: 71% of banks cited a lack of regulatory clarity as a top three challenge to tackling emerging risks, making it the most significant overall obstacle. Banks argued that without regulatory clarity it was too difficult to incorporate emerge risks in their decision-making and risk analytics.
- **Although not as far along in their RiskTech journey as capital markets firms**, the banking RiskTech market is mid-maturity, with relatively high levels of adoption. Capital markets institutions received significant support and were anchored by expectations and RiskTech definitions from their ecosystem.
- **GenAI/large language models (LLMs) are the most widespread RiskTech used by banks**: LLMs have diffused through the industry at a rapid pace. However, the details of this diffusion are more complex. The overwhelming majority of banks surveyed (98%) report some form of 'deployment', but in these instances this largely entails either trials or lightweight deployments of co-pilots/search tools. Fully industrialized production-ready platforms outside these categories are rare. Indeed, many institutions are becoming increasingly focused on model validation issues with these tools.
- **Banks are lagging capital markets in the use of biometrics and behavioral analytics**, particularly when it comes to IT and cyber risks; 49% of banks are deploying these technologies, compared to 64% of capital markets firms. However, of those banks that have adopted these technologies, the total expenditure is substantially higher. As mentioned before, capital markets focused institutions have lighter platforms, are more dependent on outsourcing, and adoption of comparable technology has much lower impact.
- **Banks are also behind in their overall use of machine learning (ML) and artificial intelligence (AI)**: 39% of banks report using these technologies in some form, compared to 52% of capital markets firms.
- **Bank spend on emerging technologies will continue to increase**: 52% of banks predicted an increase in spends on emerging technologies over the next year and 43% expected annual budgets to remain the same. Only 5% plan to reduce spends.
- **Regulatory compliance and data security and privacy are the biggest barriers to RiskTech and RegTech adoption**: 56% and 49% of banks respectively view these as high barriers.
- **KPIs**: Banks are leading in their use of data quality and integration of key performance indicators (KPIs) (70%), but are lagging in real-time actionable insights (46% vs 57% of capital markets firms) and efficiency and cost saving (35% vs 50% of capital markets firms).

2. Findings in detail

The evolving risk landscape: banking

Banks 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.



Digital transformation, operational resilience, and supply chain risk

For most commercial and retail banks, IT and cyber are the primary emerging risks they are currently tackling; 30% of respondents view these risks as very significant.

The wave of digitalization that has taken place over the last decade is transforming banks, creating a new operating environment and bringing in its wake a range of new and escalating IT, cybersecurity and privacy challenges.

Banks have always been reliant on their core IT infrastructure for operations and business activity. However, rapid digitalization has meant that they have become even more reliant on their core digital infrastructure. Firms are now placing a strong focus on digital resilience, which is becoming increasingly synonymous with overall operational resilience.

It is also important to note the rapidly shifting regulatory environment. Central banks and banking regulators, including the Bank of England and the European Banking Authority, are increasingly focused on the operational resilience of banking infrastructures. According to many bankers, the European Union's (EU) Digital Operational Resilience Act (DORA), is setting the overarching standard and benchmark for operational resilience regulations around the world.

The interconnectedness of financial services with third-party providers and the global nature of financial institutions' supply chains, particularly following digitalization, exposes firms to a wide range of risks and further amplifies their IT, cyber, and operational risks.

From a banking perspective, most supply chain risk comes from software and IT infrastructure and service providers. In this respect, third-party risks are somewhat more concentrated compared to manufacturers, energy providers or healthcare service providers. Retail banks are arguably most vulnerable to these risks. For example, while small regional banks in the USA are traditionally operationally light compared to their international counterparts, vulnerabilities exist in their outsourced ecosystems.

However, the complexities of analyzing software and IT infrastructure risks are far greater for financial institutions, 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.

As seen with DORA, there is increased regulatory focus on the third-party risk in software, which includes security aspects as well as legal and control risk in open-source software.

With increasingly prescriptive regulators, banks therefore need to look at their IT, cyber, operational and supply chain risk from both a regulatory perspective, considering how regulators would react to specific context situations in architectures, and an operational risk perspective, considering their own internal resilience.

While IT and cyber risk are often seen as central and existential from a bank's perspective, other risk areas and control points are still significant and salient. Strategic risk, including industry, technology and business model disruption, is a hugely important issue; viewed as significant by more than half of banks.

Climate risks

Climate risk is another increasingly pressing emerging risk that is identified by banks; about half viewed it as a considerably significant emerging risk, a higher proportion than capital markets and insurance firms.

In addition to physical and transition risks, banks are also facing increasing regulatory and reporting requirements in ESG. Yet, the regulatory environment around climate risk is lacking in clarity. As a result, climate risk occupies a relatively complex situation and context within banks. 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. There is also no clarity on which data sets to use or how to use them. All of this leaves banks in an uncertain position, particularly with the increasingly complicated politics surrounding climate risk.

Roadblocks to addressing emerging risks: banking

When it comes to addressing these emerging risks, like other financial institutions, banks are **facing strong technological challenges**. 68% of survey respondents identified technology as a top three challenge, and 23% perceive it to be their biggest obstacle. Issues with upgrading and replacing legacy technology infrastructure, the vulnerabilities of systems and controls around AI risks and cyber threats and struggles with data privacy and security are all significant issues for banks.

However, **a lack of regulatory clarity** is affecting banks more than other financial sectors; 23% of banks cited this as the biggest challenge to addressing emerging risks, equal to the technology challenges they are facing. 71% cited it as a top three challenge, making it the most significant overall obstacle banks feel they are facing. This highlights not only the difficulties banks are having in managing the frequency and pace of regulatory change and compliance requirements, but also a lack of regulatory clarity over the roles and responsibilities of banks in tackling these emerging risks.

As mentioned above, banks are struggling with a lack of clarity on the risks and risk measures that regulators want to be considered for non-financial risks. There are no standardized or easily calculable risk measures, in contrast with the well-defined nature of the regulatory framework for financial risks. In addition, there is a significant lack of clarity over the use of AI. There is considerable divergence in approach among different regulators, for example, the regulatory strategies adopted by the EU are currently out of line with those adopted by the US. Overall, these differences center around whether AI tools are just another statistical model, or whether they are a fundamentally different type of technology. This differing approach among regulators requires institutions to adopt geography- and industry-specific approaches, which in turn is hampering growth in capability in these areas.

Data: a central challenge and opportunity

For banks, the issues surrounding data and data management are another significant challenge, with 22% citing it as their biggest roadblock. Alongside cyber risks threatening data privacy and security and the issues of regulatory and legal compliance, banks, 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.

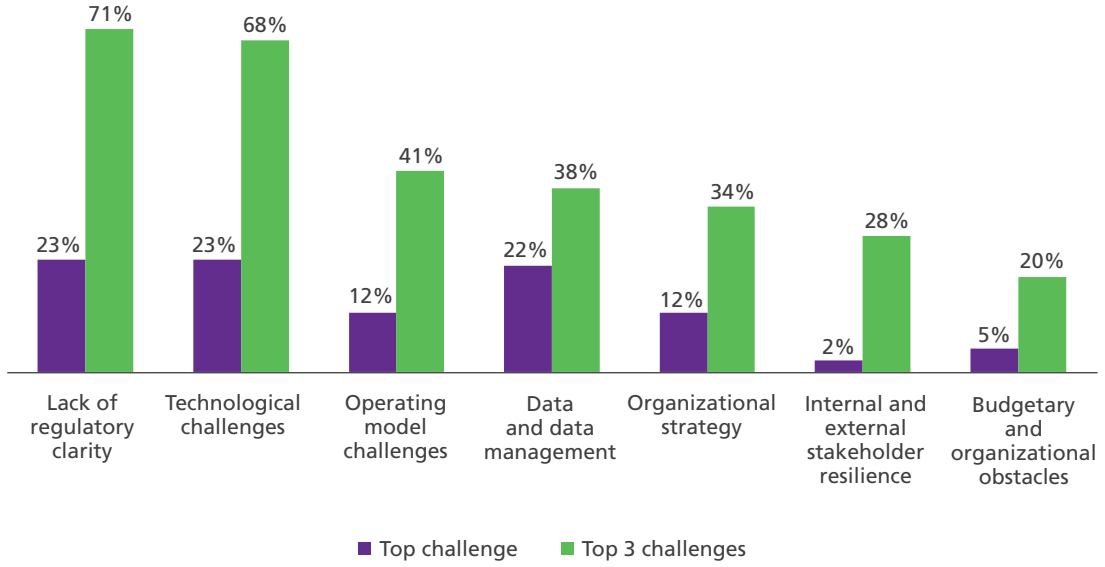
In addition to internal data challenges, banks are struggling with diverse emerging risk data sets and processes, along with a lack of sufficiently detailed information. Integrating these diverse data sets requires sophisticated data management capabilities, the development of complex data models, and data transformation tools.

Nevertheless, despite these challenges, banks are in the middle of a huge increase in commercial credit-focused activity, with more varied, structured and derived data available on areas such as:

- The prepayment details of various mortgage pools.
- Detailed transactional histories of businesses and consumers.
- Operational details of businesses.
- Supply chain details.
- Third-party overviews of businesses' IT and cyber risk (and their cyber risk posture over time).

In addition to structured data, firms can now access vast pools of geographic data and other alternative data sets of varying levels of analytical traceability. Indeed, the growth of spatial data has been revolutionary.

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



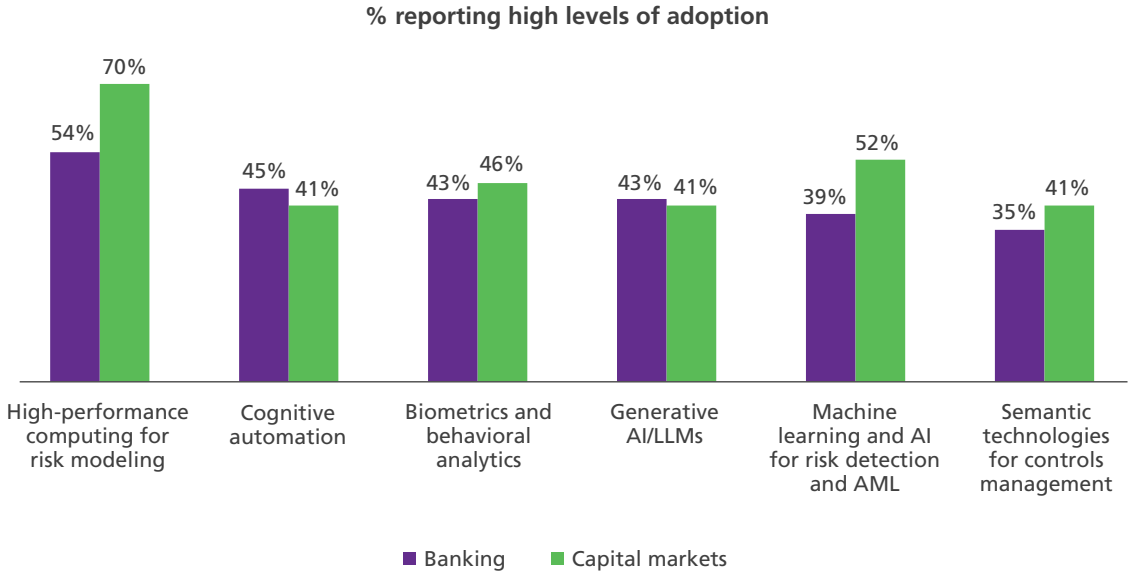
The adoption of RiskTech: banking

In addressing emerging risks, while banks are not as far along in their RiskTech journey as capital markets firms, digital technology adoption is widespread. AI +GenAI/LLMs are the most widely used, with 98% of banks reporting having deployed these technologies in some form. High performance computing (HPC) and ML and AI are also widely deployed technologies.

When it comes to the level of adoption of these technologies, significant computational infrastructure is in place, with 54% of banks reporting high levels of adoption for HPC. In addition, around four in ten banks 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	54%	27%	16%	4%
Cognitive automation	45%	29%	20%	6%
Biometrics and behavioral analytics	43%	34%	18%	5%
Generative AI/LLMs	43%	30%	24%	2%
Machine learning and AI for risk detection and AML	39%	30%	27%	4%
Semantic technologies for controls management	35%	35%	21%	9%



Deployment

However, despite relatively high overall RiskTech usage, only 30% of banks 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).

Banks are lagging capital markets firms in key areas such as ML and AI. The deployment of these technologies is also fragmented across risk types. As the most significant emerging risk, RiskTech usage among banks is generally highest for addressing IT and cyber risks. Yet only 'ML and AI' is being used by more than half of banks to address these risks.

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

Banks are also falling behind in the use of biometrics and behavioral analytics, particularly when it comes to IT and cyber risks, with 49% deploying these technologies, compared to 64% of capital markets firms. This is partly due to the complexity of analyzing the behavior of retail banking customers or small and medium enterprises (SMEs) in comparison to the transactional history of capital markets institutions, which are far more traceable and analyzable. In addition, there is a structural dynamic, as many capital markets institutions have behavioral analytics embedded into their traded instruments.

Market Insight

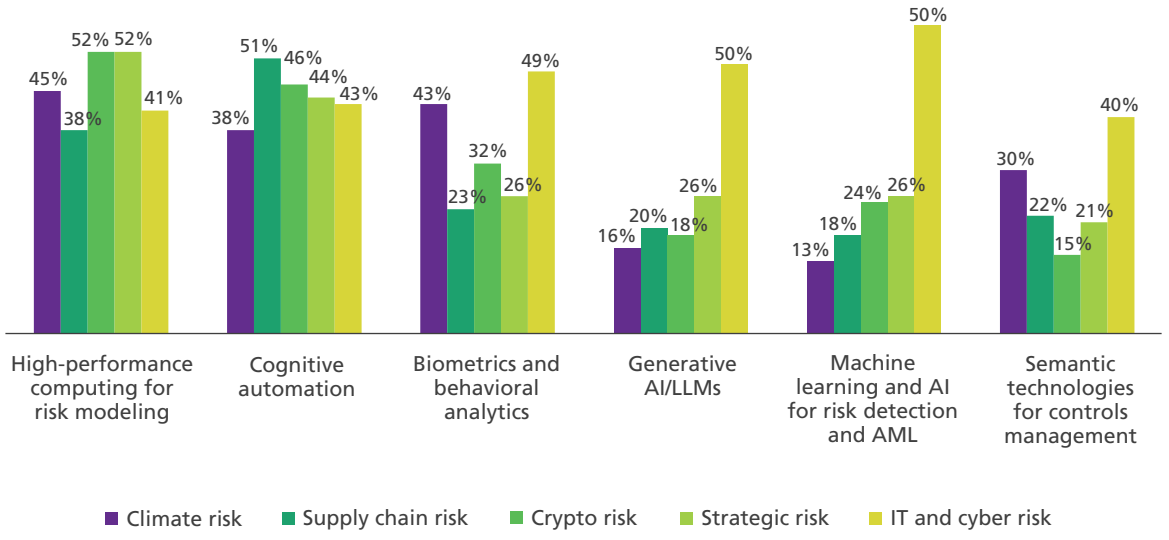
It is worth noting that banks are more advanced in their use of GenAI/LLMs than other financial institutions – 50% are using these technologies to tackle IT and cyber risks, compared to 36% of capital market firms. Retail banks are particularly focused on cyber risk. The deeper levels of digital transformation, and the fact that retail banks are significant targets for cyber criminals, mean that the cyber risk infrastructure and technologies guarding the perimeters of these organizations are generally more advanced than for capital markets firms.

However, it is also important to note the findings from our qualitative survey, which reveals that pilots and add-ons to existing technology are far more common than full adoption, indicating that banks have some way to travel before the sector can be deemed mature.

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	45%	38%	52%	52%	41%
Cognitive automation	38%	51%	46%	44%	43%
Biometrics and behavioral analytics	43%	23%	32%	26%	49%
Generative AI/LLMs	16%	20%	18%	26%	50%
Machine learning and AI for risk detection and AML	13%	18%	24%	26%	57%
Semantic technologies for controls management	30%	22%	15%	21%	40%

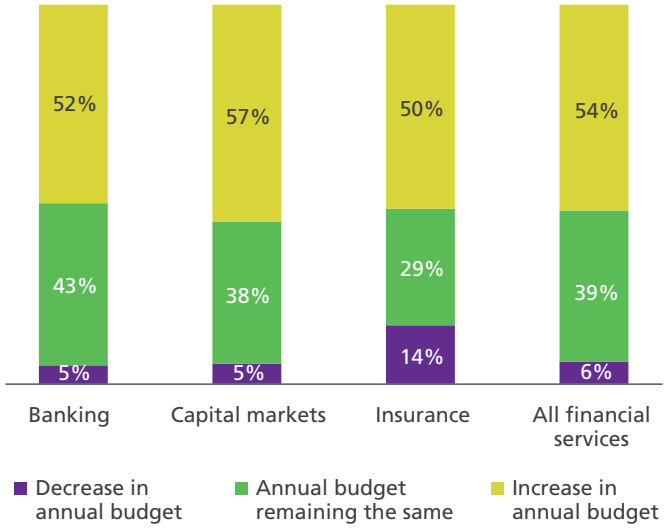
*Note: Colour coding shows comparison vs capital markets (**PURPLE** = behind, **GREEN** = equal to or higher)*



Looking ahead

As banks 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 are seemingly set to continue, with 52% of banks predicting an increase in spending on emerging technologies over the next year and 43% expecting annual budgets to remain the same. Only 5% plan to reduce spending.

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



Banks' expenditure on emerging technologies will continue to grow in the next couple of years, particularly on AI and GenAI. In the medium- to long-term, statistical AI will be a notable area of focus for retail financial institutions in areas such as fraud analytics, anti-money laundering, and non-financial risk analytics.

From our qualitative interviews, it is apparent that many institutions are rebalancing their spend, with significant refocus on the tech stack and on the enabling technologies, rather than on individual non-financial risk calculations and models.

Banks are assuming that regulatory clarity for non-financial risks is not going to be forthcoming. Regardless of these regulatory considerations, anti-fraud analytics and many aspects of digital risk management are operational and business imperatives. Therefore, while the specific analytical techniques may continue to change, banks are focusing on ensuring they have the appropriate enabling technology in place and will look to improve their infrastructure to support the deployment of statistical AI.

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 and evolve to encompass a wider set of concepts and procedures, ultimately performing a core role for successful banks and financial institutions. The functions and sub-categories of emerging risks 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 banks.

Post-quantification, banks need to tackle next steps

As operationally intensive businesses, the need for banks to quantify and analyze their operational risks, including cyber, IT, and third-party risk has become central. Many banks have already invested substantially in tackling emerging IT and cyber risks. The first wave of technological response has largely been implemented, with a focus on quantification, dashboards, and biometrics.

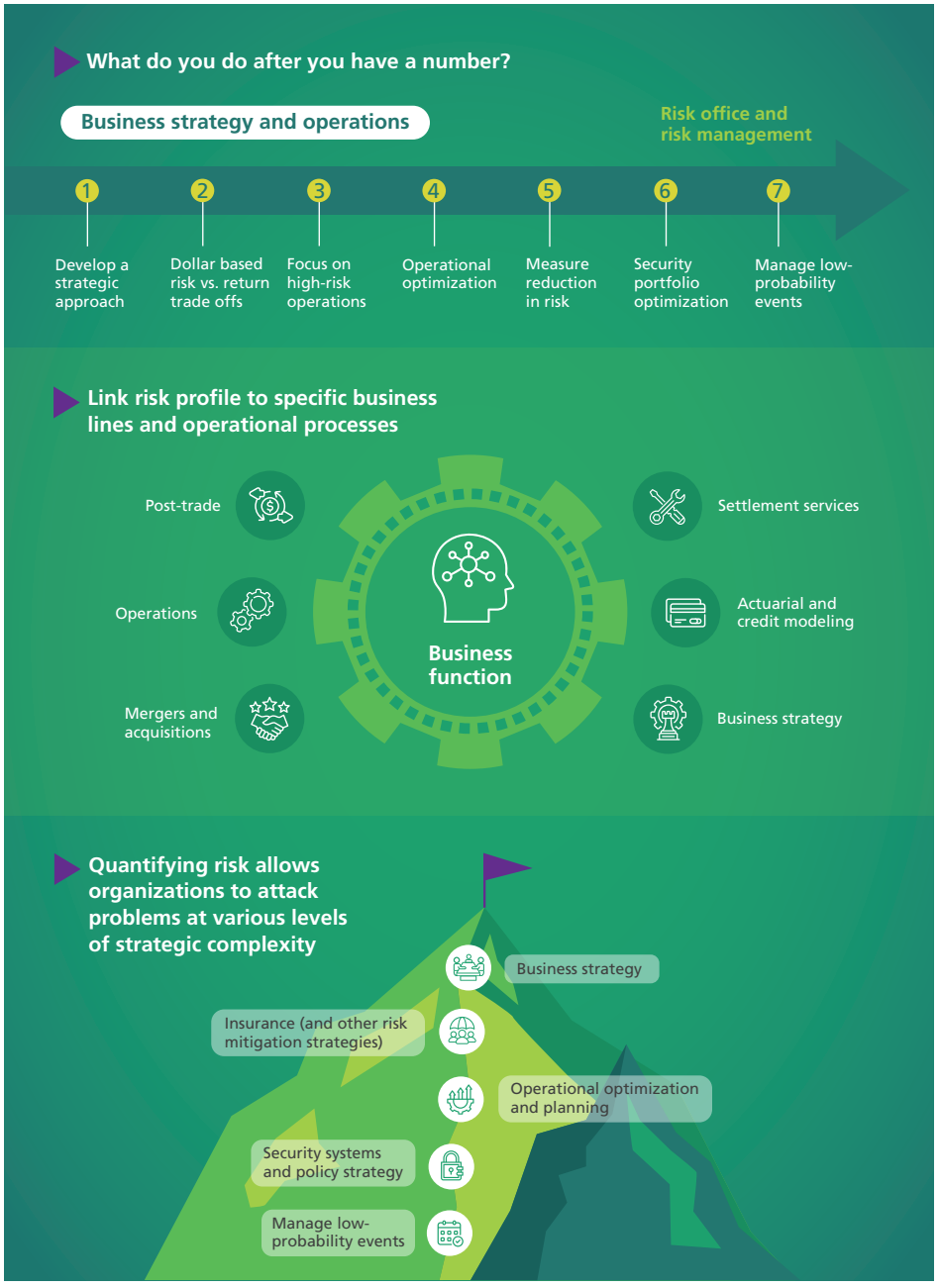
The overwhelming majority is still struggling with major methodological challenges. One of the biggest hurdles to overcome is the wide variety of quantitative techniques, alternative risk measures, and frameworks for emerging risk.

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 incorporating these data points into actual operational activities.

Quantifying risk allows organizations to attack problems at various levels of strategic complexity. However, for most banks 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, banks 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.



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, financial institutions 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 on internal networks, but the key challenge for banks is to make sensible decisions based on this data.

To analyze the data and disseminate 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.

CRITICAL TECHNOLOGIES

- Heterogeneous database infrastructures [relational database for metadata, VLDB for large-scale data storage, vector databases for analytical computing (ML)].
- Data models, data distribution frameworks, risk factor models, data aggregation frameworks and messaging standards all from critical elements of banks' data management requirements. Considerable investments are flowing into these areas.
- New programming language ecosystems based around Python, Julia, etc.
- AI, ML for data management are in most areas of banking, except in operational risk quantification (extreme non-linearly), operational process automation and retail finance.

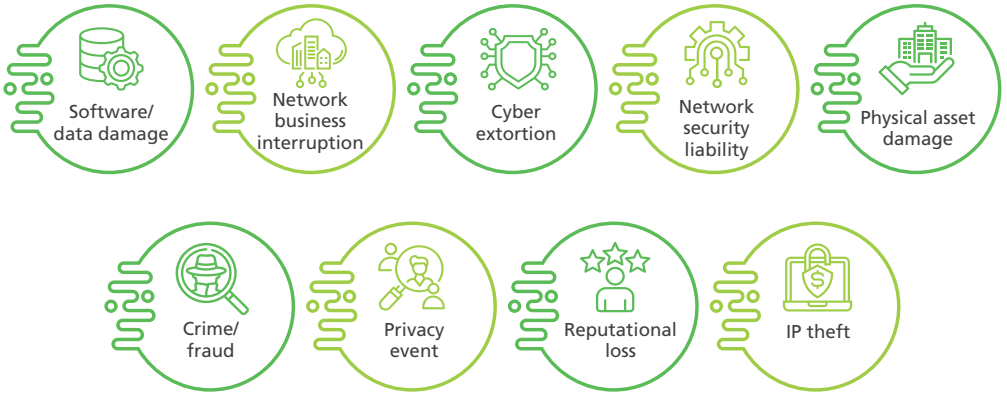
Insurance analytics provide a model for integrating cyber risks into business strategy

To develop analytical frameworks for banks, there is an increasing consensus that the mechanisms of insurance underwriting and actuarial practices can play a significant role.

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

As non-financial risk evolves, it will result in the development of a convergent framework that takes significant elements and approaches from traditional financial modelling, such as risk management measures (for e.g. 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 banks

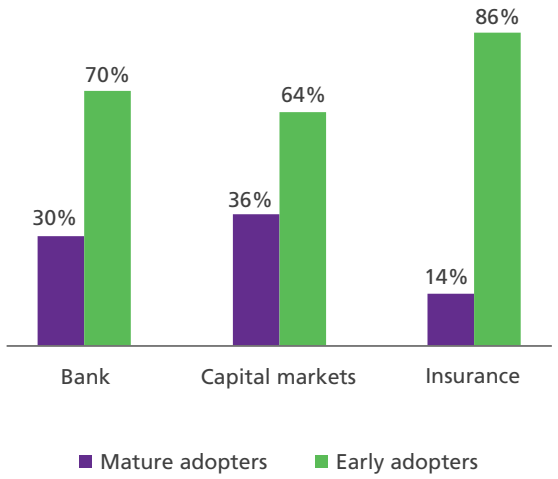


Conclusion

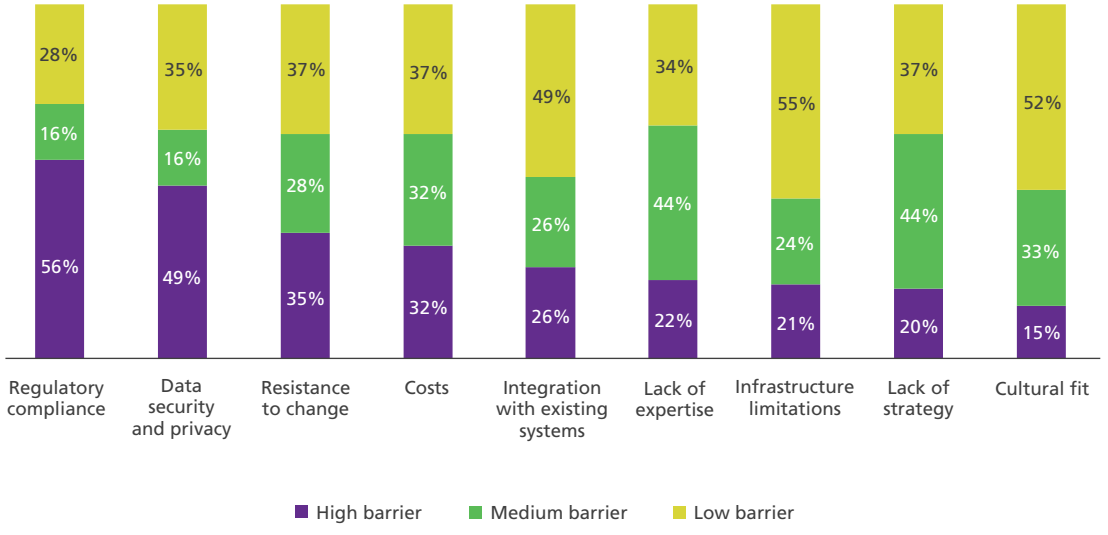
Most financial institutions are struggling to comply with varied types of emerging risks. We see key investments in digitalization and developing robust regulatory frameworks to mitigate various types of risk including enterprise and regulatory as well as to comply with regulatory reporting requirements. Financial institutions are definitely on the path to RiskTech adoption.

3. Appendix: Banking graphics/data for reference

RiskTech/RegTech technologies: mature vs early adopters



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