



Risks arising from big technology companies

Insights related to financial services sector

Board Leadership Center (India)



Technology is fast transforming the way the financial services sector operates. It is being leveraged extensively to improve consumer experience and make operating models more scalable and efficient. Adoption of newer technologies such as Artificial Intelligence/Machine Learning, Blockchain etc. is also enabling data driven transformation and opening new channels. With big technology companies (BigTech) playing an increasingly larger role, it has opened new risks which extend beyond prudential issues.

Technology companies serve financial services in two prominent ways, in addition to being potential business partners:

- Infrastructure providers, e.g., cloud platforms, data centers, software applications etc.
- Service provider, e.g., building and implementation of key applications, outsourcing of technology operations etc.

The extent of the role played by technology companies and evolving models, i.e., as a service provider and/ or a partner, make it quite complex for financial services sector and regulators alike to monitor and manage risks.



Prominent risk areas:

- 1. Contractual:** It is not uncommon in financial services to have long standing contracts, often more than 10 years, with same technology companies due to complex infrastructure. Obligations outlined in these contracts, if not reviewed regularly to keep them aligned with evolving business and technology, become ineffective. Complex pricing models, e.g., service level-based charges, volume rebates etc. are likely to lead to cost leakage, if not monitored diligently
- 2. Commercial:** Dominance of limited number of vendors, specially BigTech, can have an adverse impact. Software vendors with niche products and high market penetration introduce cost and operational barriers, making it difficult to migrate to an alternative technology

- 3. Accountability:** Multiple models to engage have blurred boundaries and clarity of roles between financial services and technology companies. Not having a clearly documented and agreed RACI (Responsible, Accountable, Consulted, Informed) matrix leads to ambiguity. Lack of relevant and regularly monitored Service Level Agreements can have significant impact
- 4. Security and vulnerability:** Commercially sourced as well as be-spoke developed applications, including source code and underlying components required to operate it, need to be assessed carefully for any security and vulnerability. Absence of a comprehensive inventory of hardware, software and underlying components can result in potential blind spots

5. Business Continuity: In addition to one's own Business Continuity Plans ('BCP'), it is critical to be aware of a technology company's BCP charter and have visibility of its effectiveness on a regular basis. This includes having a clear understanding and transparency about third and fourth parties of technology companies, and risks resulting from such arrangements

6. Talent and skill set: Financial services sector as well as technology companies are known to face challenges in building and maintaining a stable pool of talent. In absence of a strong in-house capability to work alongside a technology company, financial services sector remains heavily dependent on technology companies to run its core technology operations. This, coupled with fast evolving technology, exposes the sector to significant people related risks

7. Data Privacy: Technology companies, specially BigTech, have multiple different business operations beyond being a service provider/ partner to financial services sector. As noted in the International Monetary Fund study¹, depending on the role and broader business context, a combination of regulatory requirements extending across general laws, data protection, and competition may apply

There is a need for the board of directors to stay abreast of developments in technology and its critical role. They should look to leverage internal audit and subject matter experts (e.g. Hardware, Software, IT audits etc.) to critically challenge technology companies and internal stakeholders responsible for managing relationships with them. While this can be enabled via a robust governance mechanism, technology companies and other stakeholders can also play their role by translating technology related issues and their impact into simplified business language.



Top questions for the board to keep in mind

Focus areas

Key questions

Technology landscape

1. How do we ensure regular and clear documentation of technology landscape, including data flow between multiple systems?
2. How de-centralised is our technology? What is our plan to centralise it, from sourcing as well as operations perspective?
3. How do we maintain a list of business-critical applications? How often is the list reviewed and who signs it off?
4. What is our RACI matrix for managing technology risks and which activities pertaining to governance of technology companies are included in it?
5. Does the board have adequate skillsets to understand and act on the information coming from technology related risks?
6. How does our roadmap factor in dependency on a particular technology/ service provider?
7. How are we adequately upskilling management to keep up with the pace of evolving technology landscape and associated risks?

Hardware and software infrastructure

1. How often do we capture a detailed inventory of all hardware and software, including underlying components required to operate it?
2. What is our plan to rationalise our technology portfolio (e.g. number of applications, variation of hardware etc.)?
3. How do we monitor our consumption, especially for SaaS/ cloud subscriptions to ensure proper resource management?

¹ The big tech risk in finance, International Monetary fund, May 2021

Focus Areas

Key Questions

Contracts

1. What is the composition of technology companies engaged in our IT infrastructure in terms of their size and services availed?
2. What is the risk profile of technology companies based on parameters such as spend, criticality, performance etc.?
3. How do we capture and monitor obligations of our technology providers/ partners, including commercial arrangements, SLAs, BCP etc.?
4. How do we manage contract lifecycle to ensure critical requirements such as third/ fourth party obligations including pass through of indemnity are present?
5. What is our contingency plan? Should a particular technology provider cease to exist or become non-cooperative?
6. How do we ensure our technology suppliers are conforming to regulatory reporting requirements?
7. What controls and dispute resolution mechanisms do we have in place to prevent and mitigate exposures, particularly in foreign jurisdictions?
8. What measures do we have in place for long standing contracts, to protect our interest?
9. How well equipped are we to perform various types of audits (e.g. system, commercial etc.) on technology providers?



We would like to thank members of our Council for Governance and Risk in Financial Services for their time in providing us with their valuable insights and perspectives that have contributed to building this POV document.

Council for Governance and Risk in Financial Services members:

Mr. Ashok Barat, Mr. C J George, Mr. Debabrata Sarkar, Mr. Harun Khan, Mr. Jyotin Mehta, Ms. Sharmila Karve and Mr. Uday Chitale.

KPMG in India contacts:



home.kpmg/in/socialmedia

Ritesh Tiwari
Partner, Board Leadership Center
E: riteshtiwari@kpmg.com

Suveer Khanna
Partner, Forensic Services
E: skhanna@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance & Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000

© 2022 KPMG Assurance & Consulting Services LLP an Indian limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only. (002_FLY0419_AB)