PwC India's Financial Services (FS) Risk Symposium

Panel discussions

July 2023

PwC India conducted the inaugural event of its flagship FS Risk Symposium on 19 June 2023 at Trident, BKC Mumbai. Distinguished industry experts from the FS domain participated and shared their views over four distinctive panels.

Risk culture

The panel discussion on risk culture was deeply analysed by illustrious industry magnates:

Rishi Garg, Chief Risk Officer, Nippon Life India Asset Management Limited	Sumit Gupta, Chief Risk Officer, Yes Bank
Venugopal Ranganathan, Chief Risk Officer – India and South Asia Cluster, Standard Chartered Bank	Joydeep Roy, Financial Services Leader – Advisory, PwC India

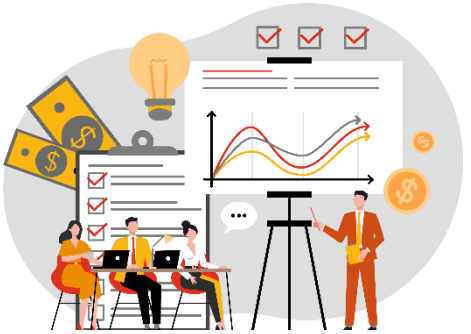
This invigorating session was moderated by Rounak Shah, Partner – Governance Risk Compliance, PwC India.

Highlights

In recent years, the significance of risk culture has become increasingly apparent in the wake of the unprecedented crises that have disrupted the balance of the global financial systems. Firms have dealt with significant shortcomings in their risk management practices. Thus, it is evident that a strong risk culture is essential to prevent excessive risk-taking, ensure financial stability and safeguard the interests of all stakeholders.

Venugopal Ranganathan, in his opening remarks, emphasised the importance of risk culture in financial institutions. He outlined three key steps for developing a robust risk culture:

01	identifying risks
02	understanding risks
03	openly discussing risk perspectives and taking action.



Furthermore, he stressed upon the need for risk culture to be integrated across all areas of firms and advocated the sharing of lessons learned among firms to foster an improved risk culture and management.

A desired risk culture is one that:

01	demonstrates respect within professional peers and senior leaders, fostering an inclusive environment
02	encourages open communication to promote a collaborative atmosphere to discuss risk aspects
03	actively brings forward observations and insights during relevant meetings
04	maintains clear and transparent communication channels across the firm
05	considers risk management as an integral part of the firm's routine operations.

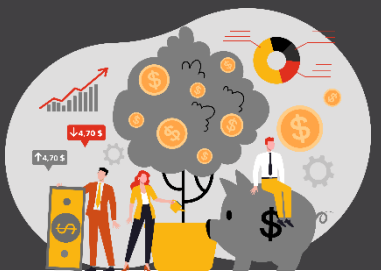
Joydeep Roy focused on the relationship between ambition and risks, resonating the need for objectivity and open discussions. He emphasised the use of management information systems (MIS) as a reliable source of truth and the importance of quantifying risks effectively. He also underscored the significance of consistency in a firm's growth while establishing robust risk mechanisms aligned with a firm's risk culture.

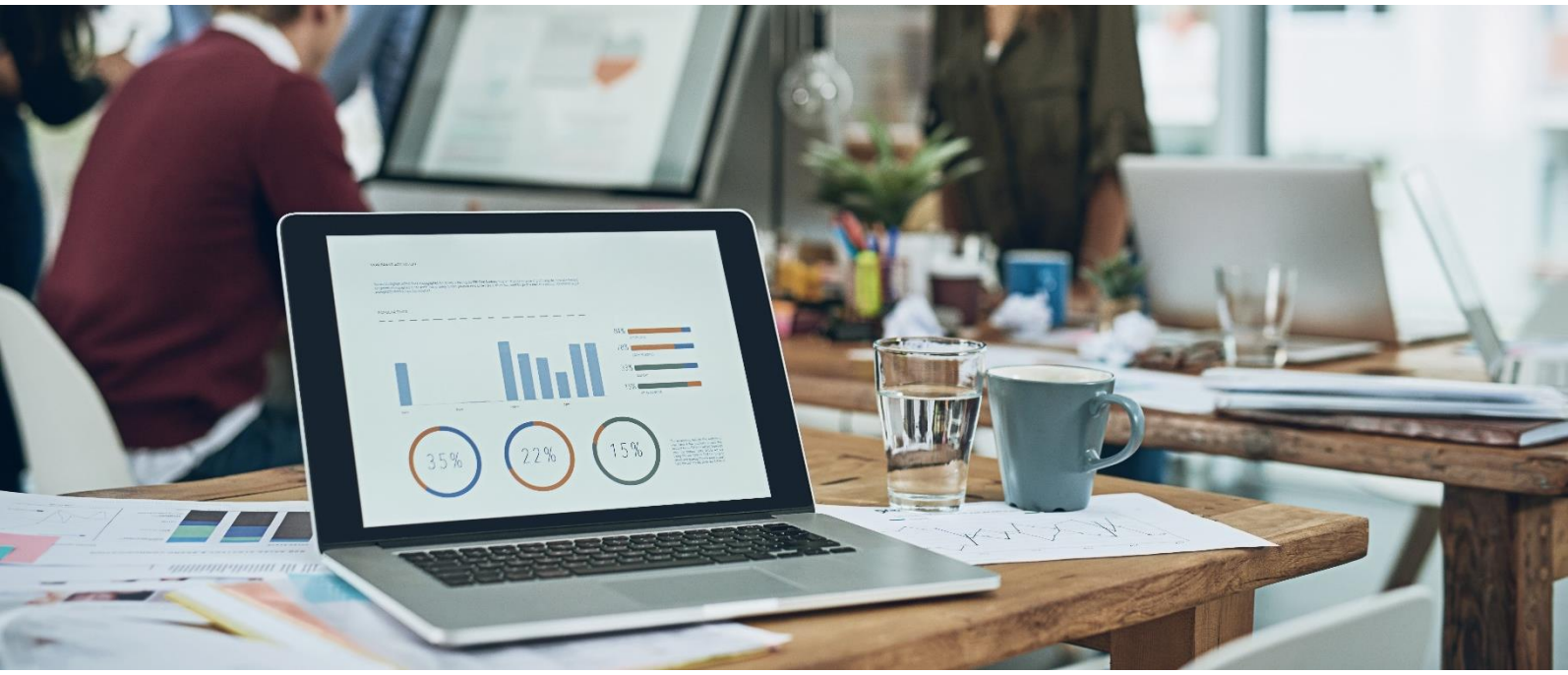
Sumit Gupta focused on the primary role of banks in risk management and the importance of discussions originating from the board level. He highlighted the need for identifying risks promptly, empowering the ability to say no when risk mindsets are misaligned and establishing clear risk-related expectations. Moreover, he suggested defining specific work streams independent of key performance indicators (KPIs) to drive risk culture within the organisation.

Together, the panellists discussed the implementation and integration of risk culture into business practices. They acknowledged the challenge of measuring the adoption of risk culture but proposed using financial metrics, iterations and instances of fraud to quantify its level within an organisation.

Conclusion:

Financial institutions need a strong risk culture, collaboration among firms, clear communication and leadership by example to effectively manage risks and foster a robust risk culture across the industry.





Cloud adoption risks

PwC invited industry experts to share their views on the various aspects of cloud security in a discussion with partners from the firm.

Vaidyanathan, Chief Information Officer, Unity Small Finance Bank Ltd	Prashant Dhanodkar, Head – Information Security and CISO, SBI General Insurance
Amarnath Bysani, Partner – Cyber Risk Consulting, PwC India	Sudhir Kesavan, Partner – Technology Consulting, PwC India

This stimulating session was moderated by Amol Bhat, Partner – Cybersecurity, PwC India.

Highlights

Cloud has revolutionised the way organisations operate, providing unparalleled flexibility, scalability and cost efficiency. However, as with any transformative endeavour, embarking on a cloud journey involves inherent risks. The panel commenced by raising a question that every risk professional should answer at the time of cloud adoption:
What were the triggers (internal and external) that prompted the organisation to consider cloud adoption? How did the cloud journey start?

Vaidyanathan elaborated on the journey a firm must undergo while adopting cloud services:

01	Understand the fundamentals of cloud computing, including infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) model. Firms should evaluate the benefits and trade-offs of each model based on their objectives.
02	Establish a realistic and flexible budget considering factors like cloud service subscriptions, data transfer, security, storage and workforce training.
03	Comply with the Reserve Bank of India (RBI)'s latest guidelines on outsourcing IT services such as the recent Draft Master Direction on Outsourcing of IT Services[1] directive that highlights cloud computing and data management for financial institutions. Adhering to relevant compliance regulations within RBI's jurisdiction is essential.

Sudhir Kesavan highlighted cloud's ability to drive innovation and customer-centric services through embedded intelligence. Cloud processing enables firms to quickly derive actionable insights from customer data, leading to tailored products and fostering stronger customer relationships. Continuous innovation supported by cloud helps firms adopt new business models and meet consumer demands.

Prashant Dhanodkar stressed the importance of addressing risks associated with cloud adoption, including security, privacy and compliance. A robust governance framework is crucial for defining strategies, security policies and best practices. Governance policies should address data security, compliance, resource provisioning, access management and service-level agreements.

Amarnath Bysani discussed cloud adoption from a security perspective, emphasising the need to tailor cloud solutions to the specific maturities of different firms. Integration of multiple vendors helps mitigate the risks of vendor lock-in and aids in optimising cost structures of adopting cloud. A common concern among clients is the availability of standardised and comprehensive cloud frameworks, which should be developed in alignment with a firm's business objectives.

Conclusion:

Embarking on the cloud journey is an exciting and a transformative step for any organisation. By paying attention to budgeting, set-up, RBI compliances and organisational capability, the stage can be set for successful and secure transition to cloud. In sum, cloud adoption is not a one-time event, but an ongoing process that requires continual improvement and adaptability.

1. https://rbidocs.rbi.org.in/rdocs/Content/PDFs/DRAFTMDOUTSOURCINGITSERVICES7B1B0F9AD111484EBF66ADEF509E6CB4.PDF

Model risk management (MRM)

The panel on MRM included eminent industry magnates:

Srinivasa Rao, Deputy MD and Chief Risk Officer (DMD & CRO), State Bank of India (SBI)	G Srinivas, Chief Risk Officer, ICICI Bank

This session was moderated by Kuntal Sur, Leader – Financial Services, Risk Consulting, PwC India.

Highlights

The increasing complexity of financial models and their widespread usage within institutions today has heightened the need for robust MRM practices. These models can include risk assessment models, valuation models, credit scoring models and other types of quantitative tools used for decision making.

Srinivasa Rao opened the discussion by highlighting some key points regarding the use of MRM at SBI, particularly in the underwriting process for their retail segment and for anti-money laundering/countering the financing of terrorism (AML/CFT) efforts.

He underlined the following key takeaways for banks:

01	Employ systematic methods to assess and mitigate risks associated with the use of models in decision making.
02	Recognise the significance of identifying and managing risks associated with models, as errors or inaccuracies in models can have substantial consequences.
03	Place emphasis on the accurate assessment and management of risks associated with models, prioritising integrity and reliability over potential financial gains.
04	Employ rigorous processes to ensure models used in various operations are thoroughly tested and validated for better accuracy and reliability.
05	Recognise the evolving nature of models and the necessity to reassess and validate them at regular intervals to ensure they remain effective and aligned with evolving environments.

G Srinivas added several key points to the discussion:

01	**Model definition and inventory:** It is essential to clearly define a model and maintain an inventory of all models being used. Additionally, independent checks should be performed to ensure the soundness of each model.
02	**Separation of duties:** The individual responsible for creating a model should not be the one running it. There should be a clear separation of duties to avoid conflicts of interest and ensure unbiased results.
03	**Valid sources for sample data:** Sample data should always be sourced from reliable and valid sources.
04	**Operational risks in production:** The production phase of implementing models carries significant operational risks. These risks need to be carefully managed and mitigated to avoid potential issues.
05	**Maintaining morale:** Cleaning and extracting data can be a challenging task. To keep the morale of these individuals high, senior leadership should consistently provide motivation and support.
06	**Importance of common sense:** All models are statistical, complex and sophisticated, leading to a tendency for users to overly trust the data they produce. It is crucial to balance reliance on models with the application of common sense.

Skills required for MRM:

The entire MRM cycle involves interplay between four roles:

01	the core model architect, who provides the theoretical construct;
02	the coder, who writes the algorithm based on the theoretical construct either in open source or any proprietary system;
03	the mediator, who interprets the output with the business context and shares the limitations of the model; and
04	the users, who diligently use the output for the defined business, risk or regulatory purposes.

Conclusion:

Effective MRM is crucial for mitigating potential risks associated with the use of models in various industries. It involves robust governance, comprehensive validation processes, and ongoing monitoring to ensure accurate and reliable model outputs and enhance decision making and overall organisational resilience.

Outsourcing risk management

This panel discussion was led by distinguished industry experts, representing both banking and insurance sectors.

Gopala Srinivasan, ex-Director, National Insurance Academy	Anil Bhandari, ex-CISO, State Bank of India

It was moderated by Puneet Garkhel, Leader Forensic Services, PwC India.

Highlights

Commencing the panel discussion, Gopala Srinivasan highlighted the significant role of outsourcing various activities within a firm. He highlighted the following key points:

01	The practice of outsourcing is expected to grow, but regulators express great concern due to substantial unknown risks associated with it. Currently, not enough measures are being taken to address these risks effectively.
02	Frauds, quality issues, cyber threats and reputation risks are emerging as key challenges stemming from outsourcing. Regulators permit the outsourcing of only non-core activities in Indian insurance firms. However, globally, core insurance activities are being outsourced.
03	Outsourcing risk services introduces unknown risks that demand the development of robust systems to combat threats like ransomware attacks, which can have severe reputational implications. The adoption of automated solutions is crucial for containing these unknown risks.
04	It is essential for firms to have a comprehensive understanding of the risks arising from their suppliers and supply chains, as they carry the n-th risk, implying that risks can originate from various stages of the supply chain, necessitating a thorough evaluation and management approach.

He emphasised on monitoring stringent checks and processes through an outsourcing journey:

01	Thorough understanding of vendors during the initial onboarding phase is crucial. It is essential to gather all comprehensive information about vendors, covering every aspect.
02	Continuous monitoring of vendor platforms, both onsite and offsite, is necessary. These platforms become the originating sources of cyberattacks, making vigilant monitoring imperative.
03	It is essential to clearly define critical services before considering outsourcing, as their importance cannot be replaced or substituted easily.
04	When outsourcing a service, it is essential to conduct proper due diligence. Outsource only after careful evaluation and assessment of the vendor's capabilities and suitability.
05	Gain a deep understanding of how vendors handle various aspects, such as performance metrics, data protection, retention policies, and regulatory obligations regarding data. This knowledge is vital for ensuring compliance and mitigating risks associated with data management.

Adding to the panel discussion, Anil Bhandari highlighted the challenges of assessing risks amongst a large pool of vendors and determining the ones with the best practices. He emphasised the importance of thorough vendor onboarding, which involves conducting extensive background checks and implementing continuous monitoring. These measures are essential to identify potential risks and ensure the adoption of the most reliable vendors.

Conclusion:

The discussion elaborated upon the growing importance of outsourcing in firms while highlighting the substantial unknown risks associated with it. It emphasised the need for effective measures to address these risks, including thorough understanding of vendors, continuous monitoring of platforms, clear definition of critical services, proper due diligence and deep understanding of vendor practices.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with over 360,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

PR/December 2023-M&C 33546