PwC India's Financial Services (FS) Risk Symposium

Keynote session

June 2024

On 12 June 2024 Mumbai, PwC India proudly hosted its third edition of FS Risk Symposium. Delivering a thorough dive into the current financial industry issues and concerns, the symposium saw the participation of seasoned business leaders and experts from the banking, financial services and insurance (BFSI) sector. The forum aimed to highlight the pressing need for aggressive and proactive measures to mitigate evolving emerging risks and implement strategic policies compliant with regulations.

Recently retired from the Reserve Bank of India (RBI), former Chief General Manager Bhargeshwar Banerji graced the event with a poignant keynote address, focusing on newer risks and financial industry regulatory requirements.

He initiated the session by highlighting that the Indian financial industry finds itself at a crossroads where regulatory compliance, risk management and technology developments must come together to enhance its resilience and sustainability.

He outlined the following points for financial firms to consider:

1. **Expectations from assurance functions:** He highlighted the crucial role of assurance functions in promoting internal audit policies and compliance within financial firms. Furthermore, he mentioned how these functions are expected provide independent and objective assessments, have enhanced observability for strengthened risk management strategies, encourage improved communication with regulators, embed robust compliance culture within the firm, and leverage technology for more effective audit impact. Moreover, the need for proactive risk management, coordination in testing activities and aligning audit functions with regulatory expectations were outlined as the success factors for these firms.

   In terms of compliance, Banerji stressed on the importance of keeping close associations with regulators to seek policy/guideline clarifications, identifying non-compliant areas, and incorporating compliance into the technological architecture of the firm's operations.

   Banerji also mentioned that the key expectations for internal audit functions included transitioning towards strategic risk-focused inputs during the initial design stage, coordinating testing to avoid duplicity, identifying inefficiencies, and maintaining professional expertise and transparency.

pwc

2. **Risk management function – expectations:** The risk management function must focus its efforts on creating an enterprise-wide risk governance system. Expectations include engaging with the board to establish effective risk governance, developing robust risk appetite statements (RAS), reporting to the Risk Management Committee (RMC), designing thorough risk communication strategies, and voicing regulatory concerns through top management channels – whenever necessary.

   Furthermore, the risk management function is tasked with offering constructive feedback on draft papers, assuring complete coverage of risks in Internal Capital Adequacy Assessment Process (ICAAP), implementing strengthened Interest Rate Risk in the Banking Book (IRRBB) measures, and setting limits on exposures to sectors and product lines.

Once expectations were covered in detail, Banerji focused on crucial compliance-related issues faced by financial institutions (FIs) that required immediate attention and response, as mentioned below.

Regulatory concerns – compliance

Although risk management and regulatory compliance are still the fundamental components of governance, cybersecurity concerns are evolving at a faster-than-anticipated pace, posing unique challenges for FIs today, thereby requiring proactive action.

Governance gaps, poor IT asset inventory management, data security liabilities and inadequacies in vulnerability management underline the acute necessity of a strong cybersecurity framework within FI operations. Top concerns noted were unidentified issues stemming at the organisational level, lack of structured information sharing and weak compliance culture. Moreover, limitations in management information systems (MIS) and the sustainability criteria of compliance policies underscored the need for a comprehensive regulatory framework review by FIs.

Post these insights, Banerji also provided a comprehensive summary of the IT and cybersecurity risks that financial firms are often exposed to. These have been mentioned below:

	IT risks	Cybersecurity risks
1.	**Capacity planning –** outline well-defined procedures to monitor threshold breaches on CPU/memory/disk utilisations.	**Governance –** Board/IT strategy committee oversight for cyber incident responses
2.	**Operational resilience (business continuity plan [BCP]/disaster recovery [DR]) –** regularly conduct comprehensive DR drills of critical applications.	Comprehensive IT asset inventory management
3.	Obsolescence in technology components	**Data security –** protection of sensitive data (appropriate levels of encryption/masking)
4.	**User access management –** implement multi-factor authentication	**Change management –** comprehensive security audit for application launches/movements
5.	Straight-through processing (STP) risks	**Log management –** accurate log capture and analysis
6.	**IT third-party risk management –** effective diligence and ongoing oversight of IT service providers	**Vulnerability management –** focus on remediation of high and medium-risk vulnerabilities

Initiatives by RBI on cybersecurity and IT upgradation

The RBI has taken proactive steps to strengthen FIs' cybersecurity preparedness and monitor resilience of IT infrastructure. Aiming to improve their cybersecurity posture, recent RBI initiatives include simulated phishing exercises, cyber reconnaissance efforts to find system weaknesses, and issuing of

comprehensive guidelines/cybersecurity frameworks and digital payment security controls.

New and updated policies on IT governance, operational resilience, risk management and assurance practices align with the objectives of the RBI to increase cybersecurity resilience. Within the Supervisory Action Framework (SAF), the RBI has also developed tools like the escalation matrix under which regulatory breaches are handled – including the Prompt Corrective Action (PCA) framework.

Moreover, the RBI's offsite monitoring initiatives play a crucial role in assessing the health of the financial sector. Daily liquidity and structural liquidity statements as well as the Centralised Information Management System's (CIMS) implementation will vastly improve the data collection and analytical capacity of FIs. Key elements of the RBI's proactive monitoring system include early warning signals, stress tests and quarterly systematic risk analysis. Moreover, maintaining financial stability primarily depends on the identification of stressed sectors, vulnerable groups and comprehensive evaluation of banks-non-banking financial companies (NBFC) interconnectedness.

BigTech in the financial domain

The keynote also highlighted the increasing influence of BigTech firms in the financial sector, thus presenting unique challenges and opportunities for both industry participants and regulators. To be a step ahead and address emerging risks stemming from the BigTech confluence, FIs need to delve deeper into the effects of BigTechs on financial services and cover regulatory responses to the same across geographies – including assessing competitive advantages, data protection laws and newer operational resilience frameworks.

Business model and strategy concerns

The session also touched upon issues within FI business models and strategies. Key issues noted included evaluating technology obsolescence, managing credit risk-based loan pricing and facilitating strategy planning for growth segments. For sustainable development and robust risk management, FIs need to outline targeted goals for loan book composition, develop strategic plans for foreign branches and innovate customer-centric product designs.

In conclusion, the keynote session provided a complete overview of the regulatory requirements for FIs, stressing on the importance of proactive risk management, a strong compliance culture and adoption of modern cybersecurity system within the financial industry. By aligning with regulatory expectations, FIs can navigate challenges efficiently and create a resilient foundation for a sustainable future.

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.

pwc.in

Data Classification: DC0 (Public)

KS/July 2024-M&C 39249