Financial Stability in the Emerging Technology Landscape

(Speech by Shri Swaminathan J, Deputy Governor at the International Conference of the International Association of Deposit Insurers- Asia Pacific Regional Committee (IADI-APRC) hosted by the Deposit Insurance Credit Guarantee Corporation (DICGC) held in Jaipur on August 14, 2024)

---

1. Distinguished Guests, Deputy Governor Dr Michael D Patra, Deputy Governor Shri M R Rao, Board of Directors of DICGC, colleagues from DICGC and RBI, ladies, and gentlemen. A very good morning to all of you.

2. It is, indeed, an honour to address this distinguished gathering of global deposit insurers. Deposit insurers, as vital pillars of the financial safety-net system, play a crucial role in bolstering public confidence in the banking sector and fostering overall financial stability. My compliments to the organizers of this Conference—the International Association of Deposit Insurers (IADI), which has excelled as a global standard-setter, the Asia Pacific Regional Committee (APRC), and the Deposit Insurance and Credit Guarantee Corporation (DICGC)—for their exemplary efforts in bringing this event to fruition.

3. The theme of this Conference—*"Navigating the Evolving Financial Landscape: Emerging Challenges for Deposit Insurers and the Importance of Crisis Preparedness"*—is especially relevant considering the significant structural changes occurring in the global financial sector. These transformations, driven by technological innovations, the deepening of financial markets through digital payment systems, and shifting patterns in savings and investment behaviours, are reshaping how financial institutions operate and respond to emerging risks. Accordingly, I will take this opportunity to discuss Financial Stability in the context of the Evolving Technology Landscape.

Emerging risks from the technology landscape

4. In an era where digital transformation is reshaping every facet of banking and finance, the integration of advanced technologies into financial sector, brings both unparalleled opportunities and significant risks.

5. In fact, technology-induced systemic risk has become one of the key areas of concern for the financial sector, which requires close attention. It may indeed be one of the only few truly global risks, that threaten the entire financial system across the world, as digital and online technology blur the boundaries between nations, industries and make the world into

one entity. This growing web of interdependencies means that a disruption in one area can rapidly propagate through the system, affecting numerous entities and jurisdictions simultaneously. Therefore, understanding the full scope of these interconnections has become essential for managing systemic risk. As the intensity and frequency of such events—such as cyberattacks or critical vendor disruptions—continue to rise, the importance of forward-looking risk management, adequate policy intervention and backup plans cannot be overstated.

6. Let me highlight four key facets of technology risks we need to be cognizant of and address.

Cybersecurity risks

7. The financial sector is a prime target of frequent cyberattacks due to the vast amounts of sensitive data and capital it handles. Significant cyber incidents can cause micro-prudential risks for individual financial institutions, namely solvency, liquidity, market, operational and reputational risks. Even at the macro level, the financial system performs a number of key activities that support the real economy such as lending and payments which can be disrupted by cyber incidents.

8. Therefore, protecting critical infrastructure from breaches is of paramount importance, and it requires not only advanced technical defences but also a robust culture of cybersecurity awareness across all levels of the organization. Financial institutions therefore need to have robust business continuity preparedness by testing their systems periodically encompassing possible adverse combinations.

Digital Payments

9. Secondly, today, a significant portion of banking transactions and services are conducted through digital channels. The expansion and widespread adoption of digital payment systems has enabled rapid, low-cost transactions and easy withdrawals via online banking and mobile apps. However, this shift increases the risk to operational stability and resilience, necessitating ongoing investments in IT systems and technology to manage peak loads effectively. Additionally, the 24/7 availability of online and mobile banking can heighten vulnerabilities, potentially accelerating bank runs and liquidity crises during periods of stress, as customers may withdraw funds even outside of traditional banking hours and without having to visit a Bank branch. Further, this behaviour is amplified with the emergence of digital sources of influence, such as social media platforms, that have proved their ability to drive,

disseminate financial information, adverse or otherwise, and trigger a coordinated financial behaviour.

10. These developments underscore the need for financial institutions to reassess and update their crisis preparedness to ensure they are equipped to address and mitigate the fast-evolving risks introduced by technological advancements. They should regularly assess their capability and effectiveness in accessing contingency funding within specified timeframes, depending on the type of funding needs. The events of 2023 in US revealed that some of the affected banks were either unprepared to use the existing “Federal discount window” as a source of liquidity or had not included it as one of the funding sources[1].

Dependence on third parties

11. This brings me to my next point, which is the risks from the increasing dependence on third parties. The digital transformation in banking has also led to a multitude of distinct third-party entities getting involved in the provision of a single product or service, creating a complex web of technical and operational dependencies. However, the impact of failure in any link in this chain can often be catastrophic as was seen in a global IT services outage incident last month. Further, third parties could be points of intrusion for ransomware and other cyber threats.

12. Financial institutions have the primary responsibility to preserve the Confidentiality, Integrity, and Availability of data, whether stored, processed or in transit within themselves or at third-party vendors’ end. Therefore, they must exercise effective oversight of third parties and safeguard against potential vulnerabilities while taking other measures such as maintaining regular backups of their critical data to ensure operational resilience.

Fintech and entry of entities outside the regulatory and supervisory envelope

13. Fourthly, the rise of fintech companies and the entry of entities that operate outside the traditional regulatory and supervisory framework introduce new dimensions of risk to the financial sector. While fintech innovations have greatly enhanced financial inclusion, efficiency, and customer experience, they also present challenges related to data security, consumer protection, and regulatory compliance.

[1] https://som.yale.edu/story/2023/lessons-discount-window-march-2023-bank-failures

14. With the rapid pace of innovation, it is often observed that regulatory gaps, if any, can be exploited, either intentionally or unintentionally, by entities that may not be subject to the same stringent standards as regulated financial institutions. This situation creates an uneven playing field and increases systemic risk, as failures or misconduct in these unregulated areas can have far-reaching consequences across the financial system.

15. To mitigate these risks, regulators must adopt a more agile and forward-looking approach, developing regulatory sandboxes, fostering collaboration with fintech innovators, and ensuring that new entrants are integrated into the regulatory framework in a manner that preserves the stability and integrity of the financial system.

Way forward for Deposit Insurers

16. In the context of deposit insurers, addressing these technology risks requires a tailored approach that reflects the unique role they play in maintaining financial stability. Deposit insurers must be vigilant in adapting to the evolving risk landscape, ensuring that their strategies, policies, and frameworks are robust enough to withstand the challenges posed by technological advancements. I would like to delve on a few thoughts in this regard covering the aspects of strengthening regulatory oversight, risk-based premiums, supervisory rating assessments, investing in technology and crisis preparedness.

Strengthening Regulatory Oversight

17. As the financial sector becomes more digitized, deposit insurers must work closely with regulators and supervisors to strengthen oversight mechanisms. This includes regularly updating regulatory frameworks to incorporate emerging risks associated with digital payments, cybersecurity, and fintech innovations. By adopting a proactive stance, deposit insurers can help ensure that financial institutions under their purview are adequately prepared to manage these risks, thereby safeguarding depositor confidence.

Adopting Risk-Based Premiums

18. The implementation of risk-based premium for deposit insurance merits consideration. By tying insurance premiums to the level of risk posed by individual financial institutions, deposit insurers can incentivize banks to adopt stronger risk management practices. This approach not only enhances the overall stability of the financial system but also ensures that institutions with higher risk profiles contribute more to the insurance fund.

Relying on Supervisory Rating Assessments

19. Deposit insurers can further mitigate technology risks by relying on supervisory rating assessments that incorporate evaluation of a financial institution’s technological and operational resilience. By using these assessments as a basis for setting insurance premiums or determining intervention strategies, deposit insurers can ensure that their actions are informed by a comprehensive understanding of each institution’s risk profile.

20. Deposit insurers in collaboration with supervisors need to develop advanced risk assessment tools that can effectively identify and quantify the impact of technology-induced risks on financial institutions. This includes integrating cybersecurity risk assessments into their overall evaluation of financial institutions' health, as well as monitoring the operational resilience of banks' digital payment systems.

Investing in Technology and Expertise to accelerate the Claim Settlement Process

21. To stay ahead of emerging threats, deposit insurers must invest in cutting-edge technologies and build internal expertise. Continuous training in areas such as cybersecurity, fintech, and digital payments ensures that deposit insurer teams are equipped to respond swiftly and effectively to crises. Establishing industry-wide forums for information sharing can help build a collective defence against potential threats.

22. The use of technology can also significantly improve the speed and efficiency of claim settlement processes. By integrating digital tools and automated systems, deposit insurers can reduce the time required to process claims, ensuring that depositors receive timely compensation in the event of a bank failure. These technologies can also aid detection of fraudulent claims, thereby ensuring pay-outs are made to legitimate claimants. Faster claim settlements not only enhance depositor confidence but also reinforce the credibility and reliability of the deposit insurance system.

Ensuring Crisis Preparedness

23. Finally, deposit insurers must prioritize crisis preparedness, developing comprehensive contingency plans that account for technology-induced disruptions. This includes conducting regular stress tests and simulations to assess the potential impact of cyber incidents or fintech failures on financial institutions and the broader financial system. By being well-prepared, deposit insurers can ensure that they are ready to act swiftly and

effectively in the event of a crisis, minimizing potential harm to depositors and maintaining public confidence in the financial system.

Conclusion

24. To conclude, deposit insurance stands as a key pillar of the financial safety-net system, playing a crucial role in maintaining financial stability. Alongside prudential regulation, supervision, resolution frameworks, and lender-of-last-resort arrangements, deposit insurance helps prevent bank runs that could escalate into broader financial crises. By assuring depositors that their funds up to the coverage limit are protected, deposit insurance fosters confidence and stability within the banking sector.

25. The evolving technological landscape presents both significant challenges and opportunities for deposit insurers. By adopting a proactive, risk-based approach—including enhanced oversight, risk-based premiums, reliance on supervisory ratings, faster claim settlements, and industry collaboration—deposit insurers can effectively manage these risks.

26. Conferences such as these provide a vital forum for standard setters, regulators, supervisors, and insurers to come together, discuss these challenges, and explore innovative solutions. I hope you take back valuable insights and actionable strategies that will strengthen our collective efforts in addressing these evolving risks. I would also like to extend my heartfelt thanks to the organizers for their exceptional efforts in arranging this insightful event and creating an environment conducive to meaningful dialogue. Thank you.

*****