The Digital Fifth
NEWSLETTER
159th Edition 14th April 2023

# Reserve Bank of India Strengthens IT outsourcing policy to enhance cybersecurity and risk management

The Reserve Bank of India has updated its Outsourcing of IT Services policy with a revised set of guidelines that replace the previous one issued in 2022. The newly released Final Outsourcing policy is aimed at strengthening the security and resilience of information technology infrastructure in banks, non-banking financial companies, and other regulated entities. Considering the exposure of Financial Institutions have to external resources for IT and ITeS, policy guides Financial Institutions(RE) to streamline the processes. The policy is expected to be implemented by the REs by 01-Oct-23 to all the outsourcing partners.

The new policy ensures that financial institutions have appropriate policies, frameworks, and controls in place to manage the risks associated with outsourcing IT activities. The policy requires the institution to have a comprehensive board-approved IT outsourcing policy that defines the roles and responsibilities of the board, senior management, IT function, business function,

and oversight and assurance functions.

The IT services outsourcing policy shall include outsourcing of the activities as below

· IT Infrastructure Management, Maintenance and Support
· Network and Security Solutions
· Application Development; Application Service Providers
· Data Centre Services and Operations
· Cloud Computing Services
· Managed Security Services
· Payment system management and services

The Outsourcing policy of an RE is also expected to cover the criteria for selecting service providers, defining material outsourcing, a delegation of authority depending on risk and materiality, disaster recovery and business continuity plans, monitoring and review of operations, and termination processes.

The key amendments introduced in the final policy are as follows:

· **Applicability:** The scope of the policy has been expanded to include all regulated entities, including NBFC, Regional Rural Banks and cooperative banks with asset sizes below INR 1000 crore.
· **Prior Approval:** Regulated Entities (REs) desirous of outsourcing of IT and IT-enabled services shall require prior approval from RBI, except for outsourcing arrangements for which guidelines are already in place.
· **Outsourcing Agreement:** REs must ensure that outsourcing agreements comply with the new policy at the time of renewal, but not later than six months from the date of issuance of the policy.
· **Cloud Computing**: Cloud computing services have been included as a separate category of outsourcing activities and are subject to specific guidelines.
· **Cyber Security**: The policy emphasizes the need for robust cyber security and sets out specific requirements for third-party service providers in this regard.
· **Reporting**: REs must report outsourcing arrangements to RBI on an annual basis, in a prescribed format.
· **Penalty**: The policy provides for penalties in case of non-compliance with its provisions.

Some of the initiatives to be taken by registered entities as per the newly amended policy are:

· **Evaluation of Need**: REs shall evaluate the need for outsourcing of IT services based on a comprehensive assessment of attendant benefits, risks, and availability of commensurate processes to manage those risks. The REs shall create an inventory of services provided by the service providers, map their dependency on third parties, and periodically evaluate the information received from the service providers.
· **Grievance Redressal Mechanism**: REs shall have a robust grievance redressal mechanism, and responsibility for the redressal of customers' grievances related to outsourced services shall rest with the RE.
· **Additional Requirements**: Additional requirements pertaining to using cloud computing services and outsourcing Security Operations Centre (SOC) services are also outlined.

Overall, the amended policy ensures that financial institutions have appropriate policies, frameworks, and controls in place to manage the risks associated with outsourcing IT activities. The newly released final policy on outsourcing agreements includes several additional aspects to be considered in the agreement, including regular monitoring and assessment of the service provider, specific types of data or information that the service provider is permitted to share with RE's customers or any other party, and recognition of the authority of regulators to perform an inspection of the service provider and any of its sub-contractors.

The policy also includes provisions for clauses requiring the service provider to provide details of data related to RE and its customers captured, processed and stored, controls for maintaining the confidentiality of data of RE and its customers, the right to conduct an audit of the service provider (including its sub-contractors) by the RE, suitable back-to-back arrangements between service providers and OEMs, and non-disclosure agreement with respect to information retained by the service provider.

In conclusion, the enhancement of risk management and cybersecurity measures are critical in today's rapidly evolving digital landscape of banking. With the increasing sophistication and frequency of omnichannel banking, the risk of cyber-attacks is also rising & it is essential for organizations to stay vigilant and proactive in their approach to enhance risk management and cybersecurity. By implementing a comprehensive risk management framework and adopting advanced cybersecurity technologies, organizations can protect their sensitive data and valuable assets.

Additionally, investing in employee training and awareness programs can help organizations create a culture of cybersecurity and reduce the likelihood of human error leading to a data breach. As technology continues to advance, it is imperative for organizations to continuously evaluate and enhance their risk management and cybersecurity measures to ensure they remain effective and capable of protecting against emerging threats.

## Training Calendar April-May’ 23

**CERTIFICATION IN FINANCIAL BLOCKCHAIN**

Topics Covered

- Overview of Blockchain
- Business Use Cases of Blockchain
- Technology Architecture of Blockchain
- Cyber Security in Financial Services
- Cryptocurrency and CBDC

Starting: 30th April
Duration: 2 Sundays

**CERTIFICATION IN DIGITAL BANKING**

Topics Covered

- Overview of Digital Banking
- Indian Digital Banking Ecosystem
- Digital Banking Maturity Model
- Developing Digital Strategy
- Bank & Fintech Partnerships

Starting: 14th May
Duration: 2 Sundays

Know More

## MARKET NEWS

### Banks must have diverse boards: RBI

The RBI has said that banks must have a diverse and independent board of directors, with a mix of executive and non-executive directors with certain minimum qualifications and experience. This was announced by RBI deputy governor M Rajeshwar Rao in a speech at the Thrissur Management Association. In his speech, Rao said that while the RBI has prudential norms for banks, robust governance is crucial to financial stability.

Source : Times of India

---

### RBI approves expanding UPI transactions to allow credit payments

The Reserve Bank of India (RBI) is proposing expanding the reach of the popular Unified

Payments Interface (UPI) digital payments system by allowing credit to be offered via pre-approved bank lines. In a bid to boost digital payments, the RBI recently allowed RuPay credit cards to be linked to UPI. This was to enable customers to link their credit cards and pay via UPI.

Source : Hindu Business Line

---

## WEEKLY FUNDING

| COMPANY | ROUND | AMOUNT |
|---|---|---|
| Paysharp | Seed | $ 1.28 Mn |

## KNOWLEDGE SESSION


## FOUNDERS SPEAK

**Time is now: Blockchain in Day to Day Banking**

Blockchain is one technology, which always intrigued me from my days at Bank in managing technology to be consultant working with Banks, on how to go about picking up technology to deploy and use it as part of large digital agenda.

Since the emergence of Bitcoin, Blockchain as Distributed Ledge Technology came to fore front and have deeply being explored to assess its deployment in banking and financial domain. Banks and Financial institutions have widely experimented and carried out multiple Proof of Concepts (POCs) and build consortiums to participate collectively to explore use cases.

But, real adoption of Blockchain as technology within Banking remain at distance to be part of day-to-banking as compared to other emerging technologies around APIs, Mobility, AI/ML, RPAs and others.

Keeping this thought in mind, we have planned for this session to explore reasons holding up to build day-to-day banking use cases and future around adoption of blockchain technology in Banking.

Shashank Shekhar

Co-Founder & Head of Consulting

The Digital Fifth

---

Facebook Twitter LinkedIn Youtube