An Overview And Impact Analysis Of RBI's IT Outsourcing Guidelines

written by King Stubb & Kasiva | December 6, 2023

The Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023 ("Directions"), which control and regulate information technology ("IT") services that are outsourced by regulated entities, were released by the Reserve Bank of India ("RBI") on April 10, 2023[1]. In order to ensure improved efficiencies while allowing regulated entities to continue focusing on operational resilience, it is necessary for regulated entities to have easier access to newer technologies.

This can be achieved by leveraging and outsourcing critical IT services to financial technology players. This is the rationale behind the directions, which stem from the statement on developmental and regulatory policies.

The RBI is concerned about the different risks that result from Regulated Entities' reliance on third-party IT services, even while it recognizes the necessity for Regulated Entities to outsource IT tasks. The Reserve Bank of India (Outsourcing of IT Services) Directions, 2022[2] ("Draft Directions") is a master directive on outsourcing of IT services that the RBI released for public discussion and feedback on June 23, 2022, in an effort to address the risks involved with outsourcing.

Analysis and Application/Relevance of the RBI's IT Outsourcing Guidelines

'Material Outsourcing of IT Services' agreements made by the following institutions ("Regulated Entities" or "RE(s)") are subject to the directions.

1. Local Area Banks,
2. Small Finance Banks,
3. Payments Banks,

4. Primary (Urban) Co-operative Banks[3],
5. Non-banking Financial Companies[4],
6. Credit Information Companies,
7. Scheduled Commercial Banks (save for Regional Rural Banks), and
8. All India Financial Institutions (EXIM Bank, NABARD, NaBFID, NHB and SIDBI).

In accordance with the Directions, "Material Outsourcing of IT Services" refers to any activity that could:

- seriously impair a RE's business operations if it is disrupted or compromised; or
- materially affect a RE's customers in the event that customer information is lost, stolen, or unauthorized access occurs[5].

As per the Directions, 'Outsourcing of IT Services' encompasses outsourcing of IT infrastructure management, maintenance, and support, network and security solutions, application development, testing, and maintenance, as well as services related to data centres and cloud computing.

It is apparent from the outsourcing of IT services that the RBI has two goals in mind. The first is to, shield REs from the effects that outsourcing IT services may have on their operations and business in the event that this outsourcing is disrupted or compromised; the second is to shield RE's clients from the danger of data loss, theft, or unauthorized access. Further, it might be significant to mention that the Directions give an extensive list of clauses that must be included in the outsourcing contract that RE, and its technology service provider ("TSP") have signed.

A Look at the RBI's IT Outsourcing Guidelines

- IT outsourcing policy-

  This aspect of the policy covers the selection criteria for these activities, service providers, disaster recovery and business continuity plans, delegation of authority based on risk and materiality, systems to monitor and review the operations of these activities, termination procedures and exit strategies, including business continuity in the event that a third-party service provider leaves the outsourcing arrangement.
- Responsibilities for governance-

  The Board, senior management, and the IT department are all accountable for adhering to the Directions and overseeing the duties outlined in them. All the above-mentioned persons have their specific responsibilities clearly outlined in the Directions. The IT function should normally include the internal IT team, which is qualified to comprehend the complexities of the IT services that are being outsourced or that are mandated to be outsourced and can therefore assist the Board and senior management in comprehending the outsourced IT services.

  Additionally, the senior management and IT function play a number of roles, including:

  (a) establishing a framework for approving IT outsourcing activities based on risks and materiality;

  (b) endorsing policies to assess the risks and materiality of all current and potential IT outsourcing agreements; and

  (c) recognizing risks associated with IT outsourcing as they emerge and keeping track of, managing, and reporting on them to the board.
- Recognizing and interacting with the service providers-

  REs are required to undertake due diligence prior to engaging any IT service provider on the basis of a risk-based approach and considering the

qualitative, quantitative, financial, operational, legal and reputational factors. Further, REs are required to effectively assess the impact of concentration risk posed by multiple outsourcing arrangements with the same service provider and evaluate the concentration risk posed by outsourcing of critical functions to a limited number of service providers.

- Implementing Outsourcing Agreements into Practise-
  To establish a relationship between the parties and outline each party's rights and responsibilities, a legally binding agreement must be signed by the RE and the service provider. In order to allow the RE to maintain control over the outsourced work, the agreement must be somewhat flexible and emphasize the significance of the outsourced task, the risks involved, and the techniques for reducing or controlling them.
- Keeping an eye on, and managing the risk-reduction and outsourcing framework-
  The Directions unequivocally state that the RE's top goal is to increase customers' confidence and trust in the establishment of a reliable and stable financial system. As a result, the Directions state that REs must have a risk management framework that covers all aspects of the process and functions involved in identifying, measuring, mitigating, managing, and reporting on risks related to the outsourced arrangements.
- Disclosure of cyber-attacks
  It is the responsibility of REs to make sure that cyber incidents are reported to them promptly by the service provider. This allows the RE to notify the occurrence to the RBI within six hours of the IT service provider detecting it. This schedule corresponds with the schedule set forth in the directives ("CERT-IN Directions") published on April 28, 2022 by the Indian Computer Emergency Response Team of the Ministry of Electronics and Information Technology.
- Compliances across borders
  The Directions require that a RE continuously monitor the political, social, economic, and legal conditions of the jurisdiction in which the service provider is based, as well as the government policies of that jurisdiction, in order to manage risks arising from the outsourcing of IT services to service providers outside of India.
  Additionally, the RE must establish effective procedures for mitigating such risk. Furthermore, it is imperative for REs to guarantee that they exclusively enter into outsourcing agreements with IT service providers operating inside jurisdictions that maintain confidentiality clauses, and that the controlling law within the agreement is unambiguously established.
  Additionally, the Directions state that entering into a contract with a foreign service provider shall not limit the authority of the RBI or the REs to audit or examine the service provider.
- Safe removal/destruction of client records and exit strategy:
  In accordance with the Directions, a RE is required to establish internal policies that include a defined exit strategy for outsourced IT functions, guarantee business continuity in various scenarios, and specify a minimum amount of time to carry out these preparations. In order to prevent unauthorized access to client data held by the IT service provider, it is imperative for REs to verify that the IT service providers have comprehensive frameworks in place that document their business continuity and disaster recovery plans.
  Although the outsourced activities are covered, the Directions also mandate

that REs contemplate the possibility of bringing the outsourced activities back in-house during times of crisis. Furthermore, REs need to have appropriate plans in place in case the IT service provider experiences any unanticipated terminations or insolvency or liquidation. REs must have suitable measures for removing all the assets from the possession of such IT service provider.

Conclusion

In conclusion, the pragmatic intricacies of the operational implementation of the Directions remain uncertain and await empirical observation, given that they have not yet been enacted. Presently, the instructions appear lucid, poised to facilitate the entry of neo banks and other fully digitally regulated service providers, thereby expediting the digitization of traditional brick-and-mortar financial services.

Despite potential administrative challenges, the Directions signify a constructive stride toward regulatory oversight, contributing to the protection of the interests of Regulated Entities (REs) and their clientele.

---

[1] https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12486&Mode=0

[2] https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=4156

[3] The Direction specifically excludes Tier 1 and Tier 2 Urban Co-operative Banks as defined here.
https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12416&Mode=0

[4] The Direction specifically excludes Base-layer NBFCs as defined here.
https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12416&Mode=0

[5] ("Directions on Outsourcing Financial Services")

King Stubb & Kasiva,
Advocates & Attorneys
Click Here to Get in Touch
New
Delhi | Mumbai | Bangalore | Chennai | Hyderabad | Mangalore | Pune | Kochi
Tel: +91 11 41032969 | Email: info@ksandk.com