# RBI's NORMS ON IT OUTSOURCING: AN OVERVIEW AND IMPACT ANALYSIS

## 1. INTRODUCTION

The Reserve Bank of India ("**RBI**") on April 10, 2023, issued the Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023[1] ("**Directions**") to govern and regulate Information Technology ("**IT**") services outsourced by Regulated Entities (*as defined and listed below*). The need for the Directions emanated from the Statement on Developmental and Regulatory Policies dated February 10, 2022[2], which stated that owing to the increasing dependency of customers on digital channels to avail banking services, there is a need for Regulated Entities to get easier access to newer technologies, by leveraging and outsourcing critical IT services to financial technology players, to ensure improved efficiencies while Regulated Entities can continue to focus on operational resilience. While the RBI acknowledges the need for outsourcing IT functions by Regulated Entities, the RBI's concerns are around the various risks that stem from the reliance Regulated Entities place on IT services outsourced to third parties. With the intent of solving for such associated risks with outsourcing, the RBI had on June 23, 2022, issued a draft Master Direction on outsourcing of IT services, namely, The Reserve Bank of India (Outsourcing of IT Services) Directions, 2022[3] ("**Draft Directions**") for public comments and feedback. Based on the feedback received on the Draft Directions, the RBI has now finally released the Directions, which will come into effect on October 01, 2023. As per the Directions, the underlying principles of the Directions is to ensure that the outsourcing arrangements neither weaken the Regulated Entities' ability to fulfil their obligations to the customers, nor impede the effective supervision by the RBI.

This article summarizes the key highlights of the Directions and analyses its potential implications on Regulated Entities and service providers.

## 2. BROAD OVERVIEW AND APPLICABILITY OF THE DIRECTIONS

The Directions apply to 'Material Outsourcing of IT Services' arrangements that are entered into by the following entities ("**Regulated Entities**" or "**RE(s)**"):

- Scheduled Commercial Banks (*excluding Regional Rural Banks*);
- Local Area Banks;
- Small Finance Banks;
- Payments Banks;
- Primary (Urban) Co-operative Banks[4];
- Non-Banking Financial Companies[5];
- Credit Information Companies; and
- All India Financial Institutions (EXIM Bank, NABARD, NaBFID, NHB and SIDBI).

The term 'Material Outsourcing of IT Services' has been defined under the Directions to mean anything which: (a) if disrupted or compromised has the potential to significantly impact an RE's business operations; or (b) may have a material impact on an RE's customers in the event

[1] https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12486&Mode=0
[2] https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=53248
[3] https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=4156
[4] The Direction specifically excludes Tier 1 and Tier 2 Urban Co-operative Banks as defined here.
[5] The Direction specifically excludes Base layer NBFCs as defined here.

of any unauthorized access, loss or theft of customer information.[6] The Directions define 'Outsourcing of IT Services' to include outsourcing of activities such as IT infrastructure management, maintenance and support, network and security solutions, application development, maintenance and testing, services in relation to data centers and cloud computing among others.

A coherent reading of the applicability (*set out above*) along the definitions of 'Outsourcing', 'Material Outsourcing of IT Services' and 'Outsourcing of IT Services' make it abundantly clear that the intent of the RBI is twofold. One is to protect REs from any impact that outsourcing of IT services may have on its business and operations in situations where outsourcing of these IT services are disrupted or compromised; and two is to protect customers of REs from any risk of unauthorized access, loss or theft of their data and information.

It may be pertinent to note that the Directions detail a comprehensive set of provisions that are required to be incorporated under the outsourcing agreement executed between RE and its technology service provider ("**TSP")**. In so far as existing arrangements are concerned, RBI has given REs up to twelve months from the date of issuance of the Directions to re-visit their outsourcing arrangements and comply with the requirements enclosed under the Directions if such renewals are due before October 01, 2023, and has offered thirty-six months from the date of issuance of the Directions, if their agreements are due for renewal after October 01, 2023.

## 3. A DEEP DIVE INTO THE DIRECTIONS

### 3.1. Responsibility of REs in outsourcing:

(a) *RE's liability and relation with service provider:* The Directions emphasize on the role of the RE to be primarily and solely responsible for any IT services outsourced and to ensure that such outsourcing does not impede or interfere with its ability to oversee and manage the activities and undertake supervisory functions. REs, prior to onboarding the IT service providers, shall have carried out a due diligence on the service providers and considered all relevant laws when performing such due diligence exercise. Further, REs need to ensure that the IT service providers engaged by them to render IT services, implement the highest standard of care as would have been employed by the REs, if such activities were not outsourced. REs are also cautioned against engaging IT service providers that would result in the reputation of the RE being compromised or weakened.

(b) *Maintaining inventory of services:* REs are required to create an inventory of services provided by the IT service providers (*including key entities involved in their supply chains*).

(c) *No conflict of interest*: REs are required to ensure that its IT service providers are not owned or controlled by any director, or key managerial personnel, or approver of the outsourcing arrangement of RE, or their relatives. However, an exception to this requirement may be made with the approval of the board/ board level committees, followed by appropriate disclosure, oversight and monitoring of such arrangements. The board of directors of the RE ("**Board**") must ensure that there is no conflict of interest arising out of third-party engagements.

(d) *Comprehensive assessment of need for outsourcing*: REs are also required to undertake detailed evaluation while outsourcing IT functions in terms of benefits and risks associated with outsourcing and accordingly examine the need for outsourcing and the associated risks.

[6] Note that the term 'Outsourcing' has been defined in the Directions as carrying the definition provided to it under the Directions on Managing Risks and Code in Outsourcing of Financial Services ("**Directions on Outsourcing Financial Services**"). The Directions on Outsourcing Financial Services defines the term 'Outsourcing' as "*a bank's use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities on a continuing basis that would normally be undertaken by the bank itself, now or in the future*".

(e) *Adopting a grievance redressal mechanism*: REs must implement robust grievance redressal mechanism for redressing the grievances of its customers in relation to the outsourced IT services and also to ensure that the outsourcing activity, in no way, negatively affects the rights of the customers.

(f) *Additional obligations specific to cloud computing and Security Operations Center ("**SOC**")*: The Directions stipulate comprehensive compliance requirements on REs when they avail cloud computing services offered by third-parties and outsource SOC services. These measures *inter alia* include:

- taking into account the cloud service specific factors, viz., multi-tenancy, multi-location storing/ processing of data, etc., and attendant risks, while establishing appropriate risk management framework;
- adopting and demonstrating a well-established and well-documented cloud adoption policy;
- selecting the cloud service providers ("**CSP**") based on a comprehensive risk assessment of the CSP;
- ensuring sound service and technology architecture that supports cloud-based applications which are built in adherence to globally recognised architecture principles and standards;
- ensuring that the implementation of security controls in the cloud-based application achieves similar or higher degree of control objectives than those achieved in/ by an on-premise application;
- accurately defining minimum monitoring requirements in the cloud environment;
- to have a business continuity framework that shall ensure that, in the event of a disaster affecting its cloud services or failure of the CSP, the RE can continue its critical operations with minimal disruption of services while ensuring integrity and security; and
- ensuring that the RE has adequate oversight and ownership over the rule definition, customisation and related data/ logs, meta-data and analytics (specific to the RE).

**3.2. IT outsourcing policy:**

REs intending to outsource their IT services are required to comprise a Board approved IT outsourcing policy, which mandatorily needs to include, *inter alia*, the roles and responsibilities of the Board, its committees, senior management, IT function, business function as well as oversight and assurance functions in respect of outsourcing of IT services. The policy shall further cover the criteria for selection of such activities as well as service providers, parameters for defining material outsourcing based on the broad criteria, delegation of authority depending on risk and materiality, disaster recovery and business continuity plans, systems to monitor and review the operations of these activities, and termination processes and exit strategies, including business continuity in the event of a third-party service provider exiting the outsourcing arrangement.

**3.3. Governance obligations:**

The responsibility to comply with the Directions and govern the obligations laid down under the Directions is split between the Board, the senior management and IT function. These responsibilities have been demarcated in the Directions by clearly laying down the specific responsibilities of the Board, senior management and the IT function. Albeit the Directions have not provided any particular description on who would constitute 'senior management' and who can be a part of 'IT function', from a market practice standpoint and a reading of the roles and responsibilities laid down, it can be inferred that the senior management would typically be directors, senior officers/ managers in the RE or other key managerial personnel (as defined in the Companies Act, 2013). The 'IT function' on the other hand should typically include the internal IT team that is qualified to understand the complexities of the IT services

being outsourced or required to be outsourced and thereby support the Board and senior management in understanding the outsourced IT services.

While the role of the Board is limited to putting in place a framework for approval of IT outsourcing activities, evaluating the risks and materiality of the IT outsourcing arrangements; and setting up administrative framework for the purpose of the Directions, the roles of the senior management and IT function are a lot more specific and detailed. The role of the senior management and IT function, *inter alia*, includes: (a) putting in place a framework for approval of IT outsourcing activities depending on risks and materiality; (b) approving policies to evaluate the risks and materiality of all existing and prospective IT outsourcing arrangements; and (c) identifying IT outsourcing risks as they arise, monitoring, mitigating, managing and reporting of such risks to the Board.

**3.4. Identification and engagement of the service providers:**

REs are required to undertake due diligence prior to engaging any IT service provider basis a risk-based approach and considering the qualitative, quantitative, financial, operational, legal and reputational factors. Additionally, wherever possible REs may conduct independent reviews and obtain market feedback on the IT service providers to supplement the REs' own assessment.

The Directions have enlisted an inclusive list of aspects that are to be considered by REs for conducting due diligence which *inter alia* includes factors such as capability, financial soundness, business reputation, cyber security and information risk assessment, etc. It is imperative to note that such an inclusive list of factors is also a part of the existing Directions on Outsourcing Financial Services. Accordingly, REs can apply a similar approach that is adopted while conducting due diligence for the purposes of outsourcing IT services, which are already in place for financial service providers, albeit adopting checks and balances that are IT services focused.

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.

**3.5. Execution of Outsourcing Agreements:**

An RE is required to enter into a legally binding agreement that establishes the nature of the relationship between the parties and defines the rights and obligations of each party (*that is the service provider and RE*). The agreement should highlight the importance of the outsourced task, the associated risks and the strategies for mitigating or managing them and must be fairly flexible to allow the RE to retain control over the outsourced activity. The Directions categorically highlight the need for such agreements to be carefully scrutinized by the legal counsel of the RE. Some of the key provisions that need to be covered in the outsourcing agreement *inter alia* include: (a) details of the activity being outsourced; (b) language around appropriate service and performance standards including those applicable for the sub-contractors, if any; (c) provisioning for effective access by the RE to all data, books, records, information, logs, alerts and business premises relevant to the outsourced IT services; (d) regular monitoring and assessment right; (e) imposing the need to comply with the provisions of the Information Technology Act, 2000 and other applicable laws; and (f) provision on storage of data as per extant regulatory requirements, most of which are in alignment with the Directions on Outsourcing Financial Services.

**3.6. Monitoring and controlling the structure for outsourced activities and risk management:**

REs are required to have an appropriate management structure to monitor and control outsourced IT services, which needs to include but not be limited to monitoring the performance, uptime of the systems and resources, service availability, adherence to the service level arrangements, incident response mechanism, etc. Such oversight is required to be undertaken by conducting regular audits either by the internal auditors of the RE or external auditors acting on behalf of the RE.

Further, the Directions clearly dwell on the principle that the utmost priority of the RE is to build confidence and trust amongst the customers to have a stable and reputed financial system. Accordingly, the Directions stipulate that REs are mandatorily required to have a risk management framework which comprehensively deals with the functions and process for the identification, measurement, mitigation, management, and reporting of risks associated with the outsourced arrangements.

With increasing dependency on the outsourcing arrangements for various digital functions undertaken by REs, REs may be required to appoint multiple service providers for dealing with such digital activities. Hence, it has been flagged important for REs to have appropriate systems to assess the risks amongst such IT service providers and thereby, develop an ecosystem of control wherein all the IT service providers have access to the REs data, systems, records, or resources, without compromising customer confidentiality.

Dealing with the need for engagement of multiple service providers, as a welcome step, the Directions provide that for the same IT service provider, shared/ pooled audit can be conducted by REs. Such permissibility of pooled audit will allow REs to either pool their audit resources or engage an independent third-party auditor, to jointly audit a common IT service provider.

**3.7. Reporting of cyber-attacks:**

Given that there is significant data sharing between IT service providers and REs IT service providers are highly exposed to cyber-attacks resulting in unauthorized access to customer data. Accordingly, REs are mandated to ensure that cyber incidents are reported to them by the service provider, without any undue delay, so that the same can be reported by the RE with the RBI within 6 (six) hours of detection of such incident by the IT service provider. This timeline is in line with the timeline prescribed under the directions issued by the Ministry of Electronics and Information Technology Indian Computer Emergency Response Team on April 28, 2022 ("**CERT-IN Directions**").

**3.8. Cross-border compliances:**

To manage risks originating from outsourcing of IT services to service providers outside India, the Directions mandate that an RE monitors government policies of the jurisdiction in which such service provider is based out of and the political, social, economic and legal conditions on a continuous basis, as well as establish sound procedures for mitigating such risk. Further, an RE must ensure that records are at all points of time readily available to the RE and the RBI is not affected even in case of liquidation of the IT service provider. Additionally, REs must ensure that the outsourcing agreement is only entered into by the RE with IT service providers operating in jurisdictions that uphold confidentiality clauses, and that the governing law in such agreement is clearly specified. The Directions also stipulate that contracting with a foreign service provider should not diminish the REs or RBI's right to conduct audit or inspection of the service provider.

**3.9. Exit strategy and safe removal/destruction of customer records:**

The Directions mandate the need for internal policies to be maintained by an RE, which must contain a clear exit strategy with respect to the outsourced IT activities while ensuring business continuity for different scenarios with stipulation of minimum period to execute such plans. To protect against any illicit access to the customer data available with the IT service provider, REs must ensure that the IT service providers have robust frameworks documenting business continuity plans and disaster recovery plans. While this covers the outsourced activities, the Directions also requires REs to consider the prospect of bringing back the outsourced activities in-house in crisis situations.

REs are also required to make sure that the outsourcing agreements contain appropriate clauses for safe removal/ destruction of data, hardware and all records. Further, in the event of occurrence of any unexpected terminations or insolvency/liquidation of the IT service provider, REs must have suitable measures for removing all the assets from the possession of such IT service provider.

## 4. KEY TAKEAWAYS

A reading of the Directions clearly establishes that the intent of the RBI is to improve corporate governance and ring fence REs from any risk that may arise from outsourcing of IT services. The RBI has recognized the need for having a dedicated stand-alone legislation to govern outsourcing of IT services as reliance on technology in today's digital world only keeps growing with time.

It is imperative to note that the existing Directions on Outsourcing Financial Services governs the outsourcing of non-core financial services and specifically excludes outsourcing of pureplay technology-related services. Consequently, prior to the introduction of the Directions, REs were free to outsource their IT functions without undertaking appropriate diligence or entering into a binding and comprehensive contractual arrangement with the service providers. Further, REs are privy to bulk sensitive personal information including financial data of the customers. Given the above, in the absence of a suitable regulatory framework and oversight, sharing of such information with unregulated third-party service providers exposed REs to security breaches and data leakage. As a result, the issuance of the Directions, that is focused on IT outsourcing, will only be viewed as comforting news, specifically for the customers of REs, whose data and information are often misused when collected and passed on by REs to their service providers.

The extensive set of guidelines laid down in the Directions will require REs to revisit their existing IT outsourcing arrangements to ensure compliance with the Directions and to assess and evaluate the risk of IT outsourcing before executing any future arrangements with new IT service providers.

Prior to the introduction of the Directions, REs were required to have their outsourcing policies as a part of the company's IT Policy; however, with the issuance of the Directions, REs will now be required to mandatorily maintain a separate IT outsourcing policy, dealing specifically with outsourcing of IT services. REs that already maintain a separate outsourcing policy can comply with the Directions by simply amending their existing outsourcing policy, to effectuate the same.

Separately, while the RBI has emphasized on the need to ensure that there is no conflict of interest, it has interestingly carved out an exception for any outsourcing arrangements by an RE with its group entities, provided an approval of the board/ board level committee, followed by appropriate disclosure, oversight and monitoring of such arrangements is ensured. This should be a great news for groups that house both lending entities and technology companies

and the several fintech companies that have so far historically only served as technology services and support company to other REs but have now rampantly over the past year started setting up subsidiaries to commence lending operations.

Another interesting highlight would be the elaborate list of factors that have been listed for consideration when entering into an outsourcing agreement. The list is quite exhaustive in nature and passing on specific compliance obligations especially on foreign IT service providers is likely to be a challenge for an RE.

While the Directions will be effective only in October 2023, given the extent of changes that will need to be implemented, REs may need to commence identifying the actions that are needed to be completed to enable effective compliance with the Directions at the earliest. Even from the perspective of a fintech company or any TSP servicing REs, it will be imperative that they start implementing robust internal systems and measures given the number of obligations that are likely to be contractually imposed on them by REs. Obligations such as reporting of cyber incidents within a few hours will be one such challenge imposed on an IT service provider given that the timeline provided to the service provider is likely to be anywhere between 1 (one) to 3 (three) hours and not more owing to the overall timelines imposed on REs for reporting a cyber incident being only 6 (six) hours under the Directions (*in line with the CERT-In Directions*).

## 5. CONCLUSION

Given that the Directions are yet to become operational, practical issues in actual operation remain unidentified and remain to be seen. However, for now, the Directions appear to be fairly clear. The Directions are likely to boost digitisation of traditional brick and mortar financial service industry and will pave the way for neo banks and other purely digital regulated service offerings. Administrative challenges aside, the Directions appear to be a step in the right direction to govern and protect the interests of both REs and their customers.

**Authors:** Namita Viswanath | Raghav Muthanna | Ananya Dash

**Practice Areas:** Technology, Media and Telecommunication, Financial Services Regulatory

**Date:** April 24, 2023