



April 2023

RBI Master Direction on IT outsourcing by regulated entities

Background

The Reserve Bank of India (“**RBI**”) notified the [Master Direction on Outsourcing of Information Technology Services](#) (“**Master Directions**”) on April 10, 2023. These Master Directions are released subsequent to receiving public comments on the RBI’s [draft of the Master Directions](#).

The Master Directions intend to regulate the outsourcing of information technology (“**IT**”) services by banks, non-banking financial companies (“**NBFCs**”), primary cooperative banks, EXIM Bank, National Bank for Agriculture and Rural Development, National Bank for Financing Infrastructure and Development, National Housing Bank, Small Industries Development Bank of India Credit Information Companies, etc (collectively, “**RE**”).

REs typically outsource a substantial portion of their IT and IT enabled services to third party service providers. Such dependency on third parties exposes REs to significant risks as the autonomy of its IT systems could be compromised and thereby their operational integrity could be threatened. RBI has also ramped up its checks on the soundness of cyber security practices of various institutions in the ecosystem.

Applicability and Scope

1. Effective Date

While the Master Directions will come into effect on October 1, 2023, RE must ensure compliance as follows: (a) for existing outsourcing agreements due for renewal before October 1, 2023, within 12 (twelve) months from the date of issuance of the Master Directions; and (b) for existing outsourcing agreements due for renewal after October 1, 2023, as on the renewal date or 36 (thirty six) months from the date of issuance of the Master Directions, whichever is earlier.

2. Applicability on foreign banks

Foreign banks operating in India through its branch offices are subject to a ‘comply or explain’ approach wherein such foreign banks, may deviate from any specific part of these Master Directions. This is subject to the regulator being convinced of the explanation for such deviance by the banks.

3. Applicability on IT services

These Master Directions apply to arrangements by REs involving ‘Material Outsourcing of IT Services’, which are services which:

- a) if disrupted or compromised will have the potential to significantly impact the RE’s business operations; or

b) may have a material impact on the RE's customers in the event of any unauthorised access, loss or theft of customer information.

4. **Scope**

Outsourcing of IT services includes outsourcing of activities relating to IT infrastructure and management; network and security solutions; development of an application; and cloud computing services. To clarify, activities relating to internet banking services, SMS gateways, procurement of IT hardware or appliances, any maintenance services such as security patches or fixing bugs, applications provided by financial sectors like CCIL, NSE, BSE do not form part of outsourcing of IT services.

Notably, the Master Directions provide an indicative list of entities which will not qualify as 'Third-Party Service Providers', such as payment system operators, fintech firms providing co-branded applications, services, products, telecom service providers, security and audit consultants.

Key Obligations

1. **Due Diligence**

RE should conduct a due diligence and keep an ongoing check on the service provider, in accordance with applicable regulations, to ensure that the service provider employs the same high standard of care in performing the services as would have been employed by the RE. REs should not engage an IT service provider that would compromise its reputation and should periodically and comprehensively assess the need for outsourcing the IT services.

2. **Grievance redressal mechanism**

REs should have a robust grievance redressal mechanism and must be fully responsible to redress customers' grievance related to outsourced services. Outsourcing arrangements should not affect the rights of a customer against the RE, including the ability of the customer to obtain redressal as applicable under relevant laws.

3. **Governance framework**

REs intending to outsource its IT activities must have a comprehensive 'Board approved IT outsourcing Policy' which captures *inter alia*, the roles and responsibilities such as IT functions; business functions of the board, committees of the board (if any) and senior management; the criteria for selection of service providers; parameters for defining material outsourcing; 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.

4. **Outsourcing agreement**

REs should ensure that they enter into a legally tenable written contract with each service provider, which is sufficiently flexible to allow the RE to retain adequate control over the outsourced activity and the right to intervene to meet legal and regulatory obligations and to continue its business operations. The minimum considerations required for an outsourcing agreement include a description of outsourced activity (including appropriate service and performance standards), and RE's right to access information and documentation and regular monitoring, auditing rights, to ensure the service provider's compliance with the applicable laws.

5. **Risk management framework**

REs should put in place a risk management framework for outsourcing of IT Services that comprehensively deals with the processes and responsibilities for identification, measurement, mitigation, management, and reporting of risks associated with outsourcing of IT services arrangements, and for confidentiality and integrity of customer's data. Where a service provider acts as an outsourcing agent for multiple REs, it should be ensured that each RE has adequate safeguards to avoid combining information, documents, records and assets.

6. Information security

REs should ensure that the service providers are able to isolate the REs' information, documents and records and other assets such that, in adverse conditions or termination of the contract, all documents, record of transactions and information with the service provider and assets of the RE can be removed from the service provider's possession. The service provider should be prohibited from purging, or altering any data during the transition period, unless specifically advised by the regulator or concerned RE.

7. Monitoring and control of outsourced activities

REs must have in place a management structure to monitor and control its outsourced IT activities. This will include monitoring the performance, uptime of the systems and resources, service availability, incident response mechanism, etc. The regulator is also authorized to perform inspections of the service providers and any of its sub-contractors. Where many REs avail services from the same service provider, REs may adopt pooled/ shared audit.

8. Outsourcing within a group/conglomerate

REs may outsource any IT service within its business group/ conglomerate, provided that such an arrangement is backed by the Board-approved policy and appropriate service level agreements. REs must adopt risk management practices for such outsourcing and continue to maintain an arm's length relationship in dealings with their group entities.

9. Cross border outsourcing

REs must ensure to monitor government policies along with social, economic and legal conditions of the jurisdiction where the service provider is based. If data is stored or processed outside India and the actual transactions are undertaken in India, the governing law should be such that such jurisdictions uphold confidentiality clauses and agreements. REs and the RBI should have the right to audit service providers based outside India.

10. Exit strategy

The outsourcing of IT Services policy will contain a clear exit strategy with regard to outsourced IT activities, while ensuring business continuity during and after exit. In documenting an exit strategy, the RE should identify alternative arrangements, which may include performing the activity by a different service provider or the RE itself. Service providers should also be obligated to cooperate with the RE and a new service provider (if any) for smooth transitioning.

11. Cloud computing services

While engaging any cloud services, REs must ensure that the outsourcing of IT services addressed lifecycle of data in its entirety, i.e., from the time of entry of data into cloud till the data is permanently erased. Additionally, REs must also take into account multi-location storing and processing of data to ensure adherence to the applicable laws. REs must ensure that the selection of cloud service provider is based on a comprehensive risk assessment and globally recognized principles and standards.

12. Cyber security incident reporting

The Master Directions require cyber incidents to be reported to the RE by the service provider without undue delay, such that the incident is reported by the RE to the RBI within 6 (six) hours of detection by the service providers. REs must ensure that the service providers adhere to this requirement. The draft of the Master Directions had mandated such breach reporting by the service providers to the REs within 1 (one) hour of detection; however, no such limitation is specified in the Master Directions.

Conclusion

Based on these Master Directions, the REs must ensure relevant provisions and obligations are set out in the service level agreements and the service providers adhere to these Master Directions. REs must have adequate policies and security measures to ensure that the outsourcing of IT services are in compliance with the applicable laws.

FinTech Practice

JSA is one of India's pioneering law firms in the FinTech space. JSA's FinTech group brings together an integrated multi-practice team to support clients with transactions, disputes and regulatory matters at the intersection of financial services and technology. Our practice leverages the experience and in-depth technology expertise of attorneys across practice areas and allows us to offer clients access to time-tested strategies and holistic advice. Our experienced attorneys are well positioned to assist clients navigate through the complex legal, regulatory and compliance landscape within which these businesses and their technologies operate. Our strong relationships with regulators, banks, insurers, funds, large technology companies and infrastructure and service providers mean that we understand the issues that affect every area of the financial technology ecosystem. This enables us to deliver incisive, informed and innovative advice across the FinTech spectrum. We work with financial institutions, as they adapt and transform, FinTech start-ups, from inception through to all rounds of funding, to IPO and beyond, large technology companies diversifying into FinTech and Investors and strategic acquirers as they identify and secure strategic opportunities in the FinTech space.

Our areas of expertise inter alia include: (a) Prepaid payment instruments and variations thereof, (b) Remittance (person-to-person and person-to-merchant) models and services, (c) Central treasury arrangements and collection agency models, (d) Artificial Intelligence (AI) and Machine Learning (ML) enabled payment systems, (e) Alternative lending and payment platforms, (f) blockchain enabled service offerings, including smart contracts, (g) crowdfunding and crowdsourced investments, (h) Cryptocurrencies, including initial coin offerings, (i) InsurTech products and business models, (j) investments, including PE/VC financing into fintech and financial services companies, (k) Invoice trading and receivable discounting platforms, (l) Payment services and solutions (both cross-border and domestic).

This Prism has been prepared by:



Probir Roy Chowdhury
Partner



Pranavi Pera
Senior Associate



Kavya Pankaj
Associate



Unnati Deva
Associate



17 Practices and
24 Ranked Lawyers



16 Practices and
11 Ranked Lawyers



7 Practices and
2 Ranked Lawyers



11 Practices and
39 Ranked Partners
IFLR1000 APAC Rankings 2022

Banking & Finance Team
of the Year

Fintech Team of the Year

Restructuring & Insolvency
Team of the Year



Among Top 7 Best Overall
Law Firms in India and
10 Ranked Practices

13 winning Deals in
IBLJ Deals of the Year

10 A List Lawyers in
IBLJ Top 100 Lawyer List



Banking & Financial Services
Law Firm of the Year 2022

Dispute Resolution Law
Firm of the Year 2022

Equity Market Deal of the
Year (Premium) 2022

Energy Law Firm of the Year 2021



Ranked #1
The Vahura Best Law Firms to
Work Report, 2022

Top 10 Best Law Firms for
Women in 2022

For more details, please contact km@jsalaw.com

www.jsalaw.com



Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi



This prism is not an advertisement or any form of solicitation and should not be construed as such. This prism has been prepared for general information purposes only. Nothing in this prism constitutes professional advice or a legal opinion. You should obtain appropriate professional advice before making any business, legal or other decisions. JSA and the authors of this prism disclaim all and any liability to any person who takes any decision based on this publication.