

Technology Law Analysis

April 26, 2023

NEW LEGAL FRAMEWORK FOR OUTSOURCING OF IT SERVICES IN INDIA'S BFSI SECTOR

- New legal considerations and contractual requirements for IT service providers to banks and financial institutions in India.
- IT service providers to be under additional level of compliance, audit and oversight, data storage norms and cyber security incident reporting.
- New framework applicable to cross-border arrangements, with banks to closely monitor political, social, economic and legal conditions and have audit rights over overseas IT service provider.
- Exemption for services like SMS gateways, off-the-shelf licensed software, payroll services and IT hardware; and for vendors like business correspondents, payment system operators and co-branding fintech partners.

I. BACKGROUND

- The Reserve Bank of India ("RBI") issued the Master Direction on Outsourcing of Information Technology Services ("Outsourcing Directions")¹ on April 10, 2023. This was following RBI's Statement on Developmental and Regulatory Policies released with its bi-monthly Monetary Policy Statement dated February 10, 2022,² wherein it expressed concerns regarding the outsourcing of Information Technology ("IT") services by regulated entities such as banks and non-bank financial companies, and the associated financial, operational and reputational risks. The Draft Master Direction on Outsourcing of IT Services was issued in June 2022 ("Draft Directions")³ pursuant to which these Outsourcing Directions were introduced as law.
- Timeline for compliance with the Outsourcing Directions:

Type of Outsourcing Arrangement	Compliance with the Outsourcing Directions
Existing Agreements	
Agreements up for renewal prior to October 1, 2023	By April 10, 2024
Agreements up for renewal on or after October 1, 2023	By April 10, 2026
New Agreements	
Agreements in effect prior to October 1, 2023	By April 10, 2024
Agreements in effect on or after October 1, 2023	From the date of the agreement

- As on date, there are existing directions or guidelines regulating outsourcing by different regulated entities of the RBI such as banks,⁴ co-operative banks,⁵ and non-banking financial companies ("NBFCs")⁶ (together "Existing Outsourcing Frameworks"). While these directions or guidelines regulate outsourcing by the above-mentioned entities, the Outsourcing Directions specifically address outsourcing of IT services of banks, NBFCs, credit information companies and certain financial institutions ("REs")⁷.
- The purpose of these Outsourcing Directions is to ensure that outsourcing arrangements neither diminish an RE's ability to fulfil its obligations to customers nor impede effective supervision by the RBI.

II. APPLICABILITY

- The Outsourcing Directions are only applicable to arrangements entered into for Material Outsourcing of IT Services by REs⁸. 'Outsourcing of IT Services' includes outsourcing of IT infrastructure management, maintenance and support, network and security solutions and maintenance (hardware, software or firmware), services and operations related to data centres, and management of IT infrastructure and technology services associated with the payment system ecosystem.

Research Papers

Littlel International Guide (India) 2024

November 08, 2024

Unmasking Deepfakes

October 25, 2024

Are we ready for Designer Babies

October 24, 2024

Research Articles

The Bitcoin Effect

November 14, 2024

Acquirers Beware: Indian Merger Control Regime Revamped!

September 15, 2024

Navigating the Boom: Rise of M&A in Healthcare

August 23, 2024

Audio

Digital Lending - Part 1 - What's New with NBFC P2Ps

November 19, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part I

August 26, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part II

August 26, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

"Investment return is not enough" Nishith Desai with Nikunj Dalmia (ET Now) at FI18 event in Riyadh

October 31, 2024

Analysing SEBI's Consultation Paper on Simplification of registration for FPIs

September 26, 2024

- Material Outsourcing of IT services are those services that, if disrupted or compromised, would have the potential to:
 - make a significant impact on the RE's business operations, or;
 - have a material impact on the RE's customers in the event of any unauthorized access, loss, or theft of customer information.⁹
- The Outsourcing Directions are not applicable to certain services and vendors, which illustratively include: (1) services that are not considered 'Outsourcing of IT Services',¹⁰ such as corporate internet banking services, external audit such as vulnerability assessment/penetration testing, SMS gateways, off-the-shelf software products under license, payroll processing, and procurement of IT hardware; and (2) vendors who are not considered as 'Third-Party Service Providers', such as business correspondents, payment system operators¹¹, co-branding fintech partners, telecom service providers, and IT security and audit consultants¹².
- Where REs avail cloud computing services and outsource security operations center services, there are additional requirements prescribed under the Outsourcing Directions such as cloud adoption policy and security measures, disaster recovery and incident response, audits, adequate oversight, physical access in certain areas, etc.¹³

III. KEY OBLIGATIONS UNDER THE OUTSOURCING DIRECTIONS

- **Due Diligence:** The Outsourcing Directions require that REs must evaluate the need for outsourcing based on the criticality of the activity, the expectations/outcome from outsourcing, the success factors and cost-benefit analysis, and the model for outsourcing. Adequate due diligence must be performed including any past experience of the service provider to whom services are to be outsourced by the RE ("**Service Provider**"), financial soundness and ability to undertake commitments under adverse conditions, business reputation and culture, and external factors such as political, economic, social and legal environment of the jurisdiction of the Service Provider.

- **Governance:** Outsourcing of any activity would not diminish the responsibilities of the RE, its board or senior members in any way, who will be ultimately responsible for the outsourced activity. Therefore, the RE should make sure that the Service Provider employs the same standard of care (that should be high) in performance of the activities as the RE would have undertaken if the activity had not been outsourced.

Additionally, the RE should also make sure that in case the Service Provider is not a group company, it should not be owned or controlled by any directors, key managerial personnel, or approver of the outsourcing arrangement of the RE, or their relatives. However, this requirement can be done away with board approval and proper disclosures, oversight and monitoring of such an arrangement. The REs should have a board-approved outsourcing policy in place covering all necessary roles and responsibilities and criteria for outsourcing activities. The policy should also include disaster recovery, termination processes and exit strategies, including business continuity, of the outsourcing framework. The Outsourcing Directions also provide for specific responsibilities for the board, the senior management and the IT function of the RE.

- **Grievance Redressal:** The RE should maintain a grievance redressal mechanism which should not be compromised in any manner owing to the outsourcing.
- **Outsourcing Agreement:** REs are required to have a legally binding written agreement with each Service Provider. The outsourcing agreement should be sufficiently flexible to allow the RE to retain adequate control over the outsourced activity or the right to intervene with appropriate measures. The agreement should also clearly bring out the nature of the relationship between the RE and the Service Provider.

Further, the Outsourcing Directions provide for certain set of key provisions that should be in the outsourcing agreements which include, amongst others, proper definitions of the services, monitoring and assessment, sub-contracting upon prior consent, and contingency plans. The REs must ensure that the regulator must have the authority to perform inspections of the Service Provider as well as the sub-contractors, and the authority to access the RE's infrastructure and data that is stored or processed by the Service Provider and its sub-contractors.

The Service Provider should also be obliged to comply with any directions issued by the RBI in relation to the outsourced activities and other applicable laws including the Information Technology Act, 2000. The outsourcing agreement must also cover data-related aspects such as applicable data localization requirements as per applicable law, provision of details of data processed and shared with customers of the RE and other parties, the Service Provider's liability to the RE in the event of a confidentiality/security breach, etc.

- **Risk Assessment and Exit:** The Outsourcing Directions also provide that REs must carry out risk assessments and maintain a risk management framework as they are responsible for the activities of the Service Provider to their customers including incidents in relation to cybersecurity incidents, confidentiality and integrity of information, etc. REs must ensure that incidents, including cyber incidents and those resulting in disruption of service and data loss/leakage, are reported to them by the Service Provider without undue delay, in order to enable the RE to report the incident to the RBI within 6 hours of detection by the Service Provider. This has been changed from the Draft Directions, that required immediate reporting and no later than one hour of detection.
- A management framework for monitoring and control of outsourced activities including service uptime, service levels, and certifications are prescribed. REs are also required to audit Service Providers regularly in relation to the outsourced activity, by external or internal auditors. The Outsourcing Directions also permit pooled audit of a Service Provider by REs that avail services from the same Service Provider, as long as the audit requirements are met effectively.

IV. OUTSOURCING WITHIN A GROUP

- Agreements executed for IT services being outsourced to a group entity are required to be done based on a board-approved policy, with appropriate service level arrangements/agreements with the group entity. The choice of the group entity should be based on objective reasons as would be used for choosing a third party, and all dealings should be at an arm's length basis.¹⁴

V. CROSS-BORDER OUTSOURCING

- In cases of cross-border outsourcing, the RE should also closely monitor the policies of the Service Provider's jurisdiction on a continuous basis and set up mitigation measures based on the country's risk. Further, the governing law of the arrangement can be agreed upon between the RE and Service Provider, and should be clearly specified. REs and the RBI should have the right to audit Service Providers based outside India, even in case of liquidation of the Service Providers.

VI. KEY TAKEAWAYS

- **Existing guidelines:** While the Existing Outsourcing Framework regulates outsourcing of various non-core activities of REs, including of financial services, the Outsourcing Directions are specific to outsourcing of IT services. The Existing Outsourcing Framework may continue to apply alongside the Outsourcing Directions to REs, depending on the scope of the outsourcing activities. It is to be noted that the Outsourcing Directions do not apply to payment system operators, to which the RBI Framework for Outsourcing of Payment and Settlement-related Activities by Payment System Operators, 2021 will apply.
- **Applicability of the Outsourcing Directions:** While the Outsourcing Directions are drafted as applicable only to arrangements entered into for Material Outsourcing of IT Services by REs¹⁵, an issue that may arise is the determination of materiality. The definition of 'Material Outsourcing of IT Services' is very wide and leaves scope for interpretation by the REs, and it is unclear what parameters REs are expected to follow to determine materiality.

More importantly, there are no specific obligations in the Outsourcing Directions applicable to 'Material Outsourcing of IT Services'. The obligations mentioned across the Outsourcing Directions are drafted for Outsourcing of IT Services. 'Outsourcing of IT Services' is wider in definition than 'Material Outsourcing of IT Services'.

For example, Chapter III of the Outsourcing Guidelines that deals with the governance framework requires a board-approved IT outsourcing policy for all REs intending to outsource any of its activities. Similar provisions are also elsewhere in the Outsourcing Guidelines which broadly apply to Outsourcing of IT Services (and not Materially Outsourcing of IT Services).

Practically, it is likely that REs would take a stance that the obligations under the Outsourcing Guidelines would be applicable to all Outsourcing of IT Services. Given that certain obligations are significant in terms of the powers given to the REs and RBI, such as the right to audit and control measures, Service Providers may have to undertake significant changes to adhere to such requirements. Also, REs may see pushback from Service Providers on inclusion of such clauses on the ground that the same may not amount to material outsourcing.
- **Renewal and New Agreements:** REs would also have to revisit their existing outsourcing agreements and re-examine outsourcing arrangements, especially for REs with a multi-jurisdictional presence due to the cross-border related provisions. REs would also have to ensure that such agreements are renewed in line with the Outsourcing Directions' obligations and within the timeline prescribed for adherence. REs looking to enter into new outsourcing arrangements will have to closely evaluate the outsourcing agreement requirements under these Outsourcing Directions, and ensure the requirements are adhered to within the time period provided for applicability of the Outsourcing Directions.
- **Impact on Service Providers:** Given the heightened level of compliance required by REs under the Outsourcing Directions, several compliances may be passed on to Service Providers by REs, to meet REs' own compliance with the law. The approach, proposed contractual wordings and extent of compliance passed on may differ from RE to RE viz the Service Providers. Certain compliances that may be contractually imposed on Services Providers include audit rights for the RE and RBI, data storage norms and confidentiality, immediate cyber incident reporting, and RE's flexibility to amend certain terms of the agreement as part of its risk management. IT service providers should be mindful when negotiating their arrangements with REs, and understand what the RE may be legally required to ask of them, and what may be excessive and above the scope of the Outsourcing Directions.

— Akhileshwari Anand , Aaron Kamath & Huzefa Tavawalla

You can direct your queries or comments to the authors

¹ Accessible at <https://m.rbi.org.in/Scripts/NotificationUser.aspx?Id=12486&Mode=0> (last visited April 12, 2023).

² Accessible at https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=53248 (last visited April 12, 2023).

³ Accessible at https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=4156 (last visited April 12, 2023).

⁴ RBI Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks, 2006, accessible at: <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=3148&Mode=0> (last visited April 12, 2023).

⁵ RBI Guidelines for Managing Risk in Outsourcing of Financial Services by Co-operative Banks, 2021, accessible at <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12123&Mode=0> (last visited April 12, 2023).

⁶ RBI Directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs, 2017, accessible at https://rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=11160 (last visited April 12, 2023).

⁷ The Outsourcing Directions are addressed to banking companies (including corresponding new banks and SBI), primary co-operative banks, non-banking financial companies (NBFCs), credit information companies and All India Financial Institutions such as NHB, NABARD, SIDBI, EXIM Bank and NaBFID.

⁸ Clause 2(c), Outsourcing Directions: "Material Outsourcing of IT Services" are those which: a) if disrupted or compromised shall have the potential to significantly impact the RE's business operations; or b) may have material impact on the RE's customers in the event of any unauthorised access, loss or theft of customer information.'

⁹Clause 3(a)(ii), Outsourcing Directions.

¹⁰Clause 3(a)(iv), Outsourcing Directions: “Outsourcing of IT Services” shall include outsourcing of the following activities: a) IT infrastructure management, maintenance and support (hardware, software or firmware); b) Network and security solutions, maintenance (hardware, software or firmware); c) Application Development, Maintenance and Testing; Application Service Providers (ASPs) including ATM Switch ASPs; d) Services and operations related to Data Centres;

e) Cloud Computing Services; f) Managed Security Services; and g) Management of IT infrastructure and technology services associated with payment system ecosystem.’

¹¹Authorised under the Payment and Settlement Systems Act, 2007.

¹²Appendix III.B, Outsourcing Directions. This includes: “i. Vendors providing business services using IT. Example – BCs, ii. Payment System Operators authorised by the Reserve Bank of India under the Payment and Settlement Systems Act, 2007 for setting up and operating Payment Systems in India

iii. Partnership based Fintech firms such as those providing co-branded applications, service, products (would be considered under outsourcing of financial services), iv. Services of Fintech firms for data retrieval, data validation and verification services such as (list is not exhaustive): a. Bank statement analysis

b. GST returns analysis, c. Fetching of vehicle information, d. Digital document execution, e. Data entry and Call centre services, v. Telecom Service Providers from whom leased lines or other similar kind of infrastructure are availed and used for transmission of the data, vi. Security/ Audit Consultants appointed for certification/ audit/ VA-PT related to IT infra/ IT services/ Information Security services in their role as independent third-party auditor/ consultant/ lead implementer”.

¹³Appendix I and II, Outsourcing Directions.

¹⁴Clause 20, Outsourcing Directions.

¹⁵Clause 2(c), Outsourcing Directions.

DISCLAIMER

The contents of this hotline should not be construed as legal opinion. View detailed disclaimer.

This Hotline provides general information existing at the time of preparation. The Hotline is intended as a news update and Nishith Desai Associates neither assumes nor accepts any responsibility for any loss arising to any person acting or refraining from acting as a result of any material contained in this Hotline. It is recommended that professional advice be taken based on the specific facts and circumstances. This Hotline does not substitute the need to refer to the original pronouncements.

This is not a Spam mail. You have received this mail because you have either requested for it or someone must have suggested your name. Since India has no anti-spamming law, we refer to the US directive, which states that a mail cannot be considered Spam if it contains the sender's contact information, which this mail does. In case this mail doesn't concern you, please unsubscribe from mailing list.