Technology Law Analysis

July 19, 2022

NEW RULES FOR OUTSOURCING IT SERVICES – RBI INVITES COMMENTS ON FRESH GUIDELINES

- Introduction of rules on material outsourcing of IT services.
- Increased compliances and due diligence measures.
- 1-hour reporting timeline for incidents including cybersecurity breaches.
- Existing outsourcing agreements need to be re-assessed and re-negotiated.

I. BACKGROUND

The Reserve Bank of India ("**RBI**") on June 23, 2022 issued the Draft Master Direction on Outsourcing of IT Services ("**Draft Directions**").[1] As more and more technology-based fintech models become mainstream, the RBI has expressed its concern regarding the outsourcing of Information Technology ('**IT**') services by Regulated Entities ('**RE**') and the risks associated with the same and has therefore proposed this draft framework.

There are existing directions or guidelines regulating outsourcing by different regulated entities of the RBI such as banks,[2] co-operative banks,[3] non-banking financial companies ("**NBFCs**")[4] and payment system operators[5] ("**Existing Outsourcing Frameworks**"). While all these directions or guidelines regulate outsourcing of the above-mentioned, the Draft Directions specifically address outsourcing of *IT services* of banks, NBFCs, credit information companies and certain financial institutions.[6]

II. PURPOSE

The Draft Directions are released in the wake of the RBI's Statement on Developmental and Regulatory Policies released with its bi-monthly Monetary Policy Statement dated February 10, 2022.[7] In its statement, the RBI noted the need for updating and consolidating regulatory guidelines to address risk management and assessment of IT outsourcing activities. As per the Draft Directions, the underlying purpose is to ensure a balance between the convenience of providing services to the customer and ensuring effective oversight of the outsourcing.[8]

The Draft Directions state that the REs should ensure that the outsourcing of IT services should not diminish the obligations they have towards the customers and neither it should affect the oversight mechanism by the supervising authority. However, the Draft Directions make it very clear that the REs would not require a prior approval from RBI in cases of outsourcing of IT services.

III. APPLICABILITY

The Draft Directions are only applicable to arrangements entered into for *Material Outsourcing* of IT Services by REs.[9] Applicability of these Draft Directions to non-material outsourcing is not mandated. 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, reputation, strategic plans or profitability or the RE's ability to manage risk and comply with law, or;
- have a material impact on the RE's customers in the event of any unauthorized access, loss, or theft of customer information.

Where REs use cloud computing services and outsourcing of Security Operations Center (SOC) services, there are additional requirements prescribed under the Draft Directions such as cloud governance and security measures, disaster recovery and incident response, audits, adequate oversight, physical access in certain areas, etc.[10]

IV. KEY GENERAL OBLIGATIONS UNDER THE DRAFT DIRECTIONS:

Due Diligence: The Draft 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 applicable laws and conditions of approval licensing or registration. This due diligence must consider qualitative, quantitative, financial, operational, legal and reputational factors.

Governance: Outsourcing of any activity would not diminish the responsibilities of the RE, its board or senior members in any way. Therefore, the RE should make sure that the Service Provider employs the same high standard

Research Papers

Compendium of Research Papers
April 11, 2024

Third-Party Funding for Dispute Resolution in India
April 02, 2024

Opportunities in GIFT City
March 18, 2024

Research Articles

Private Client Insights - Sustainable Success: How Family Constitutions can Shape Corporate Governance, Business Succession and Familial Legacy
January 25, 2024

Private Equity and M&A in India: What to Expect in 2024?
January 23, 2024

Emerging Legal Issues with use of Generative AI
October 27, 2023

Audio

IBC allows automatic release of ED attachments: Bombay HC reaffirms
April 15, 2024

The Midnight Clause
February 29, 2024

Enforceability of unstamped or inadequately stamped Arbitration Agreements
January 10, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

Cyber Incident Response Management
February 28, 2024

Webinar : Navigating Advertising

of care in performance of the activities as the RE would have undertaken. Additionally, the RE should also make sure that in case the Service Provider is not a part of the 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. The REs should have a board-approved outsourcing policy in place covering all necessary responsibilities and criteria for outsourcing activities. The policy should also include disaster recovery, termination processes and exit strategies of the outsourcing framework. The Draft 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 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 Draft Directions provide for certain set of key provisions that should be in the outsourcing agreements which include, inter alia, proper definitions of the services, monitoring and assessment, sub-contracting upon prior consent, and contingency plans. The REs must ensure that the regulatory 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. The outsourcing agreement must also cover data-related aspects such as applicable data localization requirements, 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 Draft Directions also provide that REs must carry out risk assessments and maintain a risk management framework as they are responsible activities of the Service Provider to their customers including in relation to cybersecurity incidents, confidentiality and integrity of information, etc. *Most notably, 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 within 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 establish a robust framework for documenting, maintaining and testing Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). Finally, in case of exits by the RE from the outsourcing of services by a Service Provider, there should be proper exit strategies that ensure the continuity of the REs business during and after the exit.

V. OUTSOURCING WITHIN A GROUP

Agreements executed for IT services being outsourced to a group entity are required to be done at an arm's length basis and should demarcate shared resources like premises, personnel, technology infrastructure, details of data sharing (if any), etc. The REs must independently adopt risk management practices on a standalone basis.

VI. 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. If data is stored or processed outside India and the actual transactions are undertaken in India, the Draft Directions provide that the jurisdiction of foreign courts should not extend to the operations of the RE in India, solely based on such data processing in foreign jurisdictions. REs should have the right to audit Service Providers based outside India.

VII. TAKEAWAYS

While there are existing guidelines to regulate outsourcing of non-core activities of REs issued by the RBI, the apex bank has recognized the need to have dedicated guidelines for outsourcing IT services as India rides the booming wave of FinTech and responsible digital innovation. If the Draft Directions are finally issued in its current form, REs with existing IT services outsourcing arrangements will have to reassess if such arrangements would be deemed as 'Material Outsourcing of IT Services' based on the parameters explained above. Notably, these parameters are different from those that determine whether an RE is outsourcing 'core management functions' (which are prohibited under the Existing Outsourcing Frameworks). REs would also have to revisit their outsourcing agreements and reexamine captive outsourcing arrangements, especially for REs with a multi-jurisdictional presence. REs looking to enter into newer outsourcing arrangements will have to closely evaluate the outsourcing agreement requirements under these Draft Directions.

IT service providers, including offshore service providers, will also be significantly impacted by the obligations imposed by REs attempting to comply with these Draft Directions:

- While the Draft Directions are applicable only to REs, REs must ensure that the outsourcing agreement introduces the obligation on the service providers to comply with any directions issued by the RBI, leading to potential conflicts on the actual applicability of the Draft Directions which is only limited to REs.
- Further, unlike the Existing Outsourcing Frameworks, the service provider as well as the sub-contractors may be required to recognize the authority of regulators to carry out inspections.
- Hence, there may be increased negotiations seen while entering into IT service agreements. Service Providers engaged with multiple REs may be required to relook at their arrangements, internal allotment of resources and processes that address conflicts.

One of the other hard-hitting obligations imposed by the Draft Directions is the requirement on the REs to ensure that their service providers report any incidents including cyber security incidents within one hour of detection. This appears to add to the stringent obligations imposed by the Ministry of Electronics and Information Technology through its direction relating to "*information security practices, procedures, prevention, response, and reporting of cyber incidents for Safe & Trusted Internet*" dated April 28, 2022 ("**Cybersecurity Directions**") and related FAQs.[11] The Cybersecurity Directions require service providers to report specified incidents within 6 hours of "noticing such

Laws in India Part II Fireside Chat with Manisha Kapoor
February 27, 2024

Webinar : Navigating Advertising Laws in India
February 20, 2024

incident or being brought to notice about such incidents".[12] The Cybersecurity Directions reporting obligation drew some criticism since conclusive and effective information on cyber security incidents may not be available within 6 hours. This problem may be even more amplified given the 1-hour reporting timeline of the Draft Directions.

Another takeaway would be the comprehensive list of areas that REs are required to cover in their outsourcing agreements. While the Existing Outsourcing Frameworks did prescribe some areas to be mandatorily covered, the Draft Directions particularly prescribe in addition, data related provisions such as those covering protection of customer data, data storage, access to data, data security measures and permitted sharing of data. In addition to data, the Draft Directions also lists other specified areas such as sub-contractor liability, termination rights and arrangements between service providers and OEMs.

The publication of these Draft Directions comes timely as the RBI has also been actively nudging organizations to strengthen their cyber security practices.[13] The Draft Directions are open to suggestions by the stakeholders until 22nd of July 2022.

– Anurag Shah, Purushotham Kittane & Huzefa Tavawalla

You can direct your queries or comments to the authors

[1] Accessible at https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=4156 (last visited July 14, 2022).

[2] RBI Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks, accessible at: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=3148&Mode=0 (last visited July 14, 2022).

[3] Accessible at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12123&Mode=0 (last visited July 14, 2022).

[4] Accessible at https://rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=11160 (last visited July 14, 2022).

[5] Accessible at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12136&Mode=0 (last visited July 14, 2022).

[6] The Draft Directions are addressed to (a) Scheduled Commercial Banks (excluding Regional Rural Banks); (b)Local Area Banks; (c) Small Finance Banks; (d) Payments Banks; (e) Primary (Urban) Co-operative Banks having asset size of □1000 crore and above; (f) Non-Banking Financial Companies in Top, Upper and Middle Layers; (g) Credit Information Companies; and (h) All India Financial Institutions such as NHB, NABARD, SIDBI, EXIM Bank and NaBFID.

[7] Accessible at https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=53248 (last visited July 14, 2022)

[8] In addition to the Draft Directions, the Statement on Developmental and Regulatory Policies also mentions a draft Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2022 to be published for comments from stakeholders.

[9] The Draft Directions are applicable to the following REs:

(a) Scheduled Commercial Banks (excluding Regional Rural Banks); (b) Local Area Banks; (c) Small Finance Banks; (d) Payments Banks; (e) Primary (Urban) Co-operative Banks having asset size of □1000 crore and above; (f) Non-Banking Financial Companies in Top, Upper and Middle Layers; (g) Credit Information Companies; and (h) All India Financial Institutions (NHB, NABARD, SIDBI, EXIM Bank and NaBFID).

Payment service providers seemingly are not included in the list of REs.

[10] Direction 1.9 r/w Appendix I and II of the Draft Directions.

[11] Available at https://www.cert-in.org.in/Directions70B.jsp (last visited July 14, 2022).

[12] Our analysis of the Cybersecurity Directions are available at https://www.nishithdesai.com/SectionCategory/33/Technology-Law-Analysis/12/60/TechnologyLawAnalysis/5507/1.html and http://nishithdesai.com/SectionCategory/33/Research-and-Articles/12/60/ResearchatNDA/6139/2.html (last visited July 14, 2022).

[13] Please see https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=53405 (last visited July 14, 2022).