KHAITAN &CO ADVOCATES SINCE 1911

UPDATE

ERGO

Analysing developments impacting business

RBI RELEASES MASTER DIRECTION TO REGULATE OUTSOURCING OF IT SERVICES

15 May 2023

Background

The Reserve Bank of India (RBI) has issued a master direction on outsourcing of information technology services by REs (*as described below*) on 10 April 2023 (Direction). The RBI had published a draft master direction for public feedback on 23 June 2022, pursuant to which the Direction has been released. The Direction aims to mitigate risks (*as described below*) faced by REs due to material outsourcing of information technology (IT) or IT enabled services as identified under the Direction (collectively, "IT services") to providers of IT or IT enabled services (Service Providers).

Applicability and Scope

The Direction is applicable to regulated entities, namely, all commercial banks, non-banking financial companies, primary co-operative banks, credit information companies, 'All India Financial Institutions' as defined under the Direction (collectively, "REs"). In case of foreign banks operating in India through branch mode, reference to REs' board of directors means the head office or controlling office which has oversight over the Indian branch operations. The scope of the Direction extends to 'material outsourcing' of IT services by REs which are IT services which (i) if disrupted or compromised has the potential to significantly impact the RE's business operations, or (ii) may have material impact on the RE's customers in the event of any unauthorised access, loss or theft of customer information.

Effective Date

The Direction will come into effect from 1 October 2023 (Effective Date) for new outsourcing agreements entered into on or after the Effective Date. Further, different dates have been prescribed for existing outsourcing agreements and outsourcing agreements that will come into force before the Effective Date.

Salient features of the Direction:

- Grievance redressal: REs are required to implement a robust grievance redressal mechanism, since the responsibility of addressing customer grievances related to IT services rest with REs and outsourcing arrangements will not affect customers' rights against the REs. It is important to note that outsourcing of any IT services by REs do not dilute their obligations and REs shall be liable for the actions of their Service Providers.

- Implementation of IT outsourcing policy: REs are required to implement a comprehensive board approved policy which specifies *inter alia*: (i) roles and responsibilities of the board and senior management, (ii) selection criteria for IT services

and Service Providers, (iii) parameters for defining material outsourcing, (iv) disaster recovery and business continuity plans, (v) systems to monitor and review the operations of these activities, and (vi) termination processes and exit strategies depending on different scenarios of exit or termination of IT services (including identifying alternative arrangements for continuous provision of services).

- RE's key obligations: REs are required to ensure that the Service Provider (when not a group company) must not be owned / controlled by any director, key managerial personnel, or approver of the REs' outsourcing arrangement, or their relatives, as such terms are defined under the Companies Act 2013, unless an exception to the same is approved by the board / board level committee of the REs. REs are responsible for maintaining confidentiality and integrity of data pertaining to their customers, which is made available to the Service Providers and must create an inventory of IT services provided by the Service Providers, including key entities involved in the supply chain.

- Due diligence on Service Providers: Prior to entering into an outsourcing arrangement with a Service Provider, REs are required to carry out a risk-based due diligence exercise to assess the Service Provider's capability to comply with the outsourcing agreement. REs are also required to obtain independent review and market feedback about the Service Provider, where possible.

- Constituents of the outsourcing agreement: REs are required to ensure that the rights and obligations of the REs and their Service Providers are clearly set out in a legally binding written agreement, duly vetted by the REs' legal counsel. Certain key elements to be specified in such agreement include: (i) details of the activity being outsourced; (ii) audit, monitoring and inspection rights of the REs and RBI; (iii) governing law of the arrangement; (iv) necessary clauses on safe removal / destruction of data, hardware and records; (v) restriction on Service Provider to erase, purge, revoke, alter or change any data during transition / exit period; (vi) types of material adverse events (e.g. data breaches, etc) and incidents required to be reported by Service Provider to REs; (vii) storage of data only in India as per extant regulatory requirements; and (viii) clauses requiring non-disclosure of information and prior approval / consent of REs for use of sub-contractors by the Service Provider.

- Risk management framework: REs are required to put in place a risk management framework for IT services which will provide details regarding the processes and responsibilities for identification, measurement, mitigation, management, and reporting of risks associated with outsourcing of IT services. Risk assessments carried out by REs are required to be suitably documented and reviewed on a periodic basis. Where a Service Provider acts as an outsourcing agent for multiple REs, care must be taken to build safeguards to ensure that there is no combining of information, documents, etc.

- Reporting of cyber incidents: REs are required to ensure that cyber incidents are reported to them by their Service Providers without undue delay, so that the same can be reported by the REs to the RBI within 6 (six) hours of detection by the Service Providers. REs are also required to monitor the Service Provider's control processes and security practices to disclose security breaches, and immediately notify the RBI in case of any breach of security and leakage of confidential customer information.

- Business continuity and disaster recovery plans: REs are required to ensure that their Service Providers develop a robust framework for documenting, maintaining and testing business continuity and disaster recovery plans, commensurate with the IT services outsourced as per instructions issued by RBI. In this regard, REs are required to consider the availability of alternative Service Providers or the possibility of bringing the

outsourced IT services back in-house in an emergency, and the costs, time and resources that would be involved.

- Obligation to monitor and control outsourced activities: REs are required to implement a management structure to monitor and control IT services (including monitoring performance, uptime of systems and resources, service availability, etc) and reports on such activities are required to be reviewed periodically by senior management. In case of any adverse observation in such report, the same is required to be put up to the board for information. Further, regular audits of Service Providers (including sub-contractors) are required to be conducted by REs.

- Outsourcing within a group / conglomerate: REs may outsource any IT services within the business conglomerate, provided that such arrangement is backed by a board-approved policy and appropriate service level agreements are in place in relation to the same. In this regard, the REs' risk management practices in relation to their Service Providers within the business conglomerate is required to be identical to those specified for a non-related party.

- Cross-border outsourcing: In case of outsourcing of IT services to a Service Provider based in a jurisdiction other than India, REs are required to closely monitor government policies of such jurisdiction and the political, social, economic and legal conditions on a continuous basis to establish procedures for mitigating any country level risks (including having suitable contingency and exit strategies). Further, REs are also required to ensure that availability of records to it and the RBI are not affected even in case of liquidation of the Service Provider.

Comment

The RBI has noted that REs commonly rely on third-party Service Providers to handle their IT services. However, without a consistent regulatory framework in place, outsourcing of material IT services poses a variety of risks and security threats, especially to customers, on account of unauthorised disclosure and usage of their confidential information. To this effect, the release of this Direction is a commendable step towards strengthening the security and risk mitigation framework in relation to IT services outsourced by REs.

- *Supratim Chakraborty (Partner), Sumantra Bose (Principal Associate), Tashi Gyanee (Senior Associate) & Shramana Dwibedi (Associate)*

For any queries please contact: editors@khaitanco.com