भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

RBI/2023-24/102
DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 April 10, 2023

The Chairman/Managing Director/Chief Executive Officer
Scheduled Commercial Banks (excluding Regional Rural Banks);
Local Area Banks; Small Finance Banks; Payments Banks;
Primary (Urban) Co-operative Banks;
Non-Banking Financial Companies;
Credit Information Companies; and
All India Financial Institutions (EXIM Bank, NABARD, NaBFID, NHB and SIDBI)

Madam/Dear Sir,

Master Direction on Outsourcing of Information Technology Services

Regulated Entities (REs) have been extensively leveraging Information Technology (IT) and IT enabled Services (ITeS) to support their business models, products and services offered to their customers. REs also outsource substantial portion of their IT activities to third parties, which expose them to various risks.

2. In order to ensure effective management of attendant risks, the Statement on Developmental and Regulatory Policies dated February 10, 2022, proposed the issuance of suitable regulatory guidelines on Outsourcing of IT Services. Accordingly, a draft Master Direction on Outsourcing of IT Services was released for public comments in June 2022. Based on feedback received, the finalised Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023 are enclosed herewith.

3. The underlying principle of these Directions is to ensure that outsourcing arrangements neither diminish REs ability to fulfil its obligations to customers nor impede effective supervision by the RBI.

4. With a view to provide REs adequate time to comply with the requirements, the enclosed Directions shall come into effect from October 1, 2023.

Yours faithfully,

(T.K.Rajan)
Chief General Manager

Encl: Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023

Contents

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 April 10, 2023

Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023

In exercise of the powers conferred by Section 35A read with Section 56 of the Banking Regulation Act, 1949; Section 45L of the Reserve Bank of India Act, 1934 and Section 11 of the Credit Information Companies (Regulation) Act, 2005, and all other provisions/ laws enabling the Reserve Bank of India ('RBI') in this regard, the RBI being satisfied that it is necessary and expedient in the public interest to do so, hereby issues the Directions hereinafter specified.

Chapter – I
Preliminary

1. **Short title and Commencement**

(a) These Directions shall be called the Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023.

(b) These Directions shall come into effect from October 1, 2023.

I. With respect to existing outsourcing arrangements that are already in force as on the date of issuance of this Master Direction, REs shall ensure that:

i. the agreements that are due for renewal before October 1, 2023 shall comply with the provisions of these Directions as on the renewal date (preferably), but not later than 12 months from the date of issuance of this Master Direction.

ii. the agreements that are due for renewal on or after October 1, 2023 shall comply with the provisions of these Directions as on the renewal date or 36 months from the date of issuance of this Master Direction whichever is earlier.

II. With respect to new outsourcing arrangements, REs shall ensure that:

i. the agreements that come into force before October 1, 2023, shall comply with the provisions of these Directions as on the agreement date (preferably) but not later than 12 months from the date of issuance of this Master Direction.

ii. the agreements that come into force on or after October 1, 2023, shall comply with the provisions of these Directions from the date of agreement itself.

2. Applicability

(a) These Directions shall be applicable to the following entities, collectively referred to as 'regulated entities' or 'REs' in these directions:

(i) all Banking Companies[1], Corresponding New Banks and State Bank of India as defined under subsections (c), (da) and (nc) of section 5 of the Banking Regulation Act, 1949 (collectively referred to as 'commercial banks' hereinafter)

(ii) Primary Co-operative Banks as defined under clause (ccv) of subsection 1 of section 56 of the Banking Regulation Act, 1949 and included in 'Tier 3' and 'Tier 4' as defined in paragraphs 1.c and 1.d respectively of the Annex to RBI circular DOR.REG.No.84/07.01.000/2022-23 dated December 01, 2022 on '*Revised Regulatory Framework - Categorization of Urban Co-operative Banks (UCBs) for Regulatory Purposes*' (hereinafter referred to as 'Urban Co-operative Banks' or 'UCBs').

(iii) Non-Banking Financial Companies as defined under clause (f) of section 45I of the Reserve Bank of India Act, 1934 and included in 'Top Layer', 'Upper Layer' and 'Middle Layer' as defined in paragraphs 1.5, 1.4 and 1.3 respectively of the Annex to RBI circular DOR.CRE.REC.No.60/03.10.001/2021-22 dated October 22, 2021 on *'Scale Based Regulation (SBR): A Revised Regulatory Framework for NBFCs'* (hereinafter referred to as 'NBFCs').

[1] Includes banks incorporated outside India licensed to operate in India ('Foreign Banks'), Local Area Banks (LABs), Small Finance Banks (SFBs), Payments Banks (PBs)

(iv) Credit Information Companies as defined under clause (e) of section 2 of the Credit Information Companies (Regulation) Act, 2005 (hereinafter referred to as 'Credit Information Companies' or 'CICs').

(v) EXIM Bank, National Bank for Agriculture and Rural Development ('NABARD'), National Bank for Financing Infrastructure and Development ('NaBFID'), National Housing Bank ('NHB') and Small Industries Development Bank of India ('SIDBI') as established by the Export-Import Bank of India Act, 1981; the National Bank for Agriculture and Rural Development Act, 1981; the National Bank For Financing Infrastructure and Development Act, 2021; National Housing Bank Act, 1987 and the Small Industries Development Bank of India Act, 1989, respectively (hereinafter referred to as 'All India Financial Institutions or 'AIFIs').

(b) In the case of foreign banks operating in India through branch mode, reference to the Board or Board of Directors in these Directions should be read as reference to the Head Office or controlling office which has the oversight over the branch operations in India. Further, such foreign banks shall be subject to a *'comply or explain'* approach wherein such foreign banks, may deviate from any specific part of these Directions subject to examination and acceptance by the RBI of a reasonably justifiable explanation for the same.

(c) These Directions shall apply to Material Outsourcing of Information Technology ('IT') Services arrangements (as defined in clause 3(a)(ii) below) entered by the REs.

3. **Definitions**

a) In these Directions, unless the context states otherwise, the terms herein shall bear the meanings assigned to them below:

(i) **"Group"** shall be as defined in the *'Guidelines on Management of Intra-Group Transactions and Exposures'* issued vide circular DBOD.No.BP.BC.96/21.06.102/2013-14 dated February 11, 2014, as amended from time to time.

(ii) **"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.

(iii) **"Outsourcing"** shall be as defined in RBI *'Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks'* issued vide circular DBOD.NO.BP.40/ 21.04.158/ 2006-07 dated November 3, 2006, as amended from time to time.

(iv) **"Outsourcing of IT Services"**[2] 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.

(v) **"Service Provider"**[3] means the provider of IT or IT enabled services including entities related to the RE or those which belong to the same group or conglomerate to which the RE belongs. Appendix III provides an indicative (but not exhaustive) list of a) Services/ Activities not

[2] The term 'outsourcing' (unless mentioned explicitly as outsourcing of financial services), implies 'outsourcing of IT Services/ IT enabled Services/ IT activities' and are used interchangeably in this Master Direction.

[3] Depending upon the IT Outsourcing services provided (if any) by an RE to other RE(s), even an RE could be considered as a service provider to other RE, within this Master Direction.

considered under “Outsourcing of IT Services” for the purpose of this Master Direction and b) Vendors / Entities who are not considered as Third-Party Service Provider (TPSP) for the purpose of this Master Direction.

b) All expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949 or the Reserve Bank of India Act, 1934 or Credit Information Companies (Regulation) Act, 2005 or Information Technology Act, 2000 or Companies Act, 2013 and Rules made thereunder or any statutory modification or re-enactment thereto or as used in RBI Directions / Circulars, as the case may be.

Chapter – II
Role of the Regulated Entity

4. **Regulatory and Supervisory requirements**

a) Outsourcing of any activity shall not diminish RE’s obligations as also of its Board and Senior Management, who shall be ultimately responsible for the outsourced activity. RE shall take steps 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, if the same activity was not outsourced. REs shall not engage an IT service provider that would result in reputation of RE being compromised or weakened.

b) Notwithstanding whether the service provider is located in India or abroad, the REs shall ensure that the outsourcing should neither impede nor interfere with the ability of the RE to effectively oversee and manage its activities. Further, the RE shall ensure that the outsourcing does not impede the RBI in carrying out its supervisory functions and objectives.

c) REs shall ensure that the service provider, if not a group company, shall not be owned or controlled by any director, or key managerial personnel, or approver of the outsourcing arrangement of the RE, or their relatives. The terms ‘control’, ‘director’, ‘key managerial personnel’, and ‘relative’ have the same meaning as assigned under the Companies Act, 2013 and the Rules

framed thereunder from time to time. However, an exception to this requirement may be made with the approval of Board/ Board level Committee, followed by appropriate disclosure, oversight and monitoring of such arrangements. The Board shall *inter-alia* ensure that there is no conflict of interest arising out of third-party engagements.

d) Additional requirements pertaining to usage of cloud computing services and outsourcing of Security Operations Center (SOC) services are outlined in Appendix I and Appendix II, respectively.

5. **Comprehensive assessment of need for outsourcing and attendant risks**

REs shall evaluate the need for Outsourcing of IT Services based on comprehensive assessment of attendant benefits, risks and availability of commensurate processes to manage those risks. REs shall *inter-alia* consider:

a) determining the need for outsourcing based on criticality of activity to be outsourced;
b) determining expectations and outcome from outsourcing;
c) determining success factors and cost-benefit analysis; and
d) deciding the model for outsourcing.

6. **Compliance with all applicable statutory and regulatory requirements**

The RE shall consider all relevant laws, regulations, rules, guidelines and conditions of approval, licensing or registration, when performing its due diligence in relation to outsourcing of IT services.

7. **Grievance Redressal Mechanism**

a) REs shall have a robust grievance redressal mechanism that shall not be compromised in any manner on account of outsourcing, i.e., responsibility for redressal of customers' grievances related to outsourced services shall rest with the RE.

b) Outsourcing arrangements shall not affect the rights of a customer against the RE, including the ability of the customer to obtain redressal as applicable under relevant laws.

8. **Inventory of Outsourced Services**

REs shall create an inventory of services provided by the service providers (including key entities involved in their supply chains). Further, REs shall map their dependency on third parties and periodically evaluate the information received from the service providers.

Chapter – III
Governance Framework

9. **IT Outsourcing Policy**

An RE intending to outsource any of its IT activities shall put in place a comprehensive Board approved IT outsourcing policy. The policy shall incorporate, *inter alia*, the roles and responsibilities of the Board, Committees of the Board (if any) and Senior Management, IT function, business function as well as oversight and assurance functions in respect of outsourcing of IT services. It 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.

10. **Role of the Board**

The Board of the RE shall be responsible, *inter alia*, for:

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) setting up suitable administrative framework of Senior Management for the purpose of these Directions.

11. **Role of the Senior Management**

The Senior Management of the RE shall, *inter alia,* be responsible for:

a) formulating IT outsourcing policies and procedures, evaluating the risks and materiality of all existing and prospective IT outsourcing arrangements based on the framework commensurate with the complexity, nature and scope, in line with the enterprise-wide risk management of the organisation approved by the Board and its implementation;

b) prior evaluation of prospective IT outsourcing arrangements and periodic evaluation of the existing outsourcing arrangements covering the performance review, criticality and associated risks of all such arrangements based on the policy approved by the Board;

c) identifying IT outsourcing risks as they arise, monitoring, mitigating, managing and reporting of such risks to the Board/ Board Committee in a timely manner;

d) ensuring that suitable business continuity plans based on realistic and probable disruptive scenarios, including exit of any third-party service provider, are in place and tested periodically;

e) ensuring (i) effective oversight over third party for data confidentiality and (ii) appropriate redressal of customer grievances in a timely manner;

f) ensuring an independent review and audit on a periodic basis for compliance with the legislations, regulations, Board-approved policy and performance standards and reporting the same to Board/ Board Committee; and

g) creating essential capacity with required skillsets within the organisation for proper oversight of outsourced activities.

12. **Role of IT Function**

The responsibilities of the IT Function of the RE shall, *inter alia*, include:

a) assisting the Senior Management in identifying, measuring, monitoring, mitigating and managing the level of IT outsourcing risk in the organisation;

b) ensuring that a central database of all IT outsourcing arrangements is maintained and is accessible for review by Board, Senior Management, Auditors and Supervisors;

c) effectively monitor and supervise the outsourced activity to ensure that the service providers meet the laid down performance standards and provide uninterrupted services, report to the Senior Management; co-ordinate periodic due diligence and highlight concerns, if any; and

d) putting in place necessary documentation required for contractual agreements including service level management, monitoring of vendor operations, key risk indicators and classifying the vendors as per the determined risk.

Chapter – IV
Evaluation and Engagement of Service Providers

13. **Due Diligence on Service Providers**

a) In considering or renewing an Outsourcing of IT Services arrangement, appropriate due diligence shall be performed to assess the capability of the service provider to comply with obligations in the outsourcing agreement on an ongoing basis.

b) A risk-based approach shall be adopted in conducting such due diligence activities.

c) Due diligence shall take into consideration qualitative, quantitative, financial, operational, legal and reputational factors. Where possible, the RE shall obtain independent reviews and market feedback on the service provider to supplement its own assessment.

d) REs shall also consider, while evaluating the capability of the service provider, risks arising from concentration of outsourcing arrangements with a single or a few service provider/s.

14. **Aspects to be considered**

Due diligence shall involve evaluation of all available information, as applicable, about the service provider, including but not limited to:

a) past experience and demonstrated competence to implement and support the proposed IT activity over the contract period;

b) financial soundness and ability to service commitments even under adverse conditions;

c) business reputation and culture, compliance, complaints and outstanding or potential litigations;

d) conflict of interest, if any;

e) external factors like political, economic, social and legal environment of the jurisdiction in which the service provider operates and other events that may impact data security and service performance;

f) details of the technology, infrastructure stability, security and internal control, audit coverage, reporting and monitoring procedures, data backup arrangements, business continuity management and disaster recovery plan;

g) capability to identify and segregate REs data;

h) quality of due diligence exercised by the service provider with respect to its employees and sub-contractors[4];

i) capability to comply with the regulatory and legal requirements of the Outsourcing of IT Services arrangement;

j) information/ cyber security risk assessment;

k) ensuring that appropriate controls, assurance requirements and possible contractual arrangements are in place to ensure data protection and RE's access to the data which is processed, managed or stored by the service provider;

[4] Sub-contractor in this Master Direction refers only to those providing material / significant IT services to the TPSP specific to the material IT Services arrangement that the RE has entered into with the TPSP.

l) ability to effectively service all the customers while maintaining confidentiality, especially where a service provider has exposure to multiple entities; and

m) ability to enforce agreements and the rights available thereunder including those relating to aspects such as data storage, data protection and confidentiality.

Chapter – V
Outsourcing Agreement

15. **Legally binding agreement**

a) REs shall ensure that their rights and obligations and those of each of their service providers are clearly defined and set out in a legally binding written agreement.

b) In principle, the provisions of the agreement should appropriately reckon the criticality of the outsourced task to the business of the RE, the associated risks and the strategies for mitigating or managing them.

c) The terms and conditions governing the contract shall be carefully defined and vetted by the RE's legal counsel for their legal effect and enforceability. The agreement shall be sufficiently flexible to allow the RE to retain adequate control over the outsourced activity and the right to intervene with appropriate measures to meet legal and regulatory obligations.

d) The agreement shall also bring out the nature of legal relationship between the parties.

16. **Aspects to be considered in agreement**

The agreement at a minimum should include (as applicable to the scope of Outsourcing of IT Services) the following aspects:

a) details of the activity being outsourced, including appropriate service and performance standards including for the sub-contractors, if any;

b) effective access by the RE to all data, books, records, information, logs, alerts and business premises relevant to the outsourced activity, available with the service provider;

c) regular monitoring and assessment of the service provider by the RE for continuous management of the risks holistically, so that any necessary corrective measure can be taken immediately;

d) type of material adverse events (e.g., data breaches, denial of service, service unavailability, etc.) and the incidents required to be reported to RE to enable RE to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines;

e) compliance with the provisions of Information Technology Act, 2000, other applicable legal requirements and standards to protect the customer data;

f) the deliverables, including Service-Level Agreements (SLAs) formalising performance criteria to measure the quality and quantity of service levels;

g) storage of data (as applicable to the concerned REs) only in India as per extant regulatory requirements;

h) clauses requiring the service provider to provide details of data (related to RE and its customers) captured, processed and stored;

i) controls for maintaining confidentiality of data of RE's and its customers', and incorporating service provider's liability to RE in the event of security breach and leakage of such information;

j) types of data/ information that the service provider (vendor) is permitted to share with RE's customer and / or any other party;

k) specifying the resolution process, events of default, indemnities, remedies, and recourse available to the respective parties;

l) contingency plan(s) to ensure business continuity and testing requirements;

m) right to conduct audit of the service provider (including its sub-contractors) by the RE, whether by its internal or external auditors, or by agents appointed to act on its behalf, and to obtain copies of any audit or review reports and findings made about the service provider in conjunction with the services performed for the RE;

n) right to seek information from the service provider about the third parties (in the supply chain) engaged by the former;

o) recognising the authority of regulators to perform inspection of the service provider and any of its sub-contractors. Adding clauses to allow RBI or person(s) authorised by it to access the RE's IT infrastructure, applications, data, documents, and other necessary information given to, stored or processed by the service provider and/ or its sub-contractors in relation and as applicable to the scope of the outsourcing arrangement;

p) including clauses making the service provider contractually liable for the performance and risk management practices of its sub-contractors;

q) obligation of the service provider to comply with directions issued by the RBI in relation to the activities outsourced to the service provider, through specific contractual terms and conditions specified by the RE;

r) clauses requiring prior approval/ consent of the RE for use of sub-contractors by the service provider for all or part of an outsourced activity;

s) termination rights of the RE, including the ability to orderly transfer the proposed IT-outsourcing arrangement to another service provider, if necessary or desirable;

t) obligation of the service provider to co-operate with the relevant authorities in case of insolvency/ resolution of the RE;

u) provision to consider skilled resources of service provider who provide core services as “essential personnel” so that a limited number of staff with back-up arrangements necessary to operate critical functions can work on-site during exigencies (including pandemic situations);

v) clause requiring suitable back-to-back arrangements between service providers and the OEMs; and

w) clause requiring non-disclosure agreement with respect to information retained by the service provider.

Chapter – VI
Risk Management

17. **Risk Management Framework**

(a) REs shall put in place a Risk Management framework for Outsourcing of IT Services that shall comprehensively deal with the processes and responsibilities for identification, measurement, mitigation, management, and reporting of risks associated with Outsourcing of IT Services arrangements.

(b) The risk assessments carried out by the REs shall be suitably documented with necessary approvals in line with the roles and responsibilities for the Board of Directors, Senior Management and IT Function. Such risk assessments shall be subject to internal and external quality assurance on a periodic basis as determined by the Board-approved policy.

(c) REs shall be responsible for the confidentiality and integrity of data and information pertaining to the customers that is available to the service provider.

(d) Access to data at RE's location / data centre by service providers shall be on need-to-know basis, with appropriate controls to prevent security breaches and/or data misuse.

(e) Public confidence and customer trust in REs is a prerequisite for their stability and reputation. Hence, REs shall seek to ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the service provider. Access to customer information by staff of the service provider shall be on need-to-know basis.

(f) In the event of multiple service provider relationships where two or more service providers collaborate to deliver an end-to-end solution, the RE remains responsible for understanding and monitoring the control environment of all service providers that have access to the RE's data, systems, records or resources.

(g) In instances where service provider acts as an outsourcing agent for multiple REs, care shall be taken to build adequate safeguards so that there is no combining of information, documents, records and assets[5].

(h) The RE shall ensure that cyber incidents are reported to the RE by the service provider without undue delay, so that the incident is reported by the RE to the RBI within 6 hours of detection by the TPSP.

(i) The REs shall review and monitor the control processes and security practices of the service provider to disclose security breaches. The REs shall immediately notify RBI in the event of breach of security and leakage of confidential customer related information. In these eventualities, REs shall adhere to the extant instructions issued by RBI from time to time on Incident Response and Recovery Management.

(j) **Concentration Risk**: REs shall effectively assess the impact of concentration risk posed by multiple outsourcings to the same service provider and/or the concentration risk posed by outsourcing critical or material functions to a limited number of service providers.

18. **Business Continuity Plan and Disaster Recovery Plan**

a) REs shall require their service providers to develop and establish a robust framework for documenting, maintaining and testing Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) commensurate with the nature and scope of the outsourced activity as per extant instructions issued by RBI from time to time on BCP/ DR requirements.

b) In establishing a viable contingency plan, REs shall consider the availability of alternative service providers or the possibility of bringing the outsourced activity back in-house in an emergency, and the costs, time and resources that would be involved.

[5] As regards combining of data, it would suffice to comply with the following: A clear separation and isolation of data (RE and its customer specific data and information) to ensure that only the personnel as authorised by the RE is able to access data that belongs to them in a multi-tenant environment/ architecture.

c) In order to mitigate the risk of unexpected termination of the outsourcing agreement or insolvency/ liquidation of the service provider, REs shall retain an appropriate level of control over their IT-outsourcing arrangement along with right to intervene, with appropriate measures to continue its business operations.

d) REs shall ensure that service providers are able to isolate the REs' information, documents and records and other assets. This is to ensure 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 possession of the service provider, or deleted, destroyed or rendered unusable.

Chapter – VII
Monitoring and Control of Outsourced Activities

19. **Monitoring and Control of Outsourced Activities**

a) REs shall have in place a management structure to monitor and control its Outsourced IT activities. This shall include (as applicable to the scope of Outsourcing of IT Services) but not limited to monitoring the performance, uptime of the systems and resources, service availability, adherence to SLA requirements, incident response mechanism, etc.

b) RE shall conduct regular audits (as applicable to the scope of Outsourcing of IT Services) of service providers (including sub-contractors) with regard to the activity outsourced by it. Such audits may be conducted either by RE's internal auditors or external auditors appointed to act on RE's behalf.

c) While outsourcing various IT services, more than one RE may be availing services from the same third-party service provider. In such scenarios, in lieu of conducting separate audits by individual REs of the common service provider, they may adopt pooled (shared) audit. This allows the relevant REs to either pool their audit resources or engage an independent third-party auditor to jointly audit a common service provider. However, in doing so, it shall be the responsibility of REs in ensuring that the audit

requirements related to their respective contract with the service provider are met effectively.

d) The audits shall assess the performance of the service provider, adequacy of the risk management practices adopted by the service provider, compliance with laws and regulations, etc. The frequency of the audit shall be determined based on the nature and extent of risk and impact to the RE from the outsourcing arrangements. Reports on the monitoring and control activities shall be reviewed periodically by the Senior Management and in case of any adverse development, the same shall be put up to the Board for information.

e) REs, depending upon the risk assessment, may also rely upon globally recognised third-party certifications made available by the service provider in lieu of conducting independent audits. However, this shall not absolve REs of their responsibility in ensuring assurance on the controls and procedures required to safeguard data security (including availability of systems) at the service provider's end.

f) The RE shall periodically review the financial and operational condition of the service provider to assess its ability to continue to meet its Outsourcing of IT Services obligations. RE shall adopt risk-based approach in defining the periodicity. Such due diligence reviews shall highlight any deterioration or breach in performance standards, confidentiality, and security, and in operational resilience preparedness.

g) In the event of termination of the outsourcing agreement for any reason in cases where the service provider deals with the customers of the RE, the same shall be given due publicity by the RE so as to ensure that the customers stop dealing with the concerned service provider.

h) REs shall ensure that the service provider grants unrestricted and effective access to a) data related to the outsourced activities; b) the relevant business premises of the service provider; subject to appropriate security protocols, for the purpose of effective oversight use by the REs, their auditors, regulators and other relevant Competent Authorities, as authorised under law.

Chapter – VIII
Outsourcing within a Group / Conglomerate

20. **Outsourcing within a Group / Conglomerate**

a) A RE may outsource any IT activity/ IT enabled service within its business group/ conglomerate, provided that such an arrangement is backed by the Board-approved policy and appropriate service level arrangements/ agreements with its group entities are in place.

b) The selection of a group entity shall be based on objective reasons that are similar to selection of a third-party, and any conflicts of interest that such an outsourcing arrangement may entail shall be appropriately dealt with.

c) REs, at all times, shall maintain an arm's length relationship in dealings with their group entities. Risk management practices being adopted by the RE while outsourcing to a group entity shall be identical to those specified for a non-related party.

Chapter – IX
Cross-Border Outsourcing

21. **Additional requirements for Cross-Border Outsourcing**

a) The engagement of a service provider based in a different jurisdiction exposes the RE to country risk. To manage such risk, the RE shall closely monitor government policies of the jurisdiction in which the service provider is based and the political, social, economic and legal conditions on a continuous basis, as well as establish sound procedures for mitigating the country risk. This includes, *inter alia,* having appropriate contingency and exit strategies. Further, it shall be ensured that availability of records to the RE and the RBI will not be affected even in case of liquidation of the service provider.

b) The governing law of the arrangement shall also be clearly specified. In principle, arrangements shall only be entered into with parties operating in jurisdictions upholding confidentiality clauses and agreements.

c) The right of the RE and the RBI to direct and conduct audit or inspection of the service provider based in a foreign jurisdiction shall be ensured.

d) The arrangement shall comply with all statutory requirements as well as regulations issued by the RBI from time to time.

Chapter – X
Exit Strategy

22. **Exit Strategy**

a) The Outsourcing of IT Services policy shall contain a clear exit strategy with regard to outsourced IT activities/ IT enabled services, while ensuring business continuity during and after exit. The strategy should include exit strategy for different scenarios of exit or termination of services with stipulation of minimum period to execute such plans, as necessary. In documenting an exit strategy, the RE shall, *inter alia*, identify alternative arrangements, which may include performing the activity by a different service provider or RE itself.

b) REs shall ensure that the agreement has necessary clauses on safe removal/ destruction of data, hardware and all records (digital and physical), as applicable. However, service provider shall be legally obliged to cooperate fully with both the RE and new service provider(s) to ensure there is a smooth transition. Further, agreement shall ensure that the service provider is prohibited from erasing, purging, revoking, altering or changing any data during the transition period, unless specifically advised by the regulator/ concerned RE.

Appendix – I

Usage of Cloud Computing Services

There are several cloud deployment and service models that have emerged over time. These are generally based on the extent of technology stack that is proposed to be adopted by the consuming entity. Each of these models[6] come with corresponding service, business benefit and risk profiles.

In addition to the Outsourcing of IT Services controls prescribed in these Directions, REs shall adopt the following requirements for storage, computing and movement of data in cloud environments:

1. While considering adoption of cloud solution, it is imperative to analyse the business strategy and goals adopted to the current IT applications footprint and associated costs[7]. Cloud adoption ranges from moving only non-business critical workloads to the cloud to moving critical business applications such as SaaS adoption and the several combinations in-between, which should be based on a business technology risk assessment.

2. In engaging cloud services, REs shall ensure, *inter alia,* that the Outsourcing of IT Services policy addresses the entire lifecycle of data, i.e., covering the entire span of time from generation of the data, its entry into the cloud, till the data is permanently erased/ deleted. The REs shall ensure that the procedures specified are consistent with business needs and legal and regulatory requirements.

3. In adoption of cloud services, REs shall take 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. Cloud security is a shared responsibility between the RE and the Cloud Service Provider

[6] For example, some cloud service and deployment models are: a) Infrastructure as a Service (IaaS): The service provides compute, storage, network, and other basic resources so that the client can develop and deploy their applications. b) Platform as a Service (PaaS): The service provides software for building application, middleware, database, development environment and other tools along with the infrastructure to the client. c) Software as a Service (SaaS): Client uses the application(s) provided by the service provider on a cloud infrastructure. d) Besides application services, Cloud Service Providers (CSPs) also provide a range of services besides the three common services viz. Database as a Service, Security as a Service, Storage as a Service and others with varying risk levels. Deployment Models: cloud services are delivered through the popular models such as Private Cloud, Public Cloud, Hybrid Cloud, Community Cloud.

[7] For example, different heads of cloud related expenses could be application refactoring, integration, consulting, migration, projected recurring expenditure depending on the workloads, etc.

(CSP). REs may refer to some of the *cloud security best practices*[8], for implementing necessary controls, as per applicability of the shared responsibility model in the adoption of cloud services.

4. **Cloud Governance:** REs shall adopt and demonstrate a well-established and documented cloud adoption policy. Such a policy should, *inter alia*, identify the activities that can be moved to the cloud, enable and support protection of various stakeholder interests, ensure compliance with regulatory requirements, including those on privacy, security, data sovereignty, recoverability and data storage requirements, aligned with data classification. The policy should provide for appropriate due diligence to manage and continually monitor the risks associated with CSPs.

5. **Cloud Service Providers (CSP)**

Considerations for selection of CSP: REs shall ensure that the selection of the CSP is based on a comprehensive risk assessment of the CSP. REs shall enter into a contract only with CSPs subject to jurisdictions that uphold enforceability of agreements and the rights available thereunder to REs, including those relating to aspects such as data storage, data protection and confidentiality.

6. **Cloud Services Management and Security Considerations**

a) **Service and Technology Architecture:** REs shall ensure that the service and technology architecture supporting cloud-based applications is built in adherence to globally recognised architecture principles and standards. REs shall prefer a technology architecture that provides for secure container-based data management, where encryption keys and Hardware Security Modules are under the control of the RE. The architecture should provide for a standard set of tools and processes to manage containers, images and releases. Multi-tenancy environments should be protected against data integrity and confidentiality risks, and against co-mingling of data. The architecture should be resilient and enable smooth recovery in case of failure of any one or

[8] i.) NIST SP 800-210 General Access Control Guidance for Cloud Systems - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-210.pdf
ii) MeitY's cloud security best practices document - https://www.meity.gov.in/writereaddata/files/2.%20WI3_Cloud%20Security%20Best%20Practices_06112020.pdf

combination of components across the cloud architecture with minimal impact on data/ information security.

b) **Identity and Access Management (IAM):** IAM shall be agreed upon with the CSP and ensured for providing role-based access to the cloud hosted applications, in respect of user-access and privileged-access. Stringent access controls, as applicable for an on-premise application, may be established for identity and access management to cloud-based applications. Segregation of duties and role conflict matrix should be implemented for all kinds of user-access and privileged-access roles in the cloud-hosted application irrespective of the cloud service model. Access provisioning should be governed by principles of 'need to know' and 'least privileges'. In addition, multi-factor authentication should be implemented for access to cloud applications.

c) **Security Controls:** REs shall ensure 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. This includes ensuring - secure connection through appropriate deployment of network security resources and their configurations; appropriate and secure configurations, monitoring of the cloud assets utilised by the RE; necessary procedures to authorise changes to cloud applications and related resources.

d) **Robust Monitoring and Surveillance:** REs shall accurately define minimum monitoring requirements in the cloud environment. REs should ensure to assess the information/ cyber security capability of the cloud service provider, such that, the

   i) CSP maintains an information security policy framework commensurate with its exposures to vulnerabilities and threats;

   ii) CSP is able to maintain its information/ cyber security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment;

   iii) nature and frequency of testing of controls by the CSP in respect of the outsourced services is commensurate with the materiality of the services being outsourced by the RE and the threat environment; and

iv) CSP has mechanisms in place to assess the sub-contractors with regards to confidentiality, integrity and availability of the data being shared with the sub-contractors, where applicable.

e) Appropriate integration of logs, events from the CSP into the RE's SOC, wherever applicable and/ or retention of relevant logs in cloud shall be ensured for incident reporting and handling of incidents relating to services deployed on the cloud.

f) The RE's own efforts in securing its application shall be complemented by the CSP's cyber resilience controls. The CSP / RE shall ensure continuous and regular updates of security-related software including upgrades, fixes, patches and service packs for protecting the application from advanced threats/ malware.

g) Vulnerability Management: REs shall ensure that CSPs have a well-governed and structured approach to manage threats and vulnerabilities supported by requisite industry-specific threat intelligence capabilities.

7. **Disaster Recovery & Cyber Resilience**

a) The RE's business continuity framework 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.

b) REs shall ensure that the CSP puts in place demonstrative capabilities for preparedness and readiness for cyber resilience as regards cloud services in use by them. This should be systematically ensured, *inter alia*, through robust incident response and recovery practices including conduct of Disaster Recovery (DR) drills at various levels of cloud services including necessary stakeholders.

8. The following points may be evaluated while developing an exit strategy:

a) the exit strategy and service level stipulations in the SLA shall factor in, *inter alia,*

i) agreed processes and turnaround times for returning the RE's service collaterals and data held by the CSP;

ii) data completeness and portability;

iii) secure purge of RE's information from the CSP's environment;

iv) smooth transition of services; and

v) unambiguous definition of liabilities, damages, penalties and indemnities.

b) monitoring the ongoing design of applications and service delivery technology stack that the exit plans should align with.

c) contractually agreed exit / termination plans should specify how the cloud-hosted service(s) and data will be moved out from the cloud with minimal impact on continuity of the RE's business, while maintaining integrity and security.

d) All records of transactions, customer and operational information, configuration data should be promptly taken over in a systematic manner from the CSP and purged at the CSP-end and independent assurance sought before signing off from the CSP.

9. **Audit and Assurance**: The audit/ periodic review/ third-party certifications should cover, as per applicability and cloud usage, *inter alia*, aspects such as roles and responsibilities of both RE and CSP in cloud governance, access and network controls, configurations, monitoring mechanism, data encryption, log review, change management, incident response, and resilience preparedness and testing, etc.

Appendix – II

Outsourcing of Security Operations Centre

Outsourcing of Security Operations Centre (SOC) operations has the risk of data being stored and processed at an external location and managed by a third party (Managed Security Service Provider (MSSP)) to which REs have lesser visibility. To mitigate the risks, in addition to the controls prescribed in these Directions, REs shall adopt the following requirements in the case of outsourcing of SOC operations:

a) unambiguously identify the owner of assets used in providing the services (systems, software, source code, processes, concepts, etc.);

b) ensure 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);

c) assess SOC functioning, including all physical facilities involved in service delivery, such as the SOC and areas where client data is stored / processed periodically;

d) integrate the outsourced SOC reporting and escalation process with the RE's incident response process; and

e) review the process of handling of the alerts / events.

Appendix – III

Services not considered under Outsourcing of IT Services

A. Services / Activities <u>not considered</u> under "Outsourcing of IT Services" for the purpose of this Master Direction (an indicative but not exhaustive list)

i. Corporate Internet Banking services obtained by regulated entities as corporate customers/ sub members of another regulated entity

ii. External audit such as Vulnerability Assessment/ Penetration Testing (VA/PT), Information Systems Audit, security review

iii. SMS gateways (Bulk SMS service providers)

iv. Procurement of IT hardware/ appliances

v. Acquisition of IT software/ product/ application (like CBS, database, security solutions, etc.,) on a licence or subscription basis and any enhancements made to such licensed third-party application by its vendor (as upgrades) or on specific change request made by the RE.

vi. Any maintenance service (including security patches, bug fixes) for IT Infra or licensed products, provided by the Original Equipment Manufacturer (OEM) themselves, in order to ensure continued usage of the same by the RE.

vii. Applications provided by financial sector regulators or institutions like CCIL, NSE, BSE, etc.

viii. Platforms provided by entities like Reuters, Bloomberg, SWIFT, etc.

ix. Any other off the shelf products (like anti-virus software, email solution, etc.,) subscribed to by the regulated entity wherein only a license is procured with no/ minimal customisation

x. Services obtained by a RE as a sub-member of a Centralised Payment Systems (CPS) from another RE

xi. Business Correspondent (BC) services, payroll processing, statement printing

B. Vendors / Entities who are <u>not considered</u> as Third-Party Service Provider for the purpose of this Master Direction (an indicative but not exhaustive list)

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.

****