भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

RBI/2022-23/xx
DoS.CO.CSITEG/SEC.xx/31.01.015/2022-23 June 23, 2022

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 having asset size of ₹1000 crore and above;
Non-Banking Financial Companies in Top, Upper and Middle Layers;
Credit Information Companies; and
All India Financial Institutions (NHB, NABARD, SIDBI, EXIM Bank and NaBFID)

Madam/Dear Sir,

Draft Master Direction on Outsourcing of IT Services

Regulated Entities (REs) have been extensively leveraging Information Technology (IT) and IT enabled services (ITeS) to support their business models and products and services offered to their customers. REs also outsource substantial portion of their IT activities to third parties. Such reliance on IT/ ITeS provided by third parties expose the REs to significant risks.

2. In order to ensure effective management of attendant risks in outsourcing of IT activities, it was announced in the Statement on Developmental and Regulatory Policies released with the bi-monthly Monetary Policy Statement dated February 10, 2022, that draft guidelines on risk management framework for Outsourcing of IT Services, on managing related concentration risk, its periodic risk assessment and aspects of Outsourcing of IT Services to foreign service providers, will be issued by the Reserve Bank of India.

3. Accordingly, 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 in this regard, the

Reserve Bank proposes to prescribe a Master Direction on Outsourcing of IT Services as given in the **Annex**, to be implemented by the REs.

Yours faithfully,

(T.K.Rajan)
Chief General Manager

Encl: Annex

Annex

Draft Master Direction on Outsourcing of IT Services

1. Introduction

1.1 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 in this regard, the Reserve Bank being satisfied that it is necessary and expedient in the public interest to do so, hereby issues the Directions hereinafter specified.

1.2 Short title and commencement

a. These Directions shall be called the Reserve Bank of India (Outsourcing of IT Services) Directions, 2022.
b. In respect of revision to the "outsourcing agreement" clauses of the material Outsourcing of IT Services arrangements that are already in force, REs shall ensure that all such arrangements shall be revised/ finalised in compliance with these Directions at the time of renewal, but not later than ……....[*stakeholders may suggest what this date should be*]

1.3 Applicability

The provisions of these Directions shall be 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[1];
g) Credit Information Companies; and
h) All India Financial Institutions (NHB, NABARD, SIDBI, EXIM Bank and NaBFID)

1.4 Purpose: The underlying principle of these Directions is that the RE should ensure that outsourcing arrangements neither diminish its ability to fulfil its obligations to customers nor impede effective supervision by the supervising authority. REs desirous

[1] Ref: RBI/2021-22/112 DOR.CRE.REC.No.60/03.10.001/2021-22 circular on Scale Based Regulation (SBR): A Revised Regulatory Framework for NBFCs dated October 22, 2021

of outsourcing of IT and IT enabled services shall not require prior approval from RBI. However, such arrangements shall be subject to on-site/ off-site monitoring and inspection/ scrutiny by the supervising authority.

These Directions shall apply to material Outsourcing of IT Services arrangements (as defined in para 1.7 below) entered by the REs.

1.5 Service Provider: The term "Service provider" means the provider of IT/ IT enabled services[2] who may either be a member of the group / conglomerate to which the RE belongs, or an unrelated party. 'Service provider' includes, but is not limited to the vendors, agencies, consultants and / or representatives of the third parties[3]. It also includes sub-contractors to whom the third-party service providers may further outsource some activity.

1.6 Information Technology (IT) Outsourcing: 'Outsourcing of IT Services'[4] may be defined as an RE's use of a service provider to perform activities as listed below on a continuing basis. 'Continuing basis' would include agreements for a limited period. Outsourcing of IT Services mainly covers the following areas but not limited to:

a) IT infrastructure management, maintenance and support (hardware/ software/ firmware);
b) Network and security solutions maintenance (hardware/ software/ firmware);
c) Application Development, Maintenance and Testing;
d) Services and operations related to Data Centres;
e) Cloud Computing Services;
f) Managed Security Services;
g) Application Service Providers (ASPs) including ATM Switch ASPs[5]; and
h) Management of IT infrastructure and technology services associated with payment system ecosystem.

[2] Service provider engaged in handling/ managing/ storing and/ or processing data/ information/ IT infrastructure, as applicable, for/ on behalf of/ belonging to an RE.
[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.
[4] 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.
[5] The REs managing their ATM Switch ecosystem through shared services of third-party ATM Switch ASPs are also required to adhere to the instructions issued vide RBI circular DoS.CO/CSITE/BC.4084/31.01.015/2019-20 dated December 31, 2019 on "Cyber Security controls for Third party ATM Switch Application Service Providers" for cyber security related controls.

1.7 Material Outsourcing of IT Services: Material outsourcing arrangements are those, which if disrupted / compromised, have the potential to

(i) either significantly impact the RE's

(a) business operations, reputation, strategic plans or profitability or

(b) ability to manage risk and comply with applicable laws and regulations.

Or

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

1.8 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.

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

1.10 REs may consider applying these Directions to their non-material Outsourcing of IT Services arrangements also, if felt necessary, depending upon the risk perceived.

2. Criticality of Outsourcing of IT Services

2.1 The 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. In this process, RE shall consider important aspects, such as (a) determining need for outsourcing based on criticality of activity to be outsourced; (b) determining expectations / outcome from outsourcing; (c) determining success factors and cost-benefit analysis; and (d) deciding the model for outsourcing[6].

[6] For example, irrespective of CAPEX / OPEX, i. Developing a software, implementing software, consultancy etc.; ii. Managed services at RE's premises with infrastructure provided by the RE and skilled resourced provided by service provider; iii. Managed services where RE provides only data and service provider provides infrastructure, premises, and people; iv. Cloud services.

2.2 REs shall ensure that in the Outsourcing of IT Services engagement, wherein such outsourcing services support the RE's financial services, the applicable directions/ circulars[7] issued by RBI on managing risks and the code of conduct in outsourcing of financial services are adhered to.

3. RE's role in Outsourcing of IT Services- Regulatory and Supervisory requirements

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

3.2 Outsourcing of any activity of the RE shall not diminish its 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. Accordingly, the REs shall not engage an IT service provider that would result in reputation of RE being compromised or weakened.

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

3.4 REs shall ensure that the service provider shall neither impede/ interfere with the ability of the RE to effectively oversee and manage its activities nor impede the supervising authority in carrying out the supervisory functions and objectives.

---

[7] Circular DBOD.NO.BP.40/21.04.158/2006-07 dated November 3, 2006, Circular DBOD.No.BP.97/ 21.04.158/2008-09 dated December 11, 2008, Circular DBR.No.BP.BC.76/21.04.158/2014-15 dated March 11, 2015 on Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks; Circular DNBR.PD.CC.No.090/03.10.001/2017-18 Directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs dated November 09, 2017; Circular DOR.ORG.REC.27/21.04.158/2021-22 dated June 28, 2021 on Guidelines for Managing Risk in Outsourcing of Financial Services by Co-operative Banks.

3.5 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.

Grievance Redressal Mechanism

3.6 REs shall have a robust grievance redressal mechanism, which in no way shall be compromised on account of outsourcing i.e., responsibility for redressal of customers’ grievances related to outsourced services shall rest with the RE.

3.7 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.

4. Governance Framework

4.1 The 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, role and responsibilities of the Board, Board Committee and Senior Management, IT function, business function, and oversight & 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.

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

a) approving a framework to evaluate the risks and materiality of all existing and prospective IT outsourcing arrangements as also policies that apply to such arrangements;

b) putting in place a framework for approval of IT outsourcing activities depending on risks and materiality; and

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

4.3 Role of the Senior Management: The Senior Management 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 on 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 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
f) creating essential capacity with required skillsets within the organisation for proper oversight of outsourced activities.

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

a) assisting the Senior Management in identifying, measuring, 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 standard and provide uninterrupted services, and 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.

5. Evaluation and engagement of Service Providers

5.1 In considering or renewing an Outsourced 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. Due diligence shall take into consideration qualitative, quantitative, financial, operational, legal and reputational factors. REs shall also consider, while evaluating the capability of the service provider, risks arising from concentration of outsourcing arrangements with a single/ few service provider/s. Where possible, the RE shall obtain independent reviews and market feedback on the service provider to supplement its own assessment.

5.2 Due diligence shall involve an 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;
i) capability to comply with the regulatory and legal requirements of the Outsourcing of IT Services arrangement;
j) security risk assessment, including of the technology assets administered by the service provider;
k) ensuring that appropriate controls, assurance requirements and possible contractual arrangements are in place to establish data ownership;
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.

6. Outsourcing Agreement

6.1 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. 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.

6.2 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.

6.3 The agreement shall also bring out the nature of legal relationship between the parties, i.e., whether agent, principal or otherwise.

6.4 Some key areas that should be covered by the agreement (as applicable to the scope of Outsourcing of IT Services) are as follows:

a) definition of the IT 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) continuous monitoring and assessment of the service provider by the RE, so that any necessary corrective measure can be taken immediately; including termination clause and minimum period to execute such provision, if deemed necessary;
d) type of material adverse events (e.g., data breaches, denial of service, service unavailability etc.) and incident reporting requirements to the RE to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines;
e) compliance with the provisions of IT Act, 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 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 to 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 of the RE outsourced to the service provider;
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 resources of service provider who provide core services as "essential personnel" so that a limited number of staff necessary to operate

critical functions can work on-site during exigencies (including pandemic situations); and

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

7. Risk Management

7.1 A Risk Management framework for Outsourcing of IT Services shall comprehensively deal with the processes and responsibilities for identification, measurement, mitigation/ management and reporting of risks associated with Outsourcing of IT Services arrangements.

7.2 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/ external quality assurance on a periodic basis.

7.3 REs shall be responsible for the confidentiality and integrity of data / information pertaining to the customers that is available to the service provider. Also, 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.

Public confidence and customer trust in REs is a prerequisite for their stability and reputation. Hence the 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”.

7.4 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.

7.5 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. REs shall ensure that a Non-Disclosure Agreement (NDA) is in place even after the contract expires/is terminated.

7.6 REs shall 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 immediately but not later than one hour of detection.

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 the supervising authority in the event of breach of security and leakage of confidential customer related information. In these eventualities, REs shall adhere to the baseline expectations of Incident Response and Recovery Management[8].

7.7 Management of 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.

7.8 Business Continuity Plan and Disaster Recovery Plan

7.8.1 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 BCP/ DR requirements[9].

7.8.2 Wherever REs or service provider(s) are required to telework for ensuring business continuity, the baseline expectations on controls on teleworking prescribed in Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 2022[10] shall be adhered to.

[8] Ref to Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 2022 (for the definition of incident and section on incident response and recovery management), to be issued shortly for comments of stakeholders and members of public

[9] Ref to Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 2022 (section on Business Continuity Management), to be issued shortly for comments of stakeholders and members of public

[10] to be issued shortly for comments of stakeholders and members of public

7.8.3 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.

7.8.4 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.

7.8.5 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 and/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 in order to continue its business operations, or deleted, destroyed or rendered unusable.

8. Monitoring and Control of Outsourced Activities

8.1 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/ resources, service availability, adherence to SLA requirements, incident response mechanism, etc.

8.2 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 periodic audits shall assess the performance of the service provider, adequacy of the risk management practices adopted by the service provider, compliance with laws/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.

8.3 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.

8.4 The RE shall, at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet its Outsourcing of IT Services obligations. Such due diligence reviews shall highlight any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness.

8.5 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.

8.6 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.

9. Outsourcing within a Group/ Conglomerate

9.1 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.

9.2 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.

9.3 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.

9.4 Additionally, the following considerations shall also be taken into account.

a) agreements shall cover demarcation of shared resources like premises, personnel, technology infrastructure, details of data sharing (if any), etc.
b) details like scope of services, charges for services and maintaining confidentiality of customer's data shall be appropriately documented;
c) these arrangements should not compromise the ability of the RE to identify and manage risks on a standalone basis; and
d) these arrangements should not prevent RBI from being able to obtain information required for supervision of the RE or pertaining to the group as a whole.

9.5 The RE's advertisement or any agreement shall not give any overt or tacit impression that it is in any way responsible for the obligations of its group entities.

9.6 REs, at all times, shall maintain arm's length relationship in dealings with their group entities.

10. Additional requirements for cross-border outsourcing

10.1. 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 the service provider's country's government policies and its political, social, economic and legal conditions on a continuous basis, and 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 supervising authority will not be affected even in case of liquidation of the service provider.

10.2 In principle, arrangements shall only be entered into with parties operating in jurisdictions generally upholding confidentiality clauses and agreements. The governing law of the arrangement shall also be clearly specified. However, the jurisdiction of the courts outside India, where data is stored and/ or processed, shall not extend to the operations of the RE in India, on the strength of the fact that the RE's data is being stored and/ or processed there, even though the actual transactions are undertaken in India.

10.3 The right to conduct audit/ inspection of the service provider based in a different jurisdiction shall be ensured.

10.4 The arrangement shall comply with law/ regulations issued by RBI from time to time.

11. Exit Strategy

11.1 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 (e.g., change of service provider ownership, liquidation, merger/ acquisition, undesirable changes due to change in regulatory requirements affecting the service provider, security breach, regulatory action on the service provider, etc.) 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.

11.2 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 smooth transition and to agree to not to erase, purge, revoke, alter or change any data during the transition period, unless specifically advised by the regulator/ concerned RE.

11.3 REs shall require the service provider to preserve documents as required by law and take suitable steps to ensure that REs' interests are protected, even post termination of the services. REs may execute a non-disclosure agreement with respect to information retained by the service provider.

Appendix-I

Storage, Computing and Movement of Data in Cloud Environments- Usage of Cloud Computing Services

There are several popular 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[11] come with corresponding service, business benefit and risk profiles.

In addition to the Outsourcing of IT Services controls prescribed in **Annex**, 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[12]. 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, that is, 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 attended risks, while establishing appropriate risk management framework.
4. **Cloud Governance:** REs shall adopt and demonstrate a well-established and documented cloud adoption policy. Such a policy should, *inter alia*, identify the

[11] For example, some popular 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.

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

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 cast under Indian laws 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 enable smooth recovery and any failure of any one or combination of components across the cloud architecture should not result in data/ information security compromise.

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' and require the RE's approval and monitoring. 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.

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 real-time 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 Center (SOC)

10. Outsourcing of 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 **Annex**, REs shall adopt the below mentioned 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.