भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

RBI/DOR/2025-26/171
DOR.ORG.REC.No.90/21-04-158/2025-26 November 28, 2025

Reserve Bank of India (Commercial Banks – Managing Risks in Outsourcing) Directions, 2025

Table of Contents

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

Chapter I – Preliminary

A. Short Title and Commencement

1. These Directions shall be called the Reserve Bank of India (Commercial Banks - Managing Risks in Outsourcing) Directions, 2025.

2. These Directions shall come into force with immediate effect.

   Provided that a bank's existing Information Technology (IT) outsourcing agreements regardless of whether they are due for renewal on or after the effective date of these Directions shall comply with the provisions of these Directions either at the time of renewal or by **April 10, 2026**, whichever is earlier. However, the bank's new IT outsourcing agreements that come into force on or after the effective date of these Directions, shall comply with the provisions of these Directions from the date of agreement itself.

   Provided further that nothing in the preceding proviso shall be construed as permitting non-compliance with any other extant regulatory instructions or statutory requirements applicable to such arrangements.

B. Applicability and Scope

3. These Directions shall be applicable to Scheduled Commercial Banks (hereinafter collectively referred to as 'banks' and individually as a 'bank').

   For the purpose of these Directions, 'Commercial Banks' means banking companies (other than Small Finance Banks, Local Area Banks, Payments Banks and Regional Rural Banks), corresponding new banks, and the State Bank of India, as defined respectively under clauses (c), (da), and (nc) of section 5 of the Banking Regulation Act, 1949.

Provided that in respect of foreign banks operating in India through branch mode, any reference to the Board or Board of Directors in these Directions shall be read as a reference to the Head Office or Controlling Office that has oversight over the branch operations in India. Additionally, with respect to the Directions contained in Chapter IV regarding outsourcing of IT services, foreign banks shall be subject to a 'comply or explain' approach, which shall allow them to deviate from any specific provision of those Directions, subject to examination and acceptance by RBI of a reasonably justifiable explanation for such deviation.

4. The scope of provisions contained in Chapter III shall be as under:

(1) The provisions shall apply to outsourcing arrangements entered into by a bank with a service provider which may be either a member of the group / conglomerate to which the bank belongs, or an unrelated party, which is located in India or elsewhere, for outsourcing of financial services like applications processing (loan origination, credit card), document processing, marketing and research, supervision of loans, data processing and back office related activities.

Provided that for outsourced services relating to credit cards, the provisions set out in the Reserve Bank of India (Commercial Banks – Credit Cards and Debit Cards: Issuance and Conduct) Directions, 2025, as amended from time to time, shall also apply to the applicable entities.

(2) The provisions shall also apply, *mutatis mutandis*, to subcontracted activities. For this purpose, the outsourcing contract shall provide for prior approval or consent of the bank before a service provider engages any subcontractor for all or part of the outsourced activity. Before granting such consent, the bank shall review the subcontracting arrangement and ensure that the same complies with the Directions set out in Chapter III of these Directions.

(3) The provisions shall not apply to outsourcing of:

(i) IT services as defined in paragraph 53(1) of these Directions, unless specified otherwise in respective paragraphs of Chapter IV;

(ii) activities unrelated to banking services like usage of courier, catering of staff, housekeeping and janitorial services, security of the premises, and movement and archiving of records; and

(iii) audit-related assignments to Chartered Accountant firms which shall continue to be governed by the instructions and guidelines issued by the Department of Supervision, RBI.

5. The scope of provisions contained in Chapter IV shall be as under:

(1) The provisions shall apply to a bank's material outsourcing of IT services, as defined in paragraph 53(2). In this context, 'Outsourcing of IT Services' shall include outsourcing of the following services:

(i) IT infrastructure management, maintenance and support (hardware, software or firmware);

(ii) network and security solutions, and maintenance (hardware, software or firmware);

(iii) application development, maintenance, and testing by Application Service Providers (ASPs) including ATM Switch ASPs;

(iv) services and operations related to data centres;

(v) cloud computing services;

(vi) managed security services; and

(vii) management of IT infrastructure and technology services associated with payment system ecosystem.

(2) The provisions shall not apply to the following services:

(i) corporate internet banking services obtained by a bank as a corporate customer or sub-member of another Regulated Entity (RE);

Provided that for the purpose of these Directions, the following indicative (but not exhaustive) list of entities shall be considered as REs – other Commercial Banks; Local Area Banks; Small Finance Banks; Payments

Banks; Regional Rural Banks; Non-Banking Financial Companies in Base Layer (NBFC - BL), Middle Layer (NBFC - ML), and Upper Layer (NBFC – UL); All India Financial Institutions; Credit Information Companies; Urban Co-operative Banks; Rural Co-operative Banks; and, Payment System Operators;

(ii) external audit services such as Vulnerability Assessment (VA) / Penetration Testing (PT), Information Systems Audit, and security review;

(iii) SMS gateways (including bulk SMS service providers);

(iv) procurement of IT hardware or appliances;

(v) acquisition of IT software, product or application (e.g., Core Banking Solution (CBS), database, and security solutions) on a licence or subscription basis, and any enhancements made to such licensed third-party applications by the vendor (as upgrades) or on specific change request made by a bank;

(vi) any maintenance service (including security patches, and bug fixes) for IT infrastructure or licensed products, provided by the Original Equipment Manufacturer (OEM) themselves, in order to ensure continued usage of the same by the bank;

(vii) applications provided by financial sector regulators or institutions such as Clearing Corporation of India Limited (CCIL), National Stock Exchange (NSE), and Bombay Stock Exchange (BSE);

(viii) platforms provided by entities such as Reuters, Bloomberg, and Society for Worldwide Interbank Financial Telecommunication (SWIFT);

(ix) any other off-the-shelf products (e.g., anti-virus software, and email solutions) subscribed to by a bank, wherein only a license is procured with no or minimal customisation;

(x) services obtained by a bank as a sub-member of a Centralised Payment System (CPS) from another RE;

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

C. Definitions

6. In these Directions, unless the context otherwise requires,

(1) '**Outsourcing**' means use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) by a bank to perform activities on a continuing basis that would normally be undertaken by the bank itself, now or in the future. 'Continuing basis' shall include agreements for a limited period.

(2) **'Group'** shall be as defined in the Reserve Bank of India (Commercial Banks – Concentration Risk Management) Directions, 2025, as amended from time to time, for the purpose of intragroup transactions and exposures;

7. Some other terms pertaining to outsourcing of financial services and IT services have been defined in their respective Chapters as per their applicability.

8. All other 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 the Information Technology Act, 2000 or the Companies Act, 2013 and Rules made thereunder, or any statutory modification or re-enactment thereto, or Glossary of Terms published by RBI or as used in commercial parlance, as the case may be.

Chapter II – Role of the Board

9. The outsourcing of any activity by a bank does not diminish its obligations, and those of its Board and Senior Management, who have the ultimate responsibility for the outsourced activity.

A. Board-Approved Policy

10. A bank intending to outsource any of its financial or IT activities shall put in place corresponding comprehensive Board-approved outsourcing policy, the coverage of which is indicated in paragraph 20 and paragraph 57, respectively.

B. Key Responsibilities

11. The Board or a Committee of the Board to which powers have been delegated, as applicable for financial or IT outsourcing, shall be responsible for putting in place a framework to evaluate the risks and materiality of all existing and prospective outsourcing arrangements, laying down appropriate approval authorities depending on risks and materiality, and undertaking regular review.

12. In respect of outsourcing of financial services,

    (1) the Board, or a Committee of the Board to which powers have been delegated, shall be responsible, *inter alia,* for:

        (i) approving a framework to evaluate the risks and materiality of all existing and prospective outsourcing arrangements, and the policies that apply to such arrangements;

        (ii) laying down appropriate approval authorities for outsourcing depending on risks and materiality;

        (iii) undertaking regular review of outsourcing strategies and arrangements for their continued relevance, and safety and soundness;

        (iv) deciding on business activities of a material nature to be outsourced, and approving such arrangements;

        (v) reviewing records of all material outsourcing on half-yearly basis; and

(vi) ensuring submission of an Annual Compliance Certificate giving the particulars of contracts for outsourcing of financial services, the prescribed periodicity of audit by internal or external auditor, major findings of the audit, and action taken to the Department of Supervision, RBI.

(2) the Audit Committee of the Board (ACB) of a bank shall:

(i) monitor the system of internal audit of all outsourced activities; and

(ii) review the ageing analysis of entries pending reconciliation with outsourced vendors and make efforts to reduce the old outstanding items therein at the earliest.

13. In respect of outsourcing of IT services, the Board shall be responsible, *inter alia,* for:

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

(ii) approving policies to evaluate the risks and materiality of all existing and prospective outsourcing arrangements;

(iii) setting up suitable administrative framework of Senior Management;

(iv) ensuring either by itself or through its Committee that there is no conflict of interest arising out of third-party engagements, especially when permitting an exception to the requirement that the service provider of outsourced services, if not a group company, shall not be owned or controlled by any director, key managerial personnel, approver of the outsourcing arrangement, or their relatives as indicated under the proviso to paragraph 54 of these Directions; and

(v) reviewing any adverse development mentioned in reports put up to Senior Management on the monitoring and control activities.

Chapter III – Outsourcing of Financial Services

A. Definitions

14. In this Chapter, unless the context otherwise requires, **'Material Outsourcing'** means arrangements, which if disrupted, have the potential to significantly impact the business operations, reputation or profitability of a bank. 'Materiality' of outsourcing shall be based on the:

    (i) level of importance to the bank of the activity being outsourced;

    (ii) potential impact of the outsourcing on the bank on various parameters such as earnings, solvency, liquidity, funding, capital, and risk profile;

    (iii) likely impact on the bank's reputation and brand value, and ability to achieve its business objectives, strategy, and plans, should the service provider fail to perform the service;

    (iv) cost of the outsourcing as a proportion of total operating costs of the bank; and

    (v) aggregate exposure to that particular service provider, in cases where the bank outsources various functions to the same service provider.

B. Activities that shall not be outsourced

15. A bank which chooses to outsource financial services shall however not outsource core management functions including Internal Audit, compliance function, and decision-making functions like determining compliance with KYC norms for opening deposit accounts, giving sanction for loans (including retail loans), and management of investment portfolio.

C. Authorisation, Accountability, and Oversight

16. A bank which desires to outsource financial services, shall not require prior approval from RBI whether the service provider is located in or outside India.

17. As stated in paragraph 9, the outsourcing of any activity by a bank shall not diminish its obligations including to its customers and RBI, and those of its Board and Senior Management, who have the ultimate responsibility for the outsourced

activity. The bank shall, therefore, be responsible for the actions of its service provider including Direct Sales Agents (DSAs) / Direct Marketing Agents (DMAs) and recovery agents, and the confidentiality of information pertaining to the customers that is available with the service provider. The bank shall retain ultimate control of the outsourced activity.

18. A bank shall ensure that:

(i) all relevant laws, regulations, rules, guidelines and conditions of approval, licensing or registration have been considered when performing due diligence in relation to outsourcing;

(ii) outsourcing, whether the service provider is located in India or outside, does not impede RBI in carrying out its supervisory functions and objectives, or diminish the ability of a bank to fulfil its obligations to the regulator / supervisor;

(iii) outsourcing, whether the service provider is located in India or outside, does not impede or interfere with the ability of a bank to effectively oversee and manage its activities, and fulfil its obligations;

(iv) outsourcing would not result in the compromise or weakening of a bank's internal control, business conduct, or reputation;

(v) the service provider employs the same high standard of care in performing the services as would be employed by the bank, if the activities were conducted within the bank and not outsourced; and

(vi) the service provider, if not a subsidiary of the bank, shall not be owned or controlled by any director or officer / employee of the bank or their relatives having the same meaning as assigned under Companies Act, 2013 and the Rules framed thereunder, as amended from time to time.

19. A bank shall be responsible for making Currency Transactions Reports (CTRs) and Suspicious Transactions Reports (STRs) to FIU or any other competent authority in respect of its customer related activities carried out by the service providers.

D. Governance Framework

D.1 Outsourcing Policy

20. A bank intending to outsource any of its financial services shall put in place a comprehensive outsourcing policy, approved by its Board, which shall incorporate, *inter alia,* the following*:*

    (i) criteria for selection of such activities, and service providers;

    (ii) parameters for defining 'material outsourcing' based on the broad criteria indicated in paragraph 14 of these Directions;

    (iii) delegation of authority depending on risks, and materiality; and

    (iv) systems to monitor and review these activities.

D.2 Role of Senior Management

21. The Senior Management of a bank shall, *inter alia,* be responsible for:

    (i) evaluating the risks and materiality of all existing and prospective outsourcing, based on the framework approved by the Board or a Committee of the Board;

    (ii) developing and implementing sound and prudent outsourcing policies and procedures commensurate with the nature, scope, and complexity of the outsourcing;

    (iii) reviewing periodically the effectiveness of policies and procedures;

    (iv) communicating information pertaining to material outsourcing risks to the Board in a timely manner;

    (v) ensuring that contingency plans, based on realistic and probable disruptive scenarios, are in place and tested;

    (vi) ensuring that there is independent review and audit for compliance with set policies; and

    (vii) undertaking periodic review of outsourcing arrangements to identify new material outsourcing risks as they arise.

E. Risk Management

E.1 Evaluation of the Risks

22. A bank shall evaluate and guard against the following key risks when entering into outsourcing arrangements:

(i) **Strategic Risk** – such as where the service provider conducts business on its own behalf, inconsistent with the overall strategic goals of the bank.

(ii) **Reputation Risk** – such as where the service provider delivers poor service, or its customer interactions are inconsistent with the overall standards of the bank.

(iii) **Compliance Risk** – such as where, owing to outsourcing, the privacy, consumer, and prudential laws are not adequately complied with.

(iv) **Operational Risk** – which may arise due to technology failure, fraud, error, or inadequate financial capacity of the service provider to fulfil obligations or to provide remedies.

(v) **Legal Risk** – where a bank is subjected to, *inter alia,* fines, penalties, or punitive damages resulting from supervisory actions, or private settlements due to omissions and commissions by the service provider.

(vi) **Exit Strategy Risk** – may arise when a bank becomes over reliant on one service provider, loses relevant internal skills preventing it from bringing the activity back in-house, or enters into contracts that make speedy exits prohibitively expensive.

(vii) **Counterparty Risk** – such as where the service provider engages in inappropriate underwriting or credit assessments.

(viii) **Country Risk** – where the political, social, or legal climate creates added risk in the outsourcing arrangement.

(ix) **Contractual Risk** – where the bank may not have the ability to enforce the contract with the service provider.

(x) **Concentration and Systemic Risk** – where there is a lack of control of a bank over a service provider, more so when overall banking industry has considerable exposure to one service provider.

E.2 Confidentiality and Security of Information

23. A bank shall seek to ensure the security, preservation, and protection of the customer information in the custody or possession of the service provider.

24. Access to customer information by a service provider or its staff shall be on a 'need to know' basis, i.e., limited to those areas where the information is required in order to perform the outsourced function.

25. A bank shall review and monitor the security practices and control processes of its service providers on a regular basis and require the service provider to disclose security breaches.

26. In instances, where a service provider acts as an outsourcing agent for multiple entities, the bank shall take care to build strong safeguards so that there is no comingling or combining of information, documents, records, and assets.

27. A bank shall ensure that a service provider is able to isolate and clearly identify the bank's customer information, documents, records, and assets to protect the confidentiality of the information.

28. A bank shall immediately notify RBI in the event of breach of security and leakage of confidential customer related information. In these eventualities, the bank shall be liable to its customers for any damage.

F. Outsourcing Process

F.1 Service Provider Evaluation

29. A bank shall perform appropriate due diligence while considering or renewing an outsourcing arrangement, to assess the capability of the service provider to comply with obligations in the outsourcing agreement on an ongoing basis.

30. The due diligence mentioned above shall involve an evaluation of all available information, as applicable, about the service provider, including but not limited to:

(i) qualitative, quantitative, financial, operational, legal, and reputational factors;

(ii) risks arising from undue concentration, if outsourcing to a single service provider, or a limited number of service providers;

(iii) past experience, and demonstrated competence to implement and support the proposed activity over the contracted period;

(iv) financial soundness, and ability to service commitments even under adverse conditions;

(v) business reputation and culture, compliance, complaints, and outstanding or potential litigation;

(vi) quality of due diligence exercised by the service provider of its employees and sub-contractors;

(vii) security and internal control, audit coverage, reporting, and monitoring procedures, and business continuity management; and

(viii) 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.

31. Where possible, a bank shall obtain independent reviews and market feedback on the service provider to supplement the findings of its own due diligence.

32. A bank shall also evaluate whether the systems of its service provider are compatible with those of the bank, and the acceptability of their standards of performance including in the area of customer service.

F.2 Outsourcing Agreement

33. A bank shall ensure that the terms and conditions governing the outsourcing arrangement are carefully defined in written agreements and vetted by the bank's legal counsel on their legal effect and enforceability. The agreement shall appropriately reckon the associated risks and the strategies for mitigating or managing them. The bank shall ensure that such an agreement is sufficiently flexible to allow it to retain an appropriate level of control over the outsourcing, and

the right to intervene with appropriate measures to meet legal and regulatory obligations. The agreement shall also bring out the nature of legal relationship between the parties, i.e., whether agent-principal or otherwise.

34. Some of the key provisions of the agreement shall include:

(i) details of the activity being outsourced, including appropriate service, and performance standards;

(ii) bank's access to all books, records, and information relevant to the outsourced activity available with the service provider;

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

(iv) prior approval or consent by the bank for the use of subcontractors by the service provider for all, or part of an outsourced activity as set out in paragraph 4(2)of these Directions;

(v) controls for maintaining confidentiality of data including of its customers, and incorporating service provider's liability in the event of security breach and leakage of such confidential information;

(vi) contingency plans to ensure business continuity;

(vii) bank's right to conduct audits on the service provider 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 on the service provider in conjunction with the services performed for the bank;

(viii) right of RBI or persons authorised by it to access the bank's documents, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time; including in cases where the controlling / Head Offices of foreign banks operating in India outsource the activities related to the Indian operations;

(ix) right of RBI to cause an inspection to be made of the service provider by one or more of its officers, employees or other authorised persons; including in cases where the controlling / Head Offices of foreign banks operating in India outsource the activities related to the Indian operations;

(x) a termination clause and minimum period for executing termination, if deemed necessary;

(xi) provision that confidentiality of customers' information shall be maintained even after the contract expires or gets terminated; and

(xii) provisions to ensure that the service provider preserves documents and data in accordance with legal and regulatory obligations of the bank.

F.3 Monitoring and Control of Outsourced Activities

35. A bank shall have in place a management structure to monitor and control its outsourced activities and shall ensure that outsourcing agreements with its service provider contain provisions to address the same.

36. A bank shall maintain a central record of all material outsourcing of financial services for review by its Board and Senior Management. The records shall be updated promptly, and half-yearly reviews shall be placed before the Board.

37. Regular audits, by either the internal auditors or external auditors of a bank, shall assess the adequacy of the risk management practices adopted in overseeing and managing the outsourcing arrangement, the bank's compliance with its risk management framework, and the requirements of these Directions.

38. A bank 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 obligations. Such due diligence reviews, which shall be based on all available information about the service provider, shall highlight any deterioration or breach in performance standards, confidentiality, and security, and in operational resilience or business continuity preparedness.

39. Certain services, viz., outsourcing of cash management, might involve reconciliation of transaction between a bank and the service provider (or its

subcontractors). In such cases, the bank shall ensure that reconciliation of transactions between itself and the service provider (or its subcontractors) is carried out in a timely manner. A bank shall ensure that the reconciliation is carried out as advised in RBI guidelines on 'Outsourcing of Cash Management – Reconciliation of Transactions' dated May 14, 2019, as amended from time to time.

F.4 Business Continuity and Management of Disaster Recovery Plan

40. A bank shall require its service provider to develop and establish a robust framework for documenting, maintaining, and testing business continuity and recovery procedures. The bank shall ensure that the service provider periodically tests the Business Continuity and Recovery Plan and may also consider occasional joint testing and recovery exercises with its service provider.

41. In establishing a viable contingency plan, a bank 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.

42. A bank shall ensure that its service providers are able to isolate the bank's information, documents, and records, and other assets so that in adverse conditions or termination of the agreement, all documents, records of transactions and information with the service provider, and assets of the bank, can be removed from the possession of the service provider (in order to continue its business operations), or deleted, destroyed, or rendered unusable.

43. In order to mitigate the risk of unexpected termination of the outsourcing agreement, or insolvency or liquidation of its service provider, a bank shall retain an appropriate level of control over its outsourcing arrangement along with the right to intervene with appropriate measures to continue its business operations without incurring prohibitive expenses and disruption in the operations of the bank and its services to the customers.

F.5 Termination

44. If the services of a service provider are terminated by a bank, then it shall:

(i) publicise the same so as to ensure that its customers do not continue to deal with the service provider; and

(ii) inform Indian Banks' Association (IBA) of the reasons for termination to enable IBA to maintain a caution list of such service providers for sharing among banks.

G. Specific Outsourcing Arrangements

G.1 Outsourcing within a Group / Conglomerate

45. (1) In a group structure, a bank may have back-office and service arrangements or agreements with group entities such as sharing of premises, legal and other professional services, hardware and software applications and centralized back-office functions; outsourcing certain financial services to other group entities. In principle, the risk management practices to be adopted by a bank while outsourcing to a related party (i.e., party within the group / conglomerate) shall be identical to those for a non-related party.

(2) While entering into such arrangements, a bank shall ensure that these:

(i) are appropriately documented in written agreements with details like scope of services, charges for the services and maintaining confidentiality of the customer's data;

(ii) do not lead to any confusion to the customers on whose products / services they are availing;

(iii) do not compromise the ability of the bank to identify and manage risk on a stand-alone basis;

(iv) do not impinge on safety and soundness of the bank a stand-alone entity;

(v) do not prevent RBI from being able to obtain information required for the supervision of the bank or pertaining to the group as a whole; and

(vi) incorporate a clause under the written agreements that there is a clear obligation for any service provider to comply with directions given by RBI in relation to the activities of the bank.

(3) A bank shall ensure that its ability to carry out its operations in a sound fashion would not be affected, if premises or other services (such as IT systems and support staff) provided by the group entities become unavailable.

(4) If the premises of a bank are shared with the group entities for the purpose of cross-selling, the bank shall take measures to ensure that the entity's identification is distinctly visible and clear to the customers. The marketing brochure used by the group entity and verbal communication by its staff / agent in the bank's premises shall mention nature of arrangement of the entity with the bank so that the customers are clear on the seller of the product.

(5) A bank shall not publish any advertisement or enter into any agreement stating or suggesting or giving tacit impression that it is in any way responsible for the obligations of its group entities.

G.2 Offshore outsourcing

46. In principle, outsourcing arrangements shall only be entered into with parties operating in jurisdictions that uphold confidentiality agreements and clauses.

47. While engaging with service provider(s) in a foreign country, a bank shall:

(i) closely monitor government policies of the jurisdiction in which the service provider is based and political, social, economic, and legal conditions, both during the risk assessment and on a continuous basis, and establish sound procedures for dealing with country risk. This includes having appropriate contingency and exit strategies;

(ii) clearly specify the governing law of the outsourcing arrangement;

(iii) ensure that the availability of records to the bank and RBI will not be affected even in the case of liquidation of the service provider or offshore custodian;

(iv) ensure activities outsourced outside India are conducted in a manner so as not to hinder efforts to supervise or reconstruct the activities of the bank in a timely manner;

(v) ensure that, where the offshore service provider is a regulated entity, the relevant offshore regulator will neither obstruct the arrangement nor object to the RBI's inspections or visits of bank's internal or external auditors;

(vi) ensure that the regulatory authority of the offshore location does not have access to the data relating to Indian operations of the bank simply on the ground that the processing is being undertaken there;

(vii) ensure that the jurisdiction of the courts in the offshore location where data is maintained does not extend to the operations of the bank in India on the strength of the fact that the data is being processed there even though the actual transactions are undertaken in India; and

(viii) ensure that all original records continue to be maintained in India.

48. The overseas operations of a bank shall be governed by both, these Directions and the host country guidelines, and in case there are differences, the more stringent of the two shall prevail. However, where there is any conflict, the host country guidelines shall prevail.

H. Redressal of Grievances related to Outsourced Services

49. Outsourcing arrangements entered into by a bank shall not affect the rights of its customers against the bank, including the ability of the customers to obtain redressal as applicable under relevant laws.

50. In cases where customers are required to deal with a service provider in the process of dealing with a bank, the bank shall incorporate a clause in the corresponding product literature, and brochures, stating that services of the service provider, including in sales and marketing of the products, may be used. The role of the service provider may be indicated in broad terms.

51. A bank 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 bank. In case of microfinance loans, a declaration that, (i) the bank shall be accountable for inappropriate behaviour of the employees of the service provider and (ii) shall provide timely grievance redressal, shall be made in the loan agreement, and in Fair Practices Code (FPC) displayed in its office, branch premises, and its website.

52. In addition to the above,

(1) a bank shall constitute Grievance Redressal Machinery in accordance with the provisions of Reserve Bank of India (Commercial Banks - Responsible Business Conduct) Directions, 2025, and give wide publicity about it within the bank through electronic and print media;

(2) the name and contact number of designated grievance redressal officer of the bank shall be made known and widely publicised. The designated officer shall ensure that genuine grievances of customers are redressed promptly without involving delay. It shall be clearly indicated that bank's Grievance Redressal Machinery will also deal with the issue relating to services provided by the service provider; and

(3) the time frame fixed for responding to the complaints (maximum 30 days) shall be placed on the bank's website. If a complaint is rejected wholly or partly by a bank, and the complainant is not satisfied with the reply, or does not get any reply within 30 days after the bank received the complaint, the complainant shall have the option to seek grievance redressal under the RBI's Integrated Ombudsman Scheme, 2021.

Chapter IV – Outsourcing of Information Technology (IT) Services

A. Definitions

53. In this Chapter, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

(1) '**IT services**' means IT services / IT enabled services /IT activities.

(2) '**Material Outsourcing of IT Services**' are those which:

(i) if disrupted or compromised shall have the potential to significantly impact the bank's business operations; or

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

(3) '**Service Provider**' means provider of IT services including entities related to the bank, or those which belong to the same group or conglomerate to which the bank belongs.

Provided that for the purpose of this Chapter, the following indicative (but not exhaustive) list of vendors and entities shall not be considered as 'Service Providers' as defined above:

(i) vendors providing business services using IT (e.g., BCs;);

(ii) Payment System Operators (PSOs) authorised by RBI 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, products, and services (would be considered under outsourcing of financial services in Chapter III);

(iv) FinTech firms providing services for data retrieval, and data validation and verification, such as, bank statement analysis, GST returns analysis, fetching of vehicle information, digital document execution, 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 data; and

(vi) security or audit consultants appointed for certification, audit or VA / PT related to IT infrastructure, IT services, or Information Security services, in their role as independent third-party auditor, consultant, or lead implementer.

Explanation: In case an IT service is provided by an RE to a bank (as applicable to the scope of Directions under this Chapter), even the RE could be considered as a service provider to the bank, under this Chapter.

(4) '**Sub-contractor**' refers to those providing material / significant IT services to the service provider and is specific to the material / significant IT services arrangement that the bank has entered into with the service provider.

B. Authorisation, Accountability, and Oversight

54. In addition to adhering to the requirements stipulated in subparagraphs (i) to (v) of paragraph 18 of these Directions, a bank 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 bank, or their relatives. The terms 'control', 'director', 'key managerial personnel', and 'relative' shall have the same meaning as assigned under the Companies Act, 2013 and the Rules framed thereunder from time to time.

Provided that an exception to the above requirement may be made with the approval of Board or a Committee of the Board, followed by appropriate disclosure, oversight and monitoring of such arrangements.

55. A bank shall evaluate the need for outsourcing of IT services based on a comprehensive assessment of attendant benefits, risks, and availability of commensurate processes to manage those risks. For this purpose, the bank shall, *inter alia*, consider the following:

(i) the need for outsourcing based on materiality / criticality of service to be outsourced;

(ii) expectations and outcomes from outsourcing;

(iii) success factors and cost-benefit analysis; and

(iv) the model for outsourcing.

56. A bank shall ensure that cyber incidents are reported to it by the service provider without undue delay, so that an incident is reported by the bank to the RBI within six hours of detection by the service provider.

C. Governance Framework

C.1 Outsourcing Policy

57. A bank intending to outsource any of its IT services shall put in place a comprehensive Board-approved IT outsourcing policy incorporating, *inter alia*, the following:

(i) the roles and responsibilities of the Board, Committees of the Board (if any) and Senior Management, IT function, business function, and oversight and assurance functions in respect of outsourcing of IT services;

(ii) criteria for selection of such services and service providers;

(iii) parameters for defining material outsourcing based on the broad criteria defined in paragraph 53(2) of these Directions;

(iv) delegation of authority depending on risk and materiality;

(v) disaster recovery and business continuity plans;

(vi) systems to monitor and review the operations of these services; and

(vii) termination processes and exit strategies, including business continuity in the event of a service provider exiting the outsourcing arrangement.

C.2 Role of Senior Management

58. The Senior Management of a bank shall, *inter alia*, be responsible for:

(i) 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 bank approved by the Board and its implementation;

(ii) 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;

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

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

(v) ensuring (a) effective oversight over the service provider (and its subcontractors) for data confidentiality, and (b) appropriate redressal of customer grievances in a timely manner;

(vi) 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 or a Committee of the Board; and

(vii) creating essential capacity with required skillsets within the bank for proper oversight of outsourced services.

C.3 Role of IT Function

59. The responsibilities of the IT Function of a bank shall, *inter alia*, include:

(1) assisting the Senior Management in identifying, measuring, monitoring, mitigating, and managing the level of IT outsourcing risk in the bank;

(2) ensuring that a central database of all IT outsourcing arrangements is maintained and is accessible for review by Board, Senior Management, auditors, and supervisors;

(3) effectively monitoring and supervising the outsourced IT service to ensure that the service provider meets the laid down performance standards and provides uninterrupted services, reporting to the Senior Management, co-ordinating periodic due diligence, and highlighting concerns, if any; and

(4) 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.

D. Risk Management

D.1 Risk Management Framework

60. A bank shall put in place a risk management framework that comprehensively deals with the processes and responsibilities for identification, measurement, mitigation, management, and reporting of risks associated with such IT outsourcing arrangements.

61. A bank shall suitably document risk assessments with necessary approvals in line with the roles and responsibilities of the Board of Directors, Senior Management, and IT Function, and subject the same to internal and external quality assurance on a periodic basis as determined by the Board-approved policy.

62. A bank shall effectively assess the impact of concentration risk posed by multiple outsourcing arrangements to the same service provider and the concentration risk posed by outsourcing critical or material functions to a limited number of service providers.

D.2 Confidentiality and Security of Information

63. A bank shall be responsible for the confidentiality, and integrity of data and information pertaining to its customers that are available to the service provider.

64. In this regard, a bank shall adhere to directions stated in paragraph 23 to paragraph 26 of these Directions and additionally ensure that:

(1) access by service providers to data at the bank, or its data centre shall be on 'need to know' basis, with appropriate controls to prevent security breaches or data misuse;

(2) in the event of multiple service provider relationships where two or more service providers collaborate to deliver an end-to-end solution, the bank remains responsible for understanding and monitoring the control environment of all service providers that have access to its data, systems, records, or resources;

(3) it immediately notifies RBI in the event of breach of security, and leakage of confidential customer-related information. In these eventualities, the bank shall adhere to the extant instructions issued by RBI from time to time on Incident Response and Recovery Management.

65. With regard to requirement that the data should not be combined or comingled, as stipulated in paragraph 26, it would suffice if there is clear separation and isolation of data (bank, and its customer specific data and information) to ensure that only the personnel as authorised by the bank is able to access data that belongs to them in a multi-tenant environment / architecture.

E. Outsourcing Process

E.1 Service Provider Evaluation

66. The directions regarding service provider evaluation as applicable to outsourcing of financial services contained in paragraph 29 to paragraph 31 shall apply, *mutatis mutandis,* to outsourcing of IT services, with the following additional considerations:

(i) technology, infrastructural stability, data backup arrangements, and disaster recovery plan;

(ii) conflict of interest, if any;

(iii) capability to identify, and segregate bank's data;

(iv) capability to comply with the regulatory and legal requirements of the outsourcing arrangement;

(v) information / cyber security risk assessment;

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

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

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

67. A bank should adopt a risk-based approach in conducting such due diligence activities.

E.2 Outsourcing Agreement

68. A bank shall ensure that its rights and obligations and those of each service provider are clearly defined and set out in a legally binding written agreement, in line with the provisions specified in paragraph 33 of these Directions. In principle, the provisions of the agreement shall appropriately reckon the criticality of the outsourced task to the business of the bank, the associated risks, and the strategies for mitigating or managing them.

69. In addition to the requirements specified in subparagraphs (i) to (vii) of paragraph 34, a bank shall also include at minimum (as applicable to the scope of Directions in this Chapter) the following aspects in any agreement for outsourcing of IT services:

(i) provisions covering service provider's subcontractors with respect to service and performance standards [subparagraph (i) of paragraph 34] and bank's right to conduct audits [subparagraph (vii) of paragraph 34];

(ii) access by the bank to all data, books, records, information logs, alerts, and business premises relevant to the outsourced service, available with the service provider;

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

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

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

(vi) storage of data only in India (as applicable) as per extant regulatory requirements;

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

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

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

(x) contingency plan(s) to ensure testing requirements;

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

(xii) right of RBI or person(s) authorised by it to perform inspection of the service provider and any of its sub-contractors and access the bank's IT infrastructure, applications, data, documents, and other necessary information given to, stored or processed by the service provider / or its sub-

contractors, in relation and as applicable to the scope of the outsourcing arrangement;

(xiii) clauses making the service provider contractually liable for the performance and risk management practices of its subcontractors;

(xiv) obligation of the service provider to comply with directions issued by the RBI in relation to the services outsourced to the service provider, through specific contractual terms and conditions specified by the bank;

(xv) termination rights of the bank, including the ability to orderly transfer the proposed outsourcing arrangement to another service provider, if necessary or desirable;

(xvi) obligation of the service provider to co-operate with the relevant authorities in case of insolvency or resolution of the bank;

(xvii) 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);

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

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

E.3 Monitoring and Control of Outsourced Services

70. A bank shall have in place a management structure to monitor and control its outsourced services. This shall include (as applicable to the scope of Directions in this Chapter), but not be limited to, monitoring the performance, uptime of the systems and resources, service availability, adherence to SLA requirements, and incident response mechanism.

71. A bank shall conduct regular audits (as applicable to the scope of Directions in this Chapter), of service providers (including subcontractors) with regard to the service

outsourced by it. Such audits may be conducted either by bank's internal or external auditors appointed to act on bank's behalf.

72. 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.

73. The audits shall assess, *inter alia,* the performance of the service provider, adequacy of the risk management practices adopted by the service provider, and compliance with laws and regulations. The frequency of the audit shall be determined based on the nature and extent of risk, and impact on the bank 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.

74. A bank, 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 the bank of its responsibility in ensuring assurance on the controls and procedures required to safeguard data security (including availability of systems) at the service provider's end.

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

76. A bank shall ensure that the service provider grants unrestricted and effective access to (a) data related to the outsourced services; (b) the relevant business

premises of the service provider; subject to appropriate security protocols, for the purpose of effective oversight by the bank, its auditors, RBI, and other relevant Competent Authorities, as authorised under law.

E.4 Inventory of Outsourced Services

77. A bank shall create an inventory of IT services outsourced to service providers (including key entities involved in their supply chains). Further, the bank shall map its dependency on third parties and periodically evaluate the information received from the service providers.

E.5 Business Continuity and Management of Disaster Recovery Plan

78. The Directions regarding 'Business Continuity and Management of Disaster Recovery Plan' as applicable to outsourcing of financial services contained in paragraph 4140 to paragraph 43 shall apply, *mutatis mutandis,* to outsourcing of IT services. The Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) for outsourced IT services shall be commensurate with the nature and scope of the outsourced service as per extant instructions issued by RBI from time to time on BCP / DR requirements.

E.6 Exit Strategy

79. The IT outsourcing policy shall contain a clear exit strategy for ensuring business continuity during and after exit.

80. The strategy shall include plans for different scenarios of exit or termination of services with stipulation of minimum period to execute such plans, as necessary.

81. In documenting its exit strategy, a bank shall, *inter alia*, identify alternative arrangements, which may include performing the service by a different service provider, or by the bank itself.

82. A bank shall ensure that outsourcing agreements have necessary clauses on safe removal or destruction of data, hardware and all records (digital and physical), as applicable. Further, the outsourcing 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 or the concerned bank.

83. A service provider shall be legally obliged to cooperate fully with both the bank and its new service provider(s) to ensure there is a smooth transition.

E.7 Termination

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

F. Specific Outsourcing Arrangements

F.1 Outsourcing within a Group / Conglomerate

85. A bank may outsource any IT service within its business group / conglomerate, provided that such an arrangement is backed by the Board-approved policy and appropriate SLAs / agreements with its group entities are in place.

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

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

F.2 Offshore or Cross-Border outsourcing

88. In principle, outsourcing arrangements shall only be entered into with parties operating in jurisdictions that uphold confidentiality clauses and agreements.

89. While engaging with service provider(s) in a foreign country, a bank shall:

    (i) 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, and establish sound procedures for mitigating the country

risk. This includes*, inter alia,* having appropriate contingency and exit strategies;

(ii) clearly specify the governing law of the outsourcing arrangement;

(iii) ensure that availability of records to the bank and the RBI will not be affected even in case of liquidation of the service provider;

(iv) ensure the right of the bank and RBI to direct and conduct audit or inspection of the service provider based in a foreign jurisdiction; and

(v) ensure that the arrangement complies with all statutory requirements as well as regulations issued by the RBI from time to time.

F.3 Outsourcing of Security Operations Centre (SOC)

90. Considering the risks associated with outsourcing of Security Operations Centre (SOC) operations by a bank, such as data being stored and processed at an external location and managed by the service provider (or its subcontractors) to which the bank has lesser visibility, the bank, to mitigate the risks, shall adopt the following requirements in the case of outsourcing of SOC operations in addition to the controls prescribed in this Chapter:

(i) unambiguously identify the owner of assets used in providing the services (e.g., systems, software, source code, processes, and concepts);

(ii) ensure that the bank has adequate oversight and ownership over the rule definition, customisation and related data / logs, meta-data and analytics (specific to the bank);

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

(iv) integrate the outsourced SOC reporting and escalation process with the bank's incident response process; and

(v) review the process of handling of the alerts or events.

F.4 Usage of Cloud Computing Services

91. Several cloud deployment and service models have emerged over time. These are generally based on the extent of technology stack that is proposed to be adopted by the consuming entity.

(1) *Example - 1: (*i) Some cloud services are:

(a) **Infrastructure as a Service (IaaS):** The service provides computing, 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.

(ii) Besides the three common application services, Cloud Service Providers (CSPs) also provide a range of services, viz., Database as a Service, Security as a Service, Storage as a Service, and others with varying risk levels.

(2) *Example - 2:* Some of the popular deployment models for delivery of cloud services are Private Cloud, Public Cloud, Hybrid Cloud, and Community Cloud.

92. Considering the varied services, benefits, and risk profiles associated with the cloud deployment and service models, a bank that uses cloud services for storage, computing and movement of data in cloud environments shall, in addition to other applicable provisions in these Directions:

(i) undertake a comprehensive assessment of its business strategy and goals adopted to the existing IT applications' footprint and associated costs. Such assessment shall include, but not be limited to, an analysis of various heads of cloud-related expenditure, such as application refactoring, integration, consulting, migration, and projected recurring expenditure depending on the nature of workloads. The extent of cloud adoption may vary, ranging from

migration of non-business critical workloads to the cloud, to deployment of critical business applications such as SaaS, or other combinations in between, and shall be determined based on a duly conducted business technology risk assessment;

(ii) ensure, *inter alia,* that the 'IT outsourcing policy', referred to in paragraph 57 of these Directions, addresses the entire lifecycle of data, i.e., covering the entire span of time from generation of the data, to its entry into the cloud, and till the data is permanently erased or deleted. It shall also ensure that specified procedures are consistent with business needs, and legal and regulatory requirements;

(iii) take into account cloud service specific factors, viz., multi-tenancy, and multi-location storing or processing of data, and attendant risks while establishing appropriate risk management framework;

(iv) implement necessary controls by referring to the cloud security best practices, as per applicability of the shared responsibility model between the bank and the Cloud Service Provider (CSP);

For cloud security best practices, a bank may refer to, *inter alia*, NIST SP 800-210 General Access Control Guidance for Cloud Systems https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-210.pdf

(v) put in place strong cloud governance by adopting and demonstrating a well-established and documented cloud adoption policy. Such a policy shall, *inter alia,*

(a) identify the services that can be moved to the cloud;

(b) enable and support protection of various stakeholder interests;

(c) ensure compliance with regulatory requirements, including those on privacy, security, data sovereignty, recoverability, and data storage requirements, aligned with data classification; and

(d) provide for appropriate due diligence to manage and continually monitor the risks associated with CSPs;

(vi) ensure that the selection of a CSP is based on a comprehensive risk assessment of the CSP. A bank shall enter into a contract only with CSPs that are subject to jurisdictions that uphold enforceability of agreements and the rights available thereunder to the bank, including those relating to aspects such as data storage, data protection, and confidentiality;

(vii) ensure that the service and technology architecture supporting cloud-based applications is built in adherence to globally recognised architecture principles and standards. The technology architecture shall:

(a) provide for a standard set of tools and processes to manage containers, images, and releases;

(b) provide for a secure container-based data management, where encryption keys and Hardware Security Modules are under the control of the bank;

(c) be protected against data integrity and confidentiality risks, and against co-mingling of data, in case of multi-tenancy environments; and

(d) be resilient and enable smooth recovery in case of failure of any one or combination of components across the cloud architecture with minimal impact on data / information security;

(viii) agree upon the Identity and Access Management (IAM) with the CSP and ensure that role-based access to the cloud hosted applications, both in respect of user-access and privileged-access, is provided. The bank shall:

(a) establish stringent access controls, as applicable for an on-premises application, for IAM for cloud-based applications;

(b) implement segregation of duties, role conflict matrix for all kinds of user-access, and privileged-access roles in the cloud-hosted application irrespective of the cloud service model;

(c) ensure that access provisioning is governed by principles of ‘need to know’, and ‘least privileges’; and

(d) implement multi-factor authentication for access to cloud applications;

(ix) ensure that the implementation of security controls in the cloud-based application achieves similar or higher degree of control objectives than those achieved in or by an on-premises 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 bank, and necessary procedures to authorise changes to cloud applications and related resources;

(x) define minimum monitoring requirements in the cloud environment and assess the information / cyber security capability of the CSP, to ensure that it:

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

(b) 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;

(c) has set the nature and frequency of testing of controls in respect of the outsourced services commensurate with the materiality of the services being outsourced by the bank and the threat environment; and

(d) has mechanisms in place to assess the subcontractors with regards to confidentiality, integrity, and availability of the data being shared with them, where applicable;

(xi) ensure appropriate integration of logs and events from the CSP into the bank's SOC, wherever applicable and retention of relevant logs in cloud for incident reporting and handling of incidents relating to services deployed on the cloud;

(xii) ensure that the cyber resilience controls of the CSP complement the bank's own application security measures, and that both the bank and the CSP maintain continuous and regular updates of security-related software, including upgrades, fixes, patches, and service packs, to safeguard applications against advanced threats and malware;

(xiii) ensure that the CSP has a well-governed and structured approach to manage threats and vulnerabilities supported by requisite industry-specific threat intelligence capabilities;

(xiv) ensure that the business continuity framework provides for continued operation of critical functions in the event of a disaster affecting the bank's cloud services or failure of the CSP, with minimal disruption to services, and without compromising data integrity and security;

(xv) ensure that the CSP has put in place demonstrative capabilities for preparedness and readiness for cyber resilience as regards cloud services in use by them through, *inter alia*, robust incident response and recovery practices including conduct of DR drills at various levels of cloud services including necessary stakeholders;

(xvi) develop an exit strategy that shall

(a) factor, *inter alia*, agreed processes and turnaround times for returning the bank's service collaterals and data held by the CSP; data completeness and portability; secure purge of bank's information from the CSP's environment; smooth transition of services; and unambiguous definition of liabilities, damages, penalties and indemnities, which should also be a part of the service level stipulations in SLA;

(b) include exit plans which align with the ongoing design of applications and service delivery technology stack;

(c) include contractually agreed exit / termination plans, which specify how the cloud-hosted service(s) and data will be moved out from the

cloud with minimal impact on continuity of the bank's business, while maintaining integrity and security; and

(d) include clauses for prompt take-over of all records of transactions, customer and operational information, and configuration data, in a systematic manner from the CSP, and purging at the CSP end, and ensuring independent assurance before signing off from the CSP.;

(xvii) ensure that the audit / periodic review / third-party certifications cover, as per applicability and cloud usage, *inter alia*, aspects such as roles and responsibilities of both bank 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.

G. Redressal of Grievances related to Outsourced Services

93. A bank 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 bank.

94. Outsourcing arrangements entered into by a bank shall not affect the rights of its customers against the bank, including the ability of the customers to obtain redressal as applicable under relevant laws.

Chapter V – Repeal and Other Provisions

A. Repeal and saving

95. With the issue of these Directions, the existing Directions, instructions, and guidelines relating to outsourcing of financial services and IT services as applicable to Commercial Banks stand repealed, as communicated vide circular DOR.RRC.REC.302/33-01-010/2025-26 dated November 28, 2025. The Directions, instructions, and guidelines repealed prior to the issuance of these Directions shall continue to remain repealed.

96. Notwithstanding such repeal, any action taken or purported to have been taken, or initiated under the repealed Directions, instructions, or guidelines shall continue to be governed by the provisions thereof. All approvals or acknowledgments granted under these repealed lists shall be deemed as governed by these Directions. Further, the repeal of these Directions, instructions, or guidelines shall not in any way prejudicially affect:

(1) any right, obligation or liability acquired, accrued, or incurred thereunder;

(2) any, penalty, forfeiture, or punishment incurred in respect of any contravention committed thereunder;

(3) any investigation, legal proceeding, or remedy in respect of any such right, privilege, obligation, liability, penalty, forfeiture, or punishment as aforesaid; and any such investigation, legal proceedings or remedy may be instituted, continued, or enforced and any such penalty, forfeiture or punishment may be imposed as if those Directions, instructions, or guidelines had not been repealed.

B. Application of other laws not barred

97. The provisions of these Directions shall be in addition to, and not in derogation of the provisions of any other laws, rules, regulations, or Directions, for the time being in force.

C. Interpretations

98. For the purpose of giving effect to the provisions of these Directions or in order to remove any difficulties in the application or interpretation of the provisions of these Directions, the RBI may, if it considers necessary, issue necessary clarifications in respect of any matter covered herein and the interpretation of any provision of these Directions given by the RBI shall be final and binding.

(Sunil T S Nair)

Chief General Manager