Draft Reserve Bank of India (All India Financial Institutions – Managing Risks in Outsourcing) Directions, 2025

DRAFT FOR COMMENTS

RBI/2025-26/--
DoR.ORG.REC.No./ 00-00-000/2025-26 XX, 2025

Reserve Bank of India (All India Financial Institutions – Managing Risks in Outsourcing) Directions, 2025

Table of Contents

In exercise of the powers conferred by Section 45L of the Reserve Bank of India Act, 1934, 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 to do so, 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 (All India Financial Institutions - Managing Risks in Outsourcing) Directions, 2025.

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

   Provided that, an AIFI's existing IT outsourcing agreement 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 AIFI'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 above proviso shall be construed as permitting non-compliance with any other extant regulatory instructions or statutory requirements applicable to such arrangements.

B. Applicability

3. These Directions shall be applicable to All-India Financial Institutions (AIFIs) namely Export Import Bank of India ('EXIM Bank'), National Bank for Agriculture and Rural Development ('NABARD'), National Bank for Financing Infrastructure and Development ('NaBFID'), National Housing Bank ('NHB') and Small Industries Development Bank of India ('SIDBI'), hereinafter collectively referred to as 'AIFIs' and individually as an 'AIFI'.

C. Definitions

4. In these Directions, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

(1) '**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.

(2) '**IT services**' means IT services and / or IT enabled services and / or IT activities.

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

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

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

(4) '**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 an AIFI to perform activities on a continuing basis that would normally be undertaken by the AIFI itself, now or in the future. 'Continuing basis' shall include agreements for a limited period.

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

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

(i) vendors providing business services using IT. For e.g., Business Correspondents (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, services, products;

(iv) FinTech firms providing services for data retrieval, 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, etc.;

(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 Vulnerability Assessment / Penetration Testing (VA / PT) related to IT infra, IT services or information security services in their role as independent third-party auditor or consultant or lead implementer.

Explanation: Depending upon the IT Outsourcing services provided (if any) by a Regulated Entity (RE) to other RE(s), even an RE could be considered as a service provider to other RE, under the provisions of these Directions.

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

5. 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.

D. Scope

6. These Directions shall apply to an AIFI's material outsourcing of IT services, as defined in paragraph 4(3) above. In this context, 'Outsourcing of IT Services' shall include outsourcing of the following activities:

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

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

   (iii) application development, maintenance and testing; 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.

7. These Directions shall not apply to the following services / activities,

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

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

   (iii) SMS gateways (Bulk SMS service providers);

   (iv) procurement of IT hardware or appliances;

   (v) acquisition of IT software, product or application (e.g., CBS, database, security solutions, etc.) 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 an AIFI;

(vi) any maintenance service (including security patches, 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 AIFI;

(vii) applications provided by financial sector regulators or institutions such as CCIL, NSE, BSE, etc.;

(viii) platforms provided by entities such as Reuters, Bloomberg, SWIFT, etc.;

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

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

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

Chapter II – Role of the Board

8. The outsourcing of any activity by an AIFI 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

9. An AIFI intending to outsource its IT activities shall put in place a comprehensive Board-approved IT outsourcing policy, the coverage of which is indicated in paragraph 15.

B. Key responsibilities

10. 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 under the proviso to paragraph 12(vi) 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 Information Technology (IT) Services

A. Authorisation, Accountability, and Oversight

11. As stated in paragraph 9, the outsourcing of any activity by an AIFI shall not diminish its obligations, and those of its Board and Senior Management, who have the ultimate responsibility for the outsourced activity.

12. An AIFI shall ensure that:

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

(ii) it shall not engage an IT service provider that would result in its reputation being compromised or weakened;

(iii) notwithstanding whether the service provider is located in India or abroad, the outsourcing shall neither impede nor interfere with the ability of the AIFI to effectively oversee and manage its activities;

(iv) outsourcing does not impede the RBI in carrying out its supervisory functions and objectives;

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

(vi) the service provider, if not a group company, is not owned or controlled by any director, or key managerial personnel, or approver of the outsourcing arrangement of the AIFI, 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.

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

13. An AIFI 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 AIFI shall, *inter alia*, consider the following:

    (i) the need for outsourcing based on criticality of activity to be outsourced;

    (ii) expectations and outcomes from outsourcing;

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

    (iv) the model for outsourcing.

14. An AIFI shall ensure that cyber incidents are reported to it by the service provider without undue delay, so that an incident is reported by the AIFI to the RBI within six hours of detection by the third-party service provider.

B. Governance Framework

B.1 Outsourcing Policy

15. An AIFI intending to outsource any of its IT activities shall put in place a comprehensive Board approved IT outsourcing policy incorporating, *inter alia*,

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

    (ii) criteria for selection of such activities as well as service providers;

    (iii) parameters for defining material outsourcing based on the broad criteria defined in paragraph 4(3) 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 activities; and

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

B.2 Role of Senior Management

16. The Senior Management of an AIFI 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 organisation 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 / 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 third-party service provider, are in place and tested periodically;

(v) ensuring (a) effective oversight over third party 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 / a Committee of the Board; and

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

B.3 Role of IT Function

17. The responsibilities of the IT Function of an AIFI shall, *inter alia*, include:

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

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

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

(iv) 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.

C. Risk Management

C.1 Risk Management Framework

18. An AIFI 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.

19. An AIFI 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.

20. An AIFI 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.

C.2 Confidentiality and Security of Information

21. An AIFI shall be responsible for the confidentiality and integrity of data and information pertaining to its customers that is available to the service provider.

22. Access by service providers to data at the AIFI or its data centre shall be on ‘need to know’ basis, with appropriate controls to prevent security breaches and / or data misuse.

23. An AIFI shall seek to ensure the security, preservation and protection of the customer information in the custody or possession of the service provider. Access to customer information by a service provider or its staff shall be on a ‘need to know’ basis.

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

25. In instances, where a 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.

    Explanation: As regards combining of data, it would suffice if there is clear separation and isolation of data (AIFI and its customer specific data and information) to ensure that only the personnel as authorised by the AIFI is able to access data that belongs to them in a multi-tenant environment / architecture.

26. An AIFI 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.

27. An AIFI shall immediately notify RBI in the event of breach of security and leakage of confidential customer related information. In these eventualities, the AIFI shall adhere to the extant instructions issued by RBI from time to time on Incident Response and Recovery Management.

D. Outsourcing Process

D.1 Service Provider Evaluation

28. An AIFI 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.

29. 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) while evaluating the capability of the service provider, risks arising from concentration of outsourcing arrangements with a single or a few service provider/s;

    (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) conflict of interest, if any;

    (vii) 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;

    (viii) technology, infrastructural stability, security and internal control, audit coverage, reporting and monitoring procedures, data backup arrangements, business continuity management and disaster recovery plan;

    (ix) capability to identify and segregate the AIFI's data;

    (x) quality of due diligence exercised by service provider of its employees and subcontractors;

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

(xii) information / cyber security risk assessment;

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

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

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

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

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

D.2 Outsourcing Agreement

32. An AIFI 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 principle, the provisions of the agreement shall appropriately reckon the criticality of the outsourced task to the business of the AIFI, the associated risks and the strategies for mitigating or managing them.

33. The terms and conditions governing the outsourcing arrangement shall be carefully defined and vetted by the AIFI's legal counsel on their legal effect and enforceability. The AIFI shall ensure that such an agreement is sufficiently flexible to allow the AIFI to retain an adequate control over the outsourced activity 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

(xiii) right to conduct audits on the service provider (including its subcontractors) by the AIFI, 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 AIFI;

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

(xv) recognising the authority of regulators to perform inspection of the service provider and any of its sub-contractors.

(xvi) clauses to allow RBI or person(s) authorised by it to access the AIFI's IT infrastructure, applications, data, documents, and other necessary information given to, stored or processed by the service provider and / or its sub-contractors in relation and as applicable to the scope of the outsourcing arrangement;

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

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

(xix) clauses requiring prior approval or consent, as applicable, of the AIFI for the use of subcontractors by the service provider for all or part of an outsourced activity;

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

(xxi) obligation of the service provider to co-operate with the relevant authorities in case of insolvency / resolution of the AIFI;

(xxii) 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);

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

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

D.3 Monitoring and Control of Outsourced Activities

35. An AIFI shall have in place a management structure to monitor and control its outsourced activities. This shall include (as applicable to the scope of outsourcing of IT services), but not be limited to, monitoring the performance, uptime of the systems and resources, service availability, adherence to SLA requirements, incident response mechanism, etc.

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

37. 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.

38. The audits shall assess the performance of the service provider, adequacy of the risk management practices adopted by the service provider, compliance with laws and regulations, etc. The frequency of the audit shall be determined based on the nature and extent of risk and impact on the AIFI 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.

39. An AIFI, 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 AIFI 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.

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

41. An AIFI 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 by the AIFI, its auditors, regulators and other relevant Competent Authorities, as authorised under law.

D.4 Inventory of Outsourced Services

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

D.5 Business Continuity and Management of Disaster Recovery Plan

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

44. In establishing a viable contingency plan, an AIFI 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.

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

46. An AIFI shall ensure that its service providers are able to isolate the AIFI'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 given to the service provider, and assets of the AIFI, can be removed from the possession of the service provider, or deleted, destroyed or rendered unusable.

D.6 Exit Strategy

47. The IT outsourcing policy shall contain a clear exit strategy with regard to outsourced IT activities / IT enabled services, for ensuring business continuity during and after exit.

48. 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.

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

50. A service provider shall be legally obliged to co-operate fully with both the AIFI and its new service provider(s) to ensure there is a smooth transition.

51. An AIFI shall ensure that outsourcing agreements have necessary clauses on safe removal / destruction of data, hardware and all records (digital and physical), as applicable.

52. 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 AIFI.

D.7 Termination

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

E. Specific Outsourcing Arrangements

E.1 Outsourcing within a Group / Conglomerate

54. An AIFI 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.

55. 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.

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

E.2 Offshore or Cross-Border outsourcing

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

58. While engaging with service provider(s) in a foreign country, an AIFI 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 AIFI and the RBI will not be affected even in case of liquidation of the service provider;

    (iv) ensure the right of the AIFI 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.

E.3 Outsourcing of Security Operations Centre (SOC)

59. Considering the risks associated with outsourcing of Security Operations Centre (SOC) operations by an AIFI, such as data being stored and processed at an external location and managed by a third party to which the AIFI has lesser visibility, the AIFI, to mitigate the risks, shall adopt the following requirements in the case of outsourcing of SOC operations in addition to the controls prescribed in these Directions:

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

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

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

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

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

E.4 Usage of Cloud Computing Services

60. 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:* Some cloud services are:

(i) **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.

(ii) **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.

(iii) **Software as a Service (SaaS):** Client uses the application(s) provided by the service provider on a cloud infrastructure.

(iv) 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, Community Cloud.

61. Considering the varied services, benefits, and risk profiles associated with the cloud deployment and service models, an AIFI 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 Software-as-a-Service (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 15 of these Directions, addresses the entire lifecycle of data, i.e., covering the entire span of time from generation of the data, its entry into the cloud, till the data is permanently erased / deleted. 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, multi-location storing / processing of data, etc., 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 AIFI and the Cloud Service Provider (CSP);

For cloud security best practices, an AIFI 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 activities 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. An AIFI 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 AIFI, 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 AIFI;

(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 AIFI shall:

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

(b) implement segregation of duties and 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 AIFI; 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 AIFI 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 AIFI's SOC, wherever applicable and / or 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 AIFI's own application security measures, and that both the AIFI 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 AIFI'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 Disaster Recovery (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 AIFI's service collaterals and data held by the CSP; data completeness and portability; secure purge of AIFI'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 AIFI's business, while maintaining integrity and security; and

(d) include clauses for prompt take-over of all records of transactions, customer and operational information, 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 AIFI 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.

F. Redressal of Grievances related to Outsourced Services

62. An AIFI 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 AIFI.

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

Chapter IV – Repeal and Other Provisions

A. Repeal and saving

64. With the issue of these Directions, the existing Directions, instructions, and guidelines relating to outsourcing of IT services as appliable to All India Financial Institutions stand repealed, as communicated vide notification dated XX, 2025. The Directions, instructions, and guidelines repealed prior to the issuance of these Directions shall continue to remain repealed.

65. 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.

B. Application of other laws not barred

66. 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

67. 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.