BERAR FINANCE LIMITED

POLICY FOR OUTSOURCING OF INFORMATION TECHNOLOGY SERVICES

(IT OUTSOURCING POLICY)

Record of Review

Document Number	01
Version Number	03
Document Classification	External
Originally Formulated	March 30, 2023
Created by	IT Department
Reviewed by	IT Strategy Committee
Approved by	Board of Directors of the Company

Version No.	Created/Modified Date
01	March 30, 2023
02	May 30, 2023
03	March 27, 2024

Contents

1 Introduction

The IT Outsourcing Policy is intended to provide clear management guidance and ensure regulatory compliance on outsourcing of technology services and operations. The policy provides direction in ensuring secure, efficient, and resilient IT outsourcing arrangements. This signifies Berar Finance Limited's continued compliance to achieving the best practices in IT Outsourcing by establishing, enforcing, and continually refining the IT Outsourcing policy.

1.1 Background

Berar Finance Limited ("Berar Finance)" or "Company") is a Public Limited Company incorporated under the Indian Companies Act, 1956 and is registered with the Reserve Bank of India ("RBI") as a deposit taking non-banking finance company ("NBFC").

The Berar Finance shall ensure that outsourcing arrangements neither diminish its ability to fulfil its obligations to customers nor impede effective supe revision by the supervising authority. Berar Finance desirous of outsourcing of IT and IT enabled services shall not require prior approval from RBI for outsourcing such activities. However, such arrangements shall be subject to on-site/ off-site monitoring and inspection/ scrutiny by the supervising authority.

1.2 IT Outsourcing

IT outsourcing entails delegating specific information technology tasks or functions to third-party service providers. This strategy adopted by Berar Finance seeking operational efficiency offers benefits such as cost savings, access to specialized expertise, and the ability to focus on core competencies. It also introduces potential challenges, including data security concerns, quality assurance, and dependency on external entities. IT outsourcing policy provides necessary guidance for Berar Finance to adopt outsourcing of key technology services while being able to balance risks.

1.3 Objective

The IT Outsourcing Policy provides management directive to govern & manage technology outsourcing arrangements for Berar Finance Limited through appropriate control measures across the entire life cycle of outsourcing engagements. Berar Finance shall evaluate the risks and increase benefits of technology outsourcing by: -

Defining governance framework for evaluation and onboarding of technology outsourcing partner

- Establish a risk management framework to identify and manage risks associated with technology outsourcing.
- Enabling the team to develop & deploy the right set of controls for better management of outsourcing services.

1.4 Reference for the IT Outsourcing Policy

The IT Outsourcing Policy and the respective definitions have been referred to and mentioned thereafter from RBI's Master Direction on Outsourcing of Information Technology Services (RBI/2023-24/102 DoS.CO.CSITEG/SEC.1/31.01.015/2023-24) dated 10th April,2023.

1.5 Definitions

Outsourcing: 'Outsourcing' can be defined as the Company's use of a service provider through a formal agreement (either an affiliated entity within a group or an entity that is external to the Company) to perform activities on a continuous basis that would normally be undertaken by the Company itself now or in future.

IT Services outsourcing: Common technology services such as Technology Infrastructure Management, Application Maintenance and Support, Application Development, Maintenance and Testing etc. Areas related to Information Security Operations, Support in various IT areas like Services, Applications, Software, Hardware, Network etc. and Database management and various types of support services etc.

Sub-Contracting: Subcontracting refers to an arrangement whereby the outsourced agency engaged by the Company further outsources a part of its activity to another service provider (Subcontractor).

Service Provider: An entity or organization responsible for delivering specific services to the Company. The onus lies with the Service Provider to ensure consistent and quality service delivery.

1.6 Applicability

The IT Outsourcing policy provides the scenarios below as guidelines for the identification of services under IT outsourcing aligned to RBI Guidelines.

- IT infrastructure management, maintenance and support (hardware, software or firmware).
    - For example, vendors involved in end-to-end IT infrastructure management services.
- Network and security solutions, maintenance (hardware, software, or firmware).
    - Service providers providing end-to-end maintenance & administration network & security management services on ongoing basis.
- Application Development, Maintenance and Testing; Application Service Providers (ASPs)
- Services and operations related to Data Centres.
- Cloud Computing Services.
    - For example, cloud service providers as Infrastructure as a Service (IaaS) or dedicated Software as a Service (SaaS), Platform as a Service (PaaS)
- Managed Security Services; and
- Management of IT infrastructure and technology services associated with the payment system ecosystem.
    - For example, vendors involved in providing maintenance services on an ongoing basis for Payments switches and infrastructure.

Exclusions from IT outsourcing policy have been covered as part of Annexure 3.

1.7 Policy Review

The IT Outsourcing Policy shall be recommended by the IT Strategy Committee of the Board and the same will be approved by the Board of Directors of Berar Finance Limited subsequently.
The Board (IT Strategy Committee) of the Berar Finance shall review and approve the IT Outsourcing Policy on an annual basis.

1.8 Materiality & Non-Materiality of IT Outsourcing

IT outsourcing policy covers all above outsourcing engagements with third parties to provide services to Berar Finance Limited. These services could be classified into Material Outsourcing activities and other outsourcing activities.

IT Outsourcing Policy provides elevated levels of control requirements for material outsourcing arrangements.

Materiality of outsourcing arrangement would be based on:

- Services which disrupted or compromised would lead to substantial impact on the Berar Finance business functions, such as Loan Management System, Network Management Services.
- Likely material impact to Berar Finance & its customers due to any unauthorized access, loss, or theft of customer data within these services
- Likely impact on the Berar Finance reputation, and ability to achieve its technology objectives and plans; for example, critical digital application development by third parties.

Non materiality of outsourcing arrangement can be defined as any of the services which do not fall under the ambit of the respective points defining materiality above, for e.g. resource based outsourced personnel, application development etc.

2 Technology Outsourcing Governance Framework

The role of Berar Finance Limited encompasses setting clear strategic directives, ensuring that IT outsourcing decisions are adequately aligned with the Berar Finance's broader objectives, formulating policy guidelines, and supervision over vendor adherence to control standards, all while ensuring transparency, accountability, and resilience in every facet of the outsourced IT ecosystem.

2.1 Assessing the need for outsourcing

The technology team of Berar Finance Limited shall undertake a detailed assessment of any need to outsource technology services. Respective technology units initiating outsourcing requirements shall be responsible for performing complete assessment.

The technology team at Berar Finance Limited will be responsible for reviewing and confirming coverage of all aspects of assessment.

Critical aspects to be covered as part of assessment for need of any technology outsourcing:

- The need for outsourcing based on criticality of activity to be outsourced.
- Define expectations and outcomes from outsourcing, clearly spelling out benefits from outsourcing.
- Define success criteria to assess achievements of objectives of outsourcing.
- Conduct cost-benefits analysis.
- Defining model for outsourcing such as onsite or offsite, cloud vs on-premises etc
- Identification of risks associated with outsourcing services and available measures to be adopted to manage risks.

Assessment details should be part of the approval note as part of the approval process as per delegation matrix.

2.2 Compliance with all applicable statutory and regulatory requirements

As part of the assessment process, the Technology team shall ensure that all relevant laws, regulations, rules, guidelines, and conditions of approval have been considered.

Outsourcing engagement shall adhere to requirements laid down as part of Digital Personal Data Protection Act,2023 for protection of personal data shared with outsourcing partners as part of engagement. NBFC shall appropriately define Data Governance policy of Berar Finance Limited to govern data privacy requirements as part of the outsourcing engagement.

2.3 Grievance Redressal Mechanism

Berar Finance Limited should ensure a robust grievance redressal system that remains unaffected by any outsourcing initiatives. The existing customer grievance redressal process of Berar Finance shall be followed for any customer complaints or rights of customer.

2.4 Inventory Management of Outsourcing Arrangements

Berar Finance Limited should maintain a comprehensive inventory of services offered by their service providers. This should include significant entities involved in their supply chains.

The technology team shall be responsible to maintain inventory of outsourcing services covering below details:

- Sub-contractors involved in outsourcing engagement.
- Dependencies on the outsourcing partner
- Materiality of Service outsourcing

- Last evaluation/audit performed for respective outsourcing arrangements.

2.5 Role of the Board (IT Strategy Committee)

The IT Strategy Committee of the Board (ITSC) functions as the primary technology governance entity within Berar Finance Limited, aiding the Board of Directors in the formulation and execution of effective IT strategies. This committee shall be entrusted with the oversight responsibility on governance of IT outsourcing contracts.

The IT Policy document of Berar Finance Limited shall continue to be the reference document for Terms of reference for the IT Strategy committee. In addition to responsibilities covered in IT policy, IT Strategy committee shall be responsible for:

- Approving IT Outsourcing Policy
- Provide guidance on governance framework for approval of IT Outsourcing activities.
- Provide guidelines suitable for the administrative framework of Senior Management for the purpose of regulatory guidelines.
- Review risks and mitigation measures deployed for material outsourcing arrangements.

2.6 Role of the Senior Management (IT Steering Committee)

The IT Steering Committee, composed of Senior Management representatives from business units, will serve an instrumental role in supporting the IT Strategy Committee of the Board as well as Board in executing the IT Outsourcing Policy and ensuring compliance to regulatory guidelines.

The IT Policy document of the Berar Finance Limited shall continue to be the reference document for Terms of reference for the IT Steering committee. In addition to responsibilities covered in IT policy, IT Steering committee shall be responsible for:

- Formulate and Approve IT Outsourcing Policy and set up procedures to manage technology outsourcing arrangements.
- Setup risk management framework and evaluate risks associated with outsourcing engagements along with mitigation measures.
- Ensure proper evaluation of prospective IT outsourcing arrangements as well as existing contracts at regular intervals.
- Ensure setting up of appropriate business continuity plans including exit strategy for outsourcing engagements.
- Maintain oversight on data confidentiality associated with outsourcing partners as well as appropriate redressal of customer grievances in a timely manner.
- Ensure independent review and audit of outsourcing arrangements on a periodic basis.
- Apprise board on IT outsourcing risks and mitigation measures, and oversight on outsourcing engagements related to audit, performance, security, continuity of operations.

The Technology team shall be responsible to provide necessary information to IT Steering committee to fulfil its responsibilities.

2.7 Role of the IT Function

IT Function under leadership of Chief Technology Officer and technology unit heads shall be responsible for driving outsourcing arrangements for technology activities and ensuring compliance.

The CTO should establish an organizational structure to support the governance framework for outsourcing of the Berar Finance's IT operations. The responsibilities of this role would include, but are not limited to:

- Collaborate with concerned business team in identifying, measuring, monitoring, mitigating, and managing the organization's IT outsourcing risk levels.
- Maintain a centralized database of all IT outsourcing arrangements for review by Board, Senior Management, Auditors, and Supervisors; (as per RBI Master Directions on Outsourcing of Information Technology Services dated 10th April 2023).
- Monitor and supervise outsourced activities vigilantly to ensure that service providers adhere to the established performance standards and provide seamless services.
- Report to Senior Management, coordinate periodic due diligence, and raise any concerns.
- Establish the necessary documentation for contractual agreements.
- Defining and Implementing the IT outsourcing policy
- Establishing an efficient disaster recovery system and a comprehensive business continuity plan associated with outsourcing arrangements including exit strategy.
- Adhering to existing instructions on the outsourcing of IT activities
- Understanding and appropriately assessing the requirements for trained resources with the necessary skill sets for managing outsourcing engagements.

2.8 Role of the CTO/CIO

The CTO/CIO shall oversee a crucial role in managing and ensuring IT outsourcing compliance within Berar Finance. Their responsibilities are centred around ensuring Berar Finance's IT operations align with its strategic objectives, while managing and mitigating associated risks.

- Technology Team shall develop & maintain the Berar Finance's IT Outsourcing Policy, aligning all IT components with Berar Finance Limited's strategic objectives.
- Technology Team, along with respective technology units, shall ensure the identification of potential operational risks associated with IT outsourcing and conduct comprehensive risk assessments as per outsourcing risk assessment checklist.
- The Technology Team shall ensure all IT outsourcing arrangements comply strictly with statutory regulations and legal mandates, following the guidelines set by regulatory bodies.
- The Technology team should actively oversee all outsourcing contracts and ensure adherence to IT outsourcing policy.
- The team shall work with respective business units to ensure appropriate due diligence & evaluation carried out by technology team.
- The Technology team should get a business continuity plan and exit strategy for material outsourcing contacts.

2.9 Role of Business Function

- The respective business function heads should align and work with the team to implement the activities mentioned in the IT Outsourcing Policy.
- Approval of IT Outsourcing needs for business specific scenarios shall be determined by the respective Business Unit Head and Managing Director.

2.10 Role of CISO

The Chief Information Security Officer (CISO) and information security plays an important role in providing risk oversight on IT outsourcing within Berar Finance Limited. Their responsibilities are centred around ensuring Berar Finance Limited's IT operations align with identification of operational risks and more importantly, security risks associated with outsourcing arrangements. Key responsibilities shall include:

- The CISO shall review and provide all necessary guidance on IT Outsourcing policy as well as compliance of outsourcing policy across all such arrangements.
- The CISO should review the identification of potential operational and security risks linked to IT outsourcing and conduct a review of any threats and vulnerabilities.
- The CISO should review risk evaluations of vendor-managed processes at time of onboarding as part of the due-diligence process as well as during monitoring of outsourcing arrangements.
- Berar Finance's third party security management policy shall be followed during outsourcing arrangements to ensure compliance with security controls.
- In case of a security breach or leakage of confidential customer data, the respective technology unit should promptly report the incident to the CISO who then will review & subsequently report to senior management.
- The CISO, with the support of the Technology Team, will review and refine the IT Outsourcing Policy, ensuring its relevant and effectiveness in the face of evolving technology landscapes and regulatory environments.

2.11 Data Privacy & Governance

A data privacy and governance structure with reference from Berar Finance Limited's forthcoming Data Governance Policy shall be followed with clear roles and responsibilities for the respective Data Protection Officer of the Berar Finance Limited will be established for managing data usage and protection requirements pertaining to outsourcing arrangements.

2.12 Data Access

Users will be given access to data on a need-to-know basis, especially confidential or proprietary information. Personal identifiable information (PII) will be accessible only as per business need and will need prior approval from CISO/CTO. Periodic reviews should be conducted for access management.

2.13 Data Classification and Risk Assessments

Data and information assets will be classified as per Berar Finance Limited's ISMS data classification guidelines. Risk assessments considering threats to the availability, integrity, and confidentiality of the data shall be conducted.

2.14 Data Security

Data identified as sensitive or critical will be protected as per Berar Finance Limited's information asset management guidelines and cryptography policy. Access to sensitive data will be monitored. Data Governance Policy will be in place to ensure protection of customer's personal data and information.

Security measures will be implemented as per each data set classification as mentioned in data classification policy.

2.15 Data Sharing

Data sharing, data transfer and third-party access will be done via a secured channel. It will be ensured that the data is shared only with authorized parties in compliance with regulatory requirements, contractual requirements, or business requirements.

2.16 Data stored and processed at third party locations.

Business units will ensure that the Berar Finance Limited's applicable data governance requirements of data classification, protection and data quality are implemented by its business partners.

2.17 Data Regulations

Regulatory and legal requirements for data usage and protection should be considered and implemented by Berar Finance Limited

3 IT Outsourcing Management

IT Outsourcing management involves managing the entire life cycle of outsourcing contracts from identification of IT services for outsourcing to onboarding till exit of service providers. IT Outsourcing Management in Berar Finance is a structured process, designed to ensure the seamless integration of third-party services with Berar Finance ’s internal operations while maintaining the standards of security, efficiency, and regulatory compliance.

3.1 Pre-engagement of outsourcing arrangements

The Technology Team shall ensure to review & compliance for pre-engagement process before entering any IT outsourcing arrangement. This process is aimed at ensuring that the outsourcing arrangement aligns with Berar Finance's strategic objectives, operational needs, and risk management framework, and that it complies with the standards of quality, security, and regulatory compliance.

3.2 Evaluation of Service Provider

The evaluation of prospective IT outsourcing partners is a critical part of the pre-engagement process. The technology team shall ensure to assess each potential partner's capabilities, financial stability, reputation, technological competence, and adherence to industry best practices and regulatory requirements.

Critical aspects shall be covered during the evaluation process.

- Respective technology units shall follow through the existing Sanction note process of technology procurement for outsourcing engagements.
- An evaluation checklist should be followed with all necessary details by the technology team shall ensure coverage of all critical aspects including evaluation of material outsourcing.
- Factors considered for evaluation should include, but not limited to:
    - Technical Features and capabilities
    - Team capabilities & skill sets
    - Commercial terms
    - Proposed outsourcing model.

3.3 Due Diligence of Service Provider

The technology team shall conduct detailed due diligence of shortlisted service providers at times of consideration of outsourcing of technology services. The Technology& CISO team shall conduct due diligence of the service provider.

The due diligence process should follow a predefined checklist and provide all necessary details with relevant documentation. The due diligence process should follow a risk-based approach considering all risky elements having an impact on the technology management of Berar Finance Limited The process should evaluate the relevant risks mentioned in the due diligence checklist during the due diligence process. The due diligence checklist is as prescribed in Para 14 of RBI Master Directions on Outsourcing Information Technology Services dated 10th April,2023. The aspects for due diligence to be considered for the evaluation process are covered as part of Annexure 5.

3.4 Due Diligence of Service Provider at renewal

The technology team shall conduct due diligence of existing service providers at time of renewal of contract. The process should start at least one month prior to the contract renewal date. The Technology & CISO team shall conduct due diligence.

Any deviation reported during the renewal stage from the past due diligence report, shall be highlighted and communicated to senior management.

3.5 Approval matrix for evaluation and engagement for Outsourcing of IT Services

Table "Approval Matrix for evaluation and engagement for Outsourcing of IT Services" refers to the approval framework for identifying and finalizing the approval of services to be considered as "Outsourced. Refer Annexure 4.

3.6 Onboarding of service provider

Each technology unit shall ensure that all necessary aspects related to service providers are taken care at time of onboarding, including closure of agreement, security compliance as per third party security checklist.

3.7 Legal Binding Agreement with Service Provider

Every IT outsourcing engagement must have an Agreement that encompasses the exact expectations, roles, responsibilities, and deliverables. Each technology unit shall initiate the process of agreement signing with the service provider as per legally approved agreement.

The Standard Legal Outsourcing contract agreement shall include all key aspects as per regulatory guidelines and shall be approved by the legal team of Berar Finance Limited. Legal binding agreement for outsourcing arrangement shall factor in all critical elements to ensure optimum, secure service delivery throughout tenure of engagement.

The aspects required to be in the agreement with the service provider as prescribed in paragraph 16 of RBI in Master direction on Outsourcing of Information Technology Services dated April 10, 2023, shall be covered in the agreement with the service provider and has also been covered as part of Annexure 6.

The agreement review & signing process should be as per NBFC's delegation matrix and signing authority.

3.8 Variability based on Materiality and Structure

All IT outsourcing engagements differ in nature due to material and structural arrangement for delivery. Certain clauses of standard outsourcing contracts may not be applicable to certain sets of outsourcing arrangements. Any such deviations to outsourcing contracts shall be referred to the Legal department for any interpretation and ratification and further should be briefed to senior management.

3.9 Subcontracting of outsourcing engagement

Some outsourcing arrangements may involve subcontracting by a selected service provider. The service provider shall ensure that all necessary arrangements related to the contract have been duly taken care of by the service provider.

The outsourcing agreement with the service provider shall suitably cover details about subcontracting arrangements as well as ownership of complete responsibility with service provider for sub-contracting partners.

Sub-contractor in the RBI's Master Directions refers only to those providing material/significant IT services to the Third-Party Service Providers specific to the material IT services arrangement that Berar Finance Limited has entered with the Third-Party Service Provider.

Berar Finance Limited shall carry out audits applicable to the extent of IT services outsourced and based on materiality. These audits, pertaining to the activities outsourced, may include service providers and subcontractors. The audits could be executed either by Berar Finance Limited's in-house audit team or by external auditors acting on behalf of Berar Finance Limited.

3.10 Monitoring and Control of Outsourced Services

Managing complete oversight of each outsourcing arrangement for the entire contract period is crucial to ensure the right delivery of technology operations by service provider. The technology team shall assign dedicated ownership for each outsourcing arrangement and designated person shall be responsible for monitoring and control of outsourced activities.

3.11 Performance of Outsourcing Engagements

Respective technology units shall ensure that all necessary control measures defined at time of engagement are duly adhered to during the tenure of contract and carry out detailed performance monitoring review with service provider.

Service providers should submit detailed performance monitoring review reports. The frequency of performance monitoring should be quarterly or monthly depending upon material and nature of engagement and should be mentioned in the inventory of outsourcing contracts.

Performance review should include, but not limited to:

- Detailed SLA compliance with necessary data elements
- Resource utilization/ System Uptime Report etc.
- Incidents Reported during the review period.
- Open Audit Points and closure status

The Technology team shall present and submit a summary of performance monitoring review of all material outsourcing arrangements to the IT Steering Committee as well as to the IT Strategy Committee. Monitoring oversight shall enable Berar Finance to maintain accountability, manage expectations, and demonstrate the commitment to the highest standards of governance.

3.12 Audit of Outsourcing Arrangements

Berar Finance Limited's internal audit team shall conduct audits/pooled audits of outsourcing engagements at regular intervals in accordance with services outsourced and model of outsourcing. The frequency of audit shall be covered in central inventory of outsourced arrangements, based on materiality & nature of services. (Refer to Annexure I)

The technology team may engage third party auditors to carry out audits of outsourcing engagements in accordance with IT outsourcing policy. Audit program shall cover below aspects as part of audit of outsourcing engagement, but not limited to:

- Controls suggested as per contract.
- Performance adherence in line with SLA
- Security controls deployed to ensure customer data protection.
- Business continuity arrangements
- Closure of previous audit points
- Closure of risks as per risk register as well as Vendor inspection report.
- Financial and operational condition
- Risk management.
- Compliance

The audit reports will be reviewed by the Steering Committee and any adverse findings will be presented to the Board. Berar Finance Limited may additionally rely on third-party certifications, but it shall remain responsible for ensuring data security at the service provider's end.

Berar Finance Limited shall also ensure that the service provider provides unrestricted access to outsourced data and their premises for oversight purposes by Berar Finance Limited, their auditors, regulators, and other relevant Competent Authorities, as authorized under law.

The Technology team will present observations & insights, including any key risks from the audit program to the IT Steering Committee and IT Strategy Committee of the Board. The respective technology units shall work in conjunction with Service providers for defining timelines for closure of any audit observation and ensure closure of audit points in stipulated timeline.

4 Risk Management of IT Outsourcing Arrangement

Following successful IT outsourcing, Berar Finance Limited should actively manage the partnership with the outsourced vendor. Berar Finance Limited should build and adopt a risk management framework as part of IT outsourcing policy for managing risks associated with third party outsourcing engagements.

4.1 Risk Assessment of Outsourcing Arrangements

Respective technology units shall ensure to undertake a comprehensive risk assessment process for all IT outsourcing arrangements for service providers to understand the inherent risks associated with outsourcing.

These assessments should be ensured and reviewed by the Technology team, to examine potential operational, legal, financial, and reputational risks. The existing process of Vendor Inspection shall be part of the risk assessment process. This process shall aid informed decision-making and promote the use of effective risk mitigation strategies, consistent with the IT Outsourcing Policy. Risk assessment as per criticality matrix should follow process defined Mechanism for Assessing the Criticality of Outsourcing Arrangements.

4.2 Risk Reporting

Berar Finance 's Technology Team shall ensure to provide regular reports to the IT Strategy Committee stakeholders on their IT outsourcing arrangements. These reports should cover service provider performance, contract compliance, and risk management efforts.

During outsourcing engagement, following inputs should be used to prepare and manage detailed risk register for all outsourcing partners:

- **Issue and Incident Reports**: Any issues or incidents reported during review period.
- **Audit reports**: Any internal or external audit reports for outsourcing partner.
- **Performance Reports:** Report on the service provider's performance against the determined KPIs / SLAs and any deviation
- **Vendor inspection report:** Any deviation or inputs captured during vendor inspection process.

The defined risk management process shall involve maintaining a risk register. The Technology Team should include the following in the risk register:

- **Risk Description:** A detailed description of each risk identified.
- **Risk Impact:** An explanation of the potential impact of each risk.
- **Impact Level:** A rating or classification of the severity of each risk's potential impact.
- **Probability Level:** An estimation of the likelihood that each risk will occur.
- **Risk Mitigation Strategies**: A list of strategies devised to manage each risk, which could include avoidance, reduction, sharing, or acceptance.

The risk register should be updated regularly to reflect any changes in the risk landscape, ensuring that the IT Strategy Committee is informed to enable decision-making based on the most accurate and up-to-date information.

4.3 Risk Mitigation & Monitoring

The Technology Team should develop risk mitigation strategies for each outsourcing activity and monitor their efficacy. The technology unit shall undertake risk management measures which include:

- Identification of the potential risks in outsourcing activities and assessing their possible impacts.
- Creation of risk mitigation strategies based on risk assessments to minimize the potential impact.

- Conducting regular checks to understand the status of identified risks and the effectiveness of the mitigation strategies. The Technology Team shall ensure that the strategies are being implemented as intended and provide an early warning system for risks that are not being adequately managed.
- The technology team shall ensure regular reviewing and adjusting risk mitigation strategies based on the results of monitoring activities.
- The technology team shall ensure to provide updates on risk management activities and results to the IT Strategy Committee to enable transparency, accountability, & informed decision-making at the highest level.

4.4 Business Continuity Plan & Disaster Recovery

Berar Finance 's IT Outsourcing Policy shall ensure a robust and viable Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) is in place to mitigate the risk of unexpected termination of the outsourcing agreement relating to all Material Outsourcing Arrangements or liquidation of the concerned service provider.

Towards achieving the BCP & DR Plan, Berar Finance Limited should incorporate the following aspects:

- Service providers should implement and maintain BCP and DRP structures aligning with Reserve Bank of India issued master directions.
- Berar Finance Limited should ensure to consider alternative service providers and the possibility of in-house reintegration of outsourced activities in emergencies.
- The technology team shall assess factors such as costs, time, and resources involved in emergency scenarios.
- The technology team shall ensure mitigation of risks like unforeseen termination or service provider insolvency. The team must also maintain control over IT outsourcing arrangements, including the right to intervene and measures for business continuity.
- Berar Finance must ensure service providers can separate Berar Finance Limited information, documents, records, and assets which allows for removal, deletion, or destruction of all Berar Finance Limited owned materials from the service provider in case of contract termination.

4.5 Business Continuity Plan aspects for the Company

The focus of the business continuity plan is to expedite the restoration of operations, applications, and data following a disruptive event for associated outsourcing arrangements. The Technology Team shall incorporate the following aspects to measure the BCP's effectiveness:

- Respective technology unit shall prepare a contingency plan for outsourced service arrangement for material outsourcing covering recovery and restoration of services.
- Contingency plan for respective outsourcing contracts shall identify possible scenarios including unexpected termination as well as cover contingency measures such as approach for alternate service provider as well as measures to perform those services inhouse.

4.6 BCP & DR requirements from IT Outsourcing partners

Berar Finance should ensure its IT outsourcing partner's or service provider's Business Continuity Plans and Disaster Recovery strategies cover the following aspects:

- The IT outsourcing partner's Business Continuity Plans (BCP) and Disaster Recovery Plan (DR) need to align with Berar Finance's risk management process to ensure compatibility with the Berar Finance's systems and processes.
- The BCP and DR plans of the IT Outsourcing partners should ensure to limit downtime and prevent data loss as much as possible, ensuring swift recovery in the event of a disruption.

- The BCP and DR plans of the IT Outsourcing partners should be subject to regular audits. Reporting on these audits is necessary to ensure the plan’s ongoing effectiveness and alignment with Berar Finance’s requirements.
- The BCP and DR plan of the IT Outsourcing partners should comply with all relevant regulatory guidelines, including those set out by the Reserve Bank of India and any other authorities.
- The IT outsourcing partner should ensure to keep their BCP and DR strategies up to date, reflecting the evolving industry threats and trends to ensure the plan's resilience.

5 Exit Strategy

Berar Finance Limited's IT Outsourcing Policy shall ensure a comprehensive exit strategy for outsourced IT activities, ensuring business continuity. The respective technology units shall ensure that the exit strategy covers different exit scenarios and their execution timelines. The respective technology units shall also ensure alternative arrangements like switching to another service provider or internalizing the service. The respective business unit teams should monitor the exit strategy during actual transition to ensure safe disposal or destruction of data, hardware, and records by the service provider.

5.1 Defining exit needs from an IT Outsourcing partner

The IT outsourcing partner shall securely transfer data from the outgoing service provider to the Berar Finance Limited or new service provider. The IT outsourcing partner shall ensure uninterrupted service during the transition period, fulfil contractual obligations with the outgoing service provider, and maintain confidentiality and data security standards throughout the transition process.

The IT Outsourcing Partner shall safely decommission systems and securely terminate the outgoing service provider's access to Berar Finance Limited’s systems and data to prevent unauthorized access or potential data breaches.

The agreement with the respective service providers should cover the secure removal of data and hardware, ensuring full cooperation from the service provider for a smooth transition.

5.2 Exit Strategy & Company’s readiness

Berar Finance Limited shall ensure preparedness to implement an exit strategy by following a structured process which involves creating a detailed exit plan and designating a dedicated team to manage the transition. The compliance team shall undertake a legal review to ensure all regulatory and contractual obligations are met. The respective technology team shall ensure operational readiness for service continuity, procedures for secure data transfer, and arrangements for new services if a new provider is engaged.

5.3 Exit Strategy - Role & Responsibilities of Berar Finance

During the exit procedure, the role & responsibilities of the technology team off Berar Finance ’s shall cover the following aspects:

- Manage the coordination of all activities along with the concerned business unit.
- Work with the legal team to ensure all legal requirements are met.
- Ensure to oversee secure transfer of data.

6 Different outsourcing arrangements

6.1 Cross-Border Outsourcing

Berar Finance Limited may explore and outsource certain technology services to service providers operating outside India which may fall into cross-border outsourcing arrangements. In such scenarios, Berar Finance Limited shall ensure to:

- CISO and technology shall explore relevant government policies having wider impact on country level risks related to such cross-border outsourcing arrangements.
- Outsourcing contracts with such service providers shall clearly define the governing law of the arrangement, availability of all records to Berar Finance Limited & the RBI, adherence to regulatory requirements.
- The cross-border outsourcing agreement must guarantee Berar Finance Limited and RBI's authority to instruct and perform audits or inspections of the service provider based in a foreign jurisdiction.
- The arrangement must adhere to all statutory compliances as well as regulations issued by the RBI periodically.

6.2 Usage of Cloud Computing

With the evolution of Cloud computing and its inherent benefits to support Berar finance Limited's digital transformation programs, Berar Finance Limited has started engaging with cloud service providers for cloud services for any service model for moving non-critical workloads to business-critical workloads.

To enhance cost-efficiency and improve management, numerous service providers of critical Berar Finance Limited applications are choosing to offer Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), for application delivery. Consequently, Berar Finance Limited has considered adopting SaaS-based solutions for essential Berar Finance Limited. operations, including lending and fixed deposit management solution.

Key considerations shall be taken care of in such outsourcing arrangements to the cloud, in addition to adherence to IT outsourcing policy. These specific considerations include:

- Berar Finance Limited shall develop a cloud adoption policy and shall use the policy while onboarding such cloud service providers.
- The policy should provide for appropriate due diligence to manage and continually monitor the risks associated with Cloud service providers.

Annexure I: List of activities to be conducted for respective vendors:

The following matrix below is to indicate and identify if the below activities are to be conducted for vendors that are identified as material and non-material in nature:

Particulars	Material Vendors	Non - Material Vendors
1. Due Diligence	Yes	Yes
2. Evaluation of the vendor	Yes	Yes
3. Due Diligence at Renewal	Yes	Yes
4. Audit	Yes	No
5. Vendor Inspection/Assessment	Yes – Half yearly	Yes - Annual
6. Risk Assessment	Yes -Half Yearly	Yes - Annual
7. Exit Strategy	Yes	No
8. Contingency Plan	Yes	No

Annexure 2: List of responsibilities to be fulfilled by respective teams:

The following matrix below is to indicate the responsibilities of the respective teams at Berar Finance

Particulars	Responsibilities
1. Technology Team	▪ Drives technology outsourcing and ensures compliance. ▪ Oversees outsourced activities, identify & manage IT outsourcing risk, and implements the IT outsourcing policy. ▪ Perform Evaluation, Due diligence for identified outsourced partners. ▪ Ensure disaster recovery, business continuity, and compliance with outsourcing instructions. ▪ Manage IT outsourcing compliance, aligns IT operations with strategic goals, oversees contracts, and ensures business continuity and exit strategies. ▪ Develop & Maintain the IT Outsourcing Policy, identifies potential risks, and ensures regulatory compliance.
2. Business Unit	▪ Assessment of Outsourcing Needs for business specific cases ▪ Assist in Due Diligence for business specific technology outsourcing
3. Information Security Team	▪ Oversee risk in IT outsourcing, reviews compliance, identifies potential risks, and conducts audits. ▪ Ensure third-party security policy compliance, addresses security breaches, and refines the IT Outsourcing Policy.
4. Internal Audit Department	▪ Conduct audits as per provisions of the IT Outsourcing Policy as well as the audit plan. ▪ To plan audits of material vendors and enable closure
5. Compliance Department	▪ To review compliance status of vendors identified across the NBFC level
6. Legal Department	▪ Legal vetting of agreements and provide guidance on legal aspects pertaining IT Outsourcing arrangements
7. Risk Management Committee	▪ Review and guide on the identification of underlying risks and risk mitigation strategies
8. End users of Berar Finance IT Resources	▪ Read & abide the policy

Annexure 3: Services not considered under Outsourcing of IT Services

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

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

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

iii. SMS gateways (Bulk SMS service providers)

iv. Procurement of IT hardware/ appliances

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

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

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

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

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

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

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

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

I. Vendors providing business services using IT. Example – BCs
II. Payment System Operators authorised by the Reserve Bank of India under the Payment and Settlement Systems Act, 2007 for setting up and operating Payment Systems in India
III. Partnership based Fintech firms such as those providing co-branded applications, service, products (would be considered under outsourcing of financial services)
IV. Services of Fintech firms for data retrieval, data validation and verification services such as (list is not exhaustive):

a) Bank statement analysis.
b) GST returns analysis.
c) Fetching of vehicle information
d) Digital document execution
e) Data entry and Call centre services

v. Telecom Service Providers from whom leased lines or other similar kinds of infrastructure are availed and used for transmission of the data.

vi. Security/ Audit Consultants appointed for certification/ audit/ VA-PT related to IT infra/ IT services/ Information Security services in their role as independent third-party auditor/ consultant/ lead implementer.

Annexure 4: Approval Matrix for evaluation and engagement for Outsourcing of IT Services

Initiator/ Recommender	Approver
Business SPOC	Business Unit Head
IT SPOC	Head-IT
Risk Management Team	Chief Risk Officer
Internal Audit	Head-Internal Audit
Business	MD & CEO

Annexure 5: Evaluation and Engagement of Service Providers

Aspects to be considered:

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

- past experience and demonstrated competence to implement and support the proposed IT activity over the contract period.
- financial soundness and ability to service commitments even under adverse conditions.
- business reputation and culture, compliance, complaints and outstanding or potential litigations.
- conflict of interest, if any.
- 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.
- details of the technology, infrastructure stability, security and internal control, audit coverage, reporting and monitoring procedures, data backup arrangements, business continuity management and disaster recovery plan.
- capability to identify and segregate REs data.
- quality of due diligence exercised by the service provider with respect to its employees and subcontractors.
- capability to comply with the regulatory and legal requirements of the Outsourcing of IT Services arrangement.
- information/ cyber security risk assessment.
- ensuring that appropriate controls, assurance requirements and possible contractual arrangements are in place to ensure data protection and RE's access to the data which is processed, managed or stored by the service provider.
- ability to effectively service all the customers while maintaining confidentiality, especially where a service provider has exposure to multiple entities; and
- ability to enforce agreements and the rights available thereunder including those relating to aspects such as data storage, data protection and confidentiality.

Annexure 6: Aspects to be considered in agreement

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

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

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

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

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

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

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

g. storage of data (as applicable to the Company) only in India as per extant regulatory requirements.

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

i. controls for maintaining confidentiality of data of the Company and its customer's, and incorporating service provider's liability to the Company in the event of security breach and leakage of such information.

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

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

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

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

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

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

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

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

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

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

t. obligation of the service provider to cooperate with the relevant authorities in case of insolvency/ resolution of the RE.

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

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

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