Outsourcing Policy

blacksoil
AN ALTERNATE CREDIT PLATFORM

Content Management

Document Control	
Title	Outsourcing Policy
DOC ID/ Number	BCPL/POLICY/Outsourcing Policy/V.2
Policy Owner	Compliance Team
Last Update date	021/02/2024
Reviewed by	Whole Time Director
Approved by	Board of Directors

Version	Updates	Reviewed Date	Approved by
2024_V2	Outsourcing Policy	21/02/2024	Board of Directors

Review/Revision of policy:

This policy document will be reviewed and revised by the Compliance Team with Whole Time Director consultation with approval of board of directors in response to changed circumstances, and in any event, at intervals of not more than half year or shorter review periods as may be stipulated by the board of directors.

Regulatory Reference:

- RBI/DoR/2023-24/106, DoR.FIN.REC.No.45/03.10.119/2023-24 Master Direction - Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2023 dated October 19, 2023.

- RBI/2017-18/87 Directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs DNBR.PD.CC. No.090/03.10.001/2017-18 November 09, 2017

- RBI/2022-23/108 DOR.ORG.REC.65/21.04.158/2022-23 directions /circular on outsourcing of Financial Services - Responsibilities of regulated entities employing Recovery Agents dated 12th August 2022

- RBI/2023-24/102 DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 directions /circular on outsourcing of Information Technology Services dated 10th April 2023

Annexure

- Code of Conduct in Outsourcing of Financial Services- by NBFCs

Introduction

Blacksoil Capital Private limited (herein referred to as "BCPL" or "the Company") is a Systemically Important, Non-Deposit taking, Non-Banking Finance Company (NBFC-ND-SI) registered with RBI. It is base layer NBFC as defined under master directions Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2023, RBI/DoR/2023-24/105 DoR.FIN.REC. No.45/03.10.119/2023-24 dated 19 October 2023.

BCPL provides debt facility to growth companies, Financial Institutions and Supply Chain Financing for SME channel partners for their purchases and sales invoices.

Description of Debt facilities are mentioned below:

Growth Companies (GC) Financing:	• An alternative credit solution to companies that have proactively refined their business models to enhance sustainability and receive unwavering support from their existing and new equity investors.
Financial Institutions (FI):	• An alternative credit solution to NBFCs and Fintech players, including MFIs, MSMEs, Personal Loans, and HFCs.
Supply Chain Financing (SCF):	• SaralSCF offers three products - Saral Supply Chain Credit to Anchor, Saral Vendor Finance and Saral Pay Later, each committed to providing flexible credit solutions to address the working capital needs of businesses.

'Outsourcing' is defined as the NBFC's use of a Third-Party hereafter referred as ("Service Provider") to perform activities on continuing basis that would normally be undertaken by the NBFC itself, now or in the future. 'Continuing basis' includes agreements for a limited period.

Typically, 'Outsourced financial services' includes applications processing (loan origination), document processing, marketing and research, supervision of loans, data processing and back office related activities, besides others.

Part A . Policy on Outsourcing of Financials Services by the Company

Table of Contents

1. Objectives & Regulatory Framework 5
2. Roles & Responsibility 6
3. Risk in Outsourcing 7
4. Evaluation & Selection of Service Provider 7
5. Outsourcing Contract 8
6. Confidentiality and Security 9
7. Responsibilities of Direct sales agents (DSA)/Direct Marketing Agents (DMA) /Recovery Agents 10
8. Business Continuity and Management of Disaster Recovery Plan 10
9. Monitoring and Control of Outsourced Activities 11
10. Reporting of transactions to FIU or other competent authorities 11
11. Outsourcing within the group 12
12. Off-shore outsourcing of Financial Services 13
Appendix 29

1. Objectives & Regulatory Framework

BCPL may be intending to outsource any of its financial activities shall put in place a comprehensive outsourcing policy approved by its Board, which incorporates, inter alia criteria for selection of such activities as well as service providers, delegation of authority depending on risks and materiality and systems to monitor and review the operations of these activities.

The objective of having policy in place for outsourcing activity is to protect the interest of the customers & investor of BCPL and to ensure that the Company and the Reserve Bank of India have access to all relevant books, records and information available with service provider and to ensure that outsourcing arrangements neither diminish its ability to fulfil its obligations to customers and RBI nor impede effective supervision by RBI.

BCPL therefore shall take steps to ensure that the service provider employs the same high standard of care in performing the services as is expected to be employed by the BCPL, as if the activities were conducted within the BCPL and not outsourced. Accordingly, BCPL shall not engage in outsourcing that would result in the Company's internal control, business conduct or reputation being compromised or weakened.

RBI Directions

RBI has issued directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by the Company (NBFCs). The directions are applicable to material outsourcing arrangements which may be entered into by an NBFC with a service provider located in India or elsewhere. The service provider may either be a member of the group/ conglomerate to which the NBFC belongs or an unrelated party.

These directions are concerned with managing risks in outsourcing of financial services and are not applicable to technology-related issues and activities which are not related to financial services, such as usage of courier, catering of staff, housekeeping and janitorial services, security of the premises, movement and archiving of records etc.

Activities that shall not be outsourced

BCPL if choose to outsource financial services shall not outsource following services:

- Core management functions including internal audit, strategic and compliance functions.
- Decision-making functions such as determining compliance with KYC norms.
- Sanction of loans.
- Management of investment portfolio.

However, for NBFCs in a group/ conglomerate, these functions may be outsourced within the group subject to compliance with instructions elaborated below in outsourcing within the group.

Material Outsourcing Means

For the purpose of these directions, material outsourcing arrangements are those which, if disrupted, have the potential to significantly impact the business operations, reputation, profitability or customer service. Materiality of outsourcing would be based on various factors mentioned below:

- the level of importance to the NBFC of the activity being outsourced as well as the

significance of the risk posed by outsourced activity;

- the potential impact of the outsourcing activity on the NBFC on various parameters such as earnings, solvency, liquidity, funding capital and risk profile;
- the likely impact on the NBFC's reputation and brand value, and ability to achieve its business objectives, strategy and plans, if the service provider fails to perform the services;
- the cost of the outsourcing activity as a proportion of total operating costs of the NBFC;
- the aggregate exposure to that particular service provider, in cases where the NBFC outsources various functions to the same service provider and

- the significance of activities outsourced in context of customer service and protection.

2. Roles & Responsibility

i. Roles & Responsibility of Board of Directors

- Approving a framework to evaluate the risks and materiality of all existing and prospective outsourcing activities and the policies that apply to such arrangements.
- Deciding on business activities of a material nature to be outsourced and approving such arrangements;
- Laying down appropriate approval authorities for outsourcing depending on risks and materiality;
- Setting up suitable administrative framework of senior management for the purpose of these directions;
- Undertaking regular review of outsourcing strategies and arrangements for their continued relevance, safety and soundness;
- Shall take the responsibility for the actions of their service provider
- Shall take the responsibility to maintain the confidentiality of information pertaining to the customers that is available with the service provider;
- Shall ensure that the service provider, if not a group company of the BCPL, shall not be owned or controlled by any director of the Company or their relatives. These terms have the same meaning as assigned under Companies Act, 2013.

ii. Roles & Responsibility of Senior Management & Team

- Evaluating the risks and materiality of all existing and prospective outsourcing based on the framework approved by the Board;
- Developing and implementing sound and prudent outsourcing policies and procedures commensurate with the nature, scope and complexity of the outsourcing activity;
- Reviewing periodically the effectiveness of policies and procedures;
- Communicating information pertaining to material outsourcing risks to the Board in a timely manner;
- Ensuring that contingency plans, based on realistic and probable disruptive scenarios

of service provider, are in place and tested;

- Ensuring that there is independent review and audit for compliance with set policies;
- Undertaking periodic review of outsourcing arrangements to identify new material outsourcing risks as they arise and
- Shall ensure to have a robust grievance redress mechanism, which in no way shall be compromised on account of outsourcing.

3. Risk in Outsourcing

The key risks in outsourcing are Strategic Risk, Compliance Risk, Operational Risk, Legal Risk, Exit Strategy Risk, Counterparty Risk, Country Risk, Contractual Risk, Concentration and Systemic Risk. The failure of a service provider in providing a specified service, a breach in security/ confidentiality, or non-compliance with legal and regulatory requirements by the service provider can lead to financial losses or loss of reputation for the Company.

The BCPLs shall evaluate and guard against the following risks in outsourcing:

- Strategic Risk – Where the service provider conducts business on its own behalf, inconsistent with the overall strategic goals of the Company.
- Reputation Risk – Where the service provided is poor and customer interaction is not consistent with the overall standards expected of the Company.
- Compliance Risk – Where privacy, consumer and prudential laws are not adequately complied with by the service provider.
- Operational Risk- Arising out of technology failure, fraud, error, inadequate financial capacity to fulfil obligations and/ or to provide remedies.
- Legal Risk – Where the BCPL may be subjected to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements due to omissions and commissions of the service provider.
- Exit Strategy Risk – Where the Company may over-reliant on one firm, the loss of relevant skills in the Company itself preventing it from bringing the activity back in-house and contracts that make speedy exits prohibitively expensive.
- Counter party Risk – Where there is inappropriate underwriting or credit assessments.
- Contractual Risk – Where the BCPL may not have the ability to enforce the contract.
- Concentration and Systemic Risk – Where the overall industry has considerable exposure to one service provider and hence the Company may lack control over the service provider.
- Country Risk – Due to the political, social and legal climate creating added risk.

4. Evaluation & Selection of Service Provider

In considering or renewing an outsourcing arrangement, appropriate due diligence shall be performed to assess the capability of the service provider to comply with obligations in the outsourcing agreement. Due diligence shall take into consideration qualitative and quantitative, financial and operational factors.

BCPL shall consider whether the service provider's systems are compatible with its own and also whether their standards of performance including in the area of customer service are acceptable to it. The Company shall also consider, issues relating to undue concentration of outsourcing arrangements with a single service provider. Wherever possible, the Company shall obtain independent reviews and market feedback on the service provider to supplement its own findings.

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

- Past experience and competence to implement and support the proposed activity over the contracted period;
- Financial soundness and ability to service commitments even under adverse conditions;
- Business reputation and culture, compliance, complaints and pending / potential litigations;
- Security and internal control, audit coverage, reporting and monitoring environment, business continuity management and ensuring due diligence by service provider of its employees.

Further if due diligence seems all right then the selection should be done as follows:

- Service Provider's resources and capabilities, including financial soundness, to perform the outsourcing work within the timelines fixed;
- Compatibility of the practices and systems of the service provider with the BCPL's requirements and objectives;

  Market feedback of the prospective service provider's business reputation and track record of their services rendered in the past;
- Level of concentration of the outsourced arrangements with a single party;

5. Outsourcing Contract

BCPL shall ensure the terms and conditions governing the contract with the service provider are carefully defined in written agreements and vetted by BCPL's legal team on their legal effect and enforceability. Every such agreement shall address the risks and risk mitigation strategies. The agreement shall be sufficiently flexible to allow BCPL to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations. The agreement shall also bring out the nature of legal relationship between the parties- i.e. whether agent, principal or otherwise.

BCPL will consider some of the key provisions while entering into contract with the service provider, which are mentioned below:

- The contract shall clearly define what activities are going to be outsourced including appropriate service and performance standards;
- Ensure that BCPL has the ability to access all books, records and information relevant to the outsourced activity available with the service provider;

  The contract shall provide for continuous monitoring and assessment by the BCPL of the service provider so that any necessary corrective measure can be taken immediately;

- Termination clause and minimum period to execute a termination provision, if deemed necessary shall be included;
- Controls to ensure customer data confidentiality and service providers liability in case of breach of security and leakage of confidential customer related information shall be incorporated;
- There must be contingency plans to ensure business continuity;
- The contract shall provide for the prior approval/ consent by BCPL of the use of subcontractors by the service provider for all or part of an outsourced activity;
- It shall provide the Company with the right to conduct audits on the service provider whether by its internal or external auditors, or by agents appointed to act on its behalf and to obtain copies of any audit or review reports and findings made on the service provider in conjunction with the services performed for the BCPL;
- Outsourcing agreements shall include clauses to allow the Reserve Bank of India or persons authorized by it to access the BCPL's documents, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time;
- Outsourcing agreement shall also include a clause to recognize the right of the Reserve Bank to cause an inspection to be made of a service provider of the Company and its books and account by one or more of its officers or employees or other persons;
- The outsourcing agreement shall also provide that confidentiality of customer's information shall be maintained even after the contract expires or gets terminated and the BCPL shall have necessary provisions to ensure that the service provider preserves documents as required by law and take suitable steps to ensure that its interests are protected in this regard even post termination of the services.

Further care shall be taken to ensure that the outsourcing contract:

- Provides for mutual rights, obligations and responsibilities of the Company and the Service Provider, including indemnity by the parties;
- Provides for the liability of the Service Provider to the Company for unsatisfactory performance/other breach of the contract;

6. Confidentiality and Security

Public confidence and customer trust are prerequisites for the stability and reputation of the Company. Hence BCPL shall seek to ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the service provider. BCPL shall ensure that:

- Access to customer information by staff of the service provider shall be on 'need to know' basis i.e. limited to those areas where the information is required in order to perform the outsourced function.
- The service provider is able to isolate and clearly identify the BCPL's customer information, documents, records and assets to protect the confidentiality of the information.

In instances, where service provider acts as an outsourcing agent for multiple NBFCs, care shall be taken to build strong safeguards so that there is no commingling of information / documents, records and assets.

- Regular review and monitoring of the security practices and control processes of the service provider and require the service provider to disclose security breaches.
- Immediately notify RBI in the event of any breach of security and leakage of confidential customer-related information. In these eventualities, the Company/BCPL would be liable to its customers for any damages.

7. Responsibilities of Direct Sales Agents (DSA)/Direct Marketing Agent (DMA)/ Recovery Agents

- BCPL shall ensure that the DSA/ DMA/ Recovery Agents are properly trained to handle their responsibilities with care and sensitivity, particularly aspects such as soliciting customers, hours of calling, privacy of customer information and conveying the correct terms and conditions of the products on offer, etc.
- BCPL shall put in place a board approved Code of conduct for DSA/ DMA/ Recovery Agents, and obtain their undertaking to abide by the code. In addition, Recovery Agents shall adhere to extant instructions on Fair Practices Code for NBFCs as also their own code for collection of dues and repossession of security. It is essential that the Recovery Agents refrain from action that could damage the integrity and reputation of the NBFC and that they observe strict customer confidentiality.
- The Company and their agents shall not resort to intimidation or harassment of any kind, either verbal or physical, against any person in their debt collection efforts, including acts intended to humiliate publicly or intrude the privacy of the debtors' family members, referees and friends, sending inappropriate messages either on mobile or through social media, making threatening and anonymous calls, persistently calling the borrower and/or calling the borrower before 8:00 a.m. and after 7:00 p.m. for recovery of overdue loans, making false and misleading representations, etc. BCPL shall ensure that there are no violations in this regards.

8. Business Continuity and Management of Disaster Recovery Plan

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

In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, the Company shall retain an appropriate level of control over their outsourcing and the right to intervene with appropriate measures to continue its business operations in such cases without incurring prohibitive expenses and without any break in the operations of the Company and its services to the customers.

In establishing a viable contingency plan, BCPL 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.

BCPL will make sure that service providers are able to isolate the Company's information, documents and records, and other assets so that in appropriate situations, all documents, records of transactions and information given to the service provider, and assets of the BCPL, can be removed from the possession of the service provider in order to continue its business operations, or deleted, destroyed or rendered unusable.

9. Monitoring and Control of Outsourced Activities

The Company shall have in place a management structure to monitor and control its outsourcing activities. It shall ensure that outsourcing agreements with the service provider contain provisions to address their monitoring and control of outsourced activities.

A central record of all material outsourcing that is readily accessible for review by the Board and senior management of the Company shall be maintained. The records shall be updated promptly and half yearly basis reviews shall be placed before the Board or Risk Management Committee.

Regular audits would be done by either the internal auditors or external auditors of the Company to assess the adequacy of the risk management practices adopted in overseeing and managing the outsourcing arrangement.

BCPL shall at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet its outsourcing obligations. Such due diligence reviews, which can be based on all available information about the service provider shall highlight any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness.

In the event of termination of the outsourcing agreement for any reason in cases where the service provider deals with the customers, the same shall be publicized by displaying at a prominent place in all the offices, posting it on the website, and informing the customers so as to ensure that the customers do not continue to deal with the service provider.

A robust system of internal audit of all outsourced activities shall also be put in place and monitored by the Audit Committee of the Board (ACB) of the Company.

10. Reporting of transactions to FIU or other competent authorities

The Company would be responsible for making Currency Transactions Reports and Suspicious Transactions Reports to FIU or any other competent authority in respect of the NBFCs' customer related activities carried out by the service providers.

11. Outsourcing within the group

In a group structure, the Company may have back-office and service arrangements/ agreements with group entities e.g. sharing of premises, legal and other professional services, and hardware and software applications, centralize back-office functions, outsourcing certain financial services to other group entities etc.

Before entering into such arrangements with group entities the Company shall have an arrangement with their group entities which shall also cover demarcation of sharing resources i.e. premises, personnel, etc. Moreover, the customers shall be informed specifically about the company which is actually offering the product/ service, wherever there are multiple group entities involved or any cross selling observed.

While entering into such arrangements, BCPL shall ensure that:

- Arrangements are appropriately documented in written agreements with details like scope of services, charges for the services and maintaining confidentiality of the customer's data;
- Such arrangement does not lead to any confusion to the customers on whose products/ services they are availing by clear physical demarcation of the space where the activities of the BCPL and those of its other group entities are undertaken;
- Such arrangements do not compromise the ability to identify and manage risk of the Company on a stand-alone basis;
- Incorporate a clause under the written agreements that there is a clear obligation for any service provider to comply with directions given by the RBI in relation to the activities of the BCPL;
- BCPL shall ensure that their ability to carry out their operations in a sound fashion would not be affected if premises or other services (such as IT systems, support staff) provided by the group entities become unavailable;
- If the premises of the BCPL are shared with the group entities for the purpose of cross-selling, The Company shall take measures to ensure that the BCPL's identification is distinctly visible and clear to the customers. The marketing brochure used by the group entity and verbal communication by its staff / agent in the BCPL premises shall mention nature of arrangement of the entity with the BCPL so that the customers are clear on the seller of the product.
- BCPL shall not publish any advertisement or enter into any agreement stating or suggesting or giving tacit impression that they are in any way responsible for the obligations of its group entities.
- The risk management practices expected to be adopted by the Company while outsourcing to a related party (i.e. party within the Group / Conglomerate) would be identical to those specified in Para 5 of this directions.

12. Off-shore outsourcing of Financial Services

The engagement of service providers in a foreign country exposes a Company to country risk - economic, social and political conditions and events in a foreign country that may adversely affect the Company. Such conditions and events could prevent the service provider from carrying out the terms of its agreement with the Company. To manage the country risk involved in such outsourcing activities, the BCPL shall take into account and closely monitor government policies and political, social, economic and legal conditions in countries where the service provider is based, both during the risk assessment process and on a continuous basis and establish sound procedures for dealing with country risk problems. This includes having appropriate contingency and exit strategies. In principle, arrangements shall only be entered into with parties operating in jurisdictions generally upholding confidentiality clauses and agreements. The governing law of the arrangement shall also be clearly specified.

The activities outsourced outside India shall be conducted in a manner so as not to hinder efforts to supervise or reconstruct the India activities of BCPL in a timely manner.

As regards the off-shore outsourcing of financial services relating to Indian Operations, the Company shall additionally ensure that:

- Where the off-shore service provider is a regulated entity, the relevant off-shore regulator will neither obstruct the arrangement nor object to RBI inspection visits/ visits of the Company's internal and external auditors.
- The availability of records to management and the RBI will withstand the liquidation of either the offshore custodian or the Company in India.
- The regulatory authority of the offshore location does not have access to the data relating to Indian operations of the Company simply on the ground that the processing is being undertaken there (not applicable if off shore processing is done in the home country of the Company).
- The jurisdiction of the courts in the off shore location where data is maintained does not extend to the operations of the Company in India on the strength of the fact that the data is being processed there even though the actual transactions are undertaken in India and
- All original records continue to be maintained in India.

Part B . Policy on Outsourcing of Information Technology Services by the Company

Table of Contents

1. Objectives & Regulatory Framework 15
2. Definitions 16
3. Role of Regulated Entity 16
4. Governance Framework 17
5. Evaluation and Engagement of Service Providers 19
6. Outsourcing Agreement 20
7. Risk Management 22
8. Business Continuity Plan and Disaster Recovery Plan 23
9. Monitoring and Control of Outsourced Activities 23
10. Outsourced within a Group /Conglomerate 24
11. Additional requirements for Cross- Border Outsourcing 24
12. Exit Strategy 25
13. Storage, Computing and Movement of Data in Cloud Environments- Usage of Cloud Computing Services 25
14. Outsourcing of Security Operations Centre 28
15. Services not considered under Outsourcing of IT Services 28

Appendix 29

1. Objectives & Regulatory Framework

On April 10, 2023, the Reserve Bank of India ('RBI') issued the final Master Direction on Outsourcing of Information Technology Services ('the Direction') which has been finalized based on the feedback received on the draft Master Direction on Outsourcing of Information Technology (IT) Services released on 23 June 2022. The Directions have been formulated in an effort to regulate various risks arising from Regulated Entities leveraging on Information Technology (IT) and IT-enabled services (ITeS) in their business, products and services with increasing dependence on third parties.

Along with other Regulated Entities (ORE) specifically referred in the Direction, this Direction is also applicable, inter alia, to Non-Banking Financial Companies as defined under clause (f) of Section 45I of the Reserve Bank of India Act, 1934 and included in the 'Top Layer', 'Upper Layer' and 'Middle Layer' as set out in the Scale Based Regulation (SBR): A Revised Regulatory Framework for NBFCs.

The underlying principle of these Directions is to ensure that outsourcing arrangements neither diminish Res/the company's ability to fulfil its obligations to customers nor impede effective supervision by the RBI.

The Directions shall apply to Material Outsourcing of Information Technology ('IT') services arrangements and shall come into effect from October 01, 2023.

A) With respect to Existing Outsourcing Arrangements

- Agreements due for renewal before October 1, 2023, shall comply with the provisions of the Directions as on the renewal date (preferably), but not later than 12 months from the date of issuance of the Direction i.e. April 10, 2023.
- Agreements that are due for renewal on or after October 1, 2023, shall comply with the provisions of the Directions as on the renewal date or 36 months from the date of issuance of the Direction i.e. April 10, 2023 whichever is earlier.

B) With respect to New Outsourcing Arrangements

- Agreements that come into force before October 1, 2023, shall comply with the provisions of the Directions as on the agreement date (preferably) but not later than 12 months from the date of issuance of the Direction i.e. April 10, 2023.
- Agreements that come into force on or after October 1, 2023, shall comply with the provisions of the Directions from the date of agreement itself.

2. Definitions

i) Material Outsourcing of IT Services: are those which

a) if disrupted or compromised shall have the potential to significantly impact the Company's business operations; or

b) may have material impact on the Company's customers in the event of any unauthorized access, loss or theft of customer information.

ii) Outsourcing of Information Technology ("IT") Services : shall include outsourcing of the following activities:

- IT infrastructure management, maintenance and support (hardware, software or firmware);
- Network and security solutions, maintenance (hardware, software or firmware);
- Application Development, Maintenance and Testing; Application Service Providers (ASPs) including ATM Switch ASPs;
- Services and operations related to Data Centres;
- Cloud Computing Services;
- Managed Security Services; and
- Management of IT infrastructure and technology services associated with payment system ecosystem.

iii) Service Provider: The term "Service Provider" means the provider of IT or IT enabled services. Service Provider includes, but is not limited to, the vendors, agencies, consultants and / or representatives of the third parties. It also includes subcontractors to whom the third-party service providers may further outsource some activity.

3. Role of the Regulated Entity- BCPL

A) Regulatory and Supervisory requirements:

- The outsourcing of any activity shall not diminish BCPL's obligations as also of its Board and Senior Management, who shall be ultimately responsible for the outsourced activity. The Company shall take steps to ensure that the service provider employs the same high standard of care in performing the services as would have been employed by the Company if the same activity was not outsourced. The

  Company shall not engage an IT service provider that would result in reputation of BCPL being compromised or weakened.

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

- BCPL shall ensure that the service provider, if not a group company, shall not be owned or controlled by any director, or key managerial personnel, or approver of the outsourcing arrangement of the Company, 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 6 framed thereunder from time to time. However, an exception to this requirement may be made with the approval of Board/ Board level Committee, followed by appropriate disclosure, oversight and monitoring of such arrangements. The Board shall inter-alia ensure that there is no conflict of interest arising out of third-party engagements.

- Additional requirements pertaining to usage of cloud computing services and outsourcing of Security Operations Center (SOC) services are outlined in Paragraph 13 and 14 of the Part B, respectively.

B) Comprehensive assessment of need for outsourcing and attendant risks :

The Company shall evaluate the need for Outsourcing of IT Services based on comprehensive assessment of attendant benefits, risks and availability of commensurate processes to manage those risks. BCPL shall consider important aspects, such as ;

- Determining the need for outsourcing based on criticality of activity to be outsourced;
- Determining expectations and outcome from outsourcing;
- Determining success factors and cost-benefit analysis; and
- Deciding the model for outsourcing.

C) Compliance with all applicable statutory and regulatory requirements :

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

D) Grievance Redressal Mechanism :

- The Company 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 Company.

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

E) Inventory of Outsourced Services :

BCPL shall create an inventory of services provided by the service. Further, the Company shall map their dependency on third parties and periodically evaluate the information received from the service providers.

4. Governance Framework

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

A) Role of the Board

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

- putting in place approving a framework for approval of IT outsourcing activities depending on risks and materiality;
- approving policies to evaluate the risks and materiality of all existing and prospective IT outsourcing arrangements; and
- setting up suitable administrative framework of Senior Management for the purpose of these Directions.

Further the Board may delegate the above responsibilities to IT Strategy Committee of the Company.

B) Role of the Senior Management

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

- 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;
- 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;
- identifying IT outsourcing risks as they arise, monitoring, mitigating, managing and reporting of such risks to the Board/ Board Committee in a timely manner;
- 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;
- ensuring (i) effective oversight over third party for data confidentiality and (ii) appropriate redressal of customer grievances in a timely manner;
- ensuring an independent review and audit on a periodic basis for compliance with the legislations, regulations, Board-approved policy and performance standards and reporting the same to Board/ Board Committee; and
- creating essential capacity with required skillsets within the organization for proper oversight of outsourced activities.

C) Role of IT Function

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

- assisting the Senior Management in identifying, measuring, monitoring, mitigating and managing the level of IT outsourcing risk in the organisation;
- ensuring that a central database of all IT outsourcing arrangements is maintained and is accessible for review by Board, Senior Management, Auditors and Supervisors;

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

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

5. Evaluation and Engagement of Service Providers

- In considering or renewing an Outsourced IT Services arrangement, appropriate due diligence shall be performed to assess the capability of the service provider to comply with obligations in the outsourcing agreement on an ongoing basis. Due diligence shall take into consideration qualitative, quantitative, financial, operational, legal and reputational factors. The Company shall also consider, while evaluating the capability of the service provider, risks arising from the concentration of outsourcing arrangements with a single/ few service provider/s. Where possible, the Company shall obtain independent reviews and market feedback on the service provider to supplement its own assessment.

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

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

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

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

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

  d. conflict of interest, if any;

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

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

  g. capability to identify and segregate the Company's data;

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

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

j. information/ cyber security risk assessment;

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

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

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

6. Outsourcing Agreement

- The Company shall ensure that its rights and obligations and those of each of its service providers are clearly defined and set out in a legally binding written agreement. In principle, the provisions of the agreement should appropriately reckon the criticality of the outsourced task to the business of the Company, the associated risks and the strategies for mitigating or managing them.

- The terms and conditions governing the contract shall be carefully defined and vetted by the Company's legal counsel for their legal effect and enforceability. The agreement shall be sufficiently flexible to allow the Company to retain 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, i.e., whether agent, principal or otherwise.

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

  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; including termination clause and minimum period to execute such provision, if deemed necessary;

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

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

  f. the deliverables, including Service-Level Agreements (SLAs) formalising performance criteria

to measure the quality and quantity of service levels;

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

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

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

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 company, including the ability to orderly transfer the proposed IT-outsourcing arrangement to another service provider, if necessary or desirable;

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

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.

The Company has the right to extend the above clauses of the agreement to any agencies to which the service provider sub-contracts any activity related to IT services outsourced by the Company.

7. Risk Management

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

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

- BCPL shall be responsible for the confidentiality and integrity of data and information pertaining to the customers that is available to the service provider.

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

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

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

- In instances where service provider acts as an outsourcing agent for multiple Company, care shall be taken to build adequate safeguards so that there is no combining of information, documents, records and assets. The Company shall ensure that a Non-Disclosure Agreement ("NDA") is in place even after the contract expires/is terminated.

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

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

- **Concentration Risk**: The Company 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.

8. Business Continuity Plan and Disaster Recovery Plan

- The Company shall require their service providers to develop and establish a robust framework for documenting, maintaining and testing Business Continuity Plan ("BCP") and Disaster Recovery Plan ("DRP") commensurate with the nature and scope of the outsourced activity as per extant BCP/ DR requirements.

- In establishing a viable contingency plan, the Company 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.

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

- The Company shall ensure that service providers are able to isolate the Company's information, documents and records and other assets. This is to ensure that in adverse conditions and/or termination of the contract, all documents, record of transactions and information with the service provider and assets of the Company can be removed from the possession of the service provider in order to continue its business operations, or deleted, destroyed or rendered unusable.

9. Monitoring and Control of Outsourced Activities

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

- The Company 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 the Company's internal auditors or external auditors appointed to act on the Company's behalf.

- 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 Companies 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 the

Company in ensuring that the audit requirements related to their respective contract with the service provider are met effectively.

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

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

- The Company 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. The Company 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.

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

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

10. Outsourced within a Group /Conglomerate

- BCPL 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.

- 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.

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

11. Additional requirements for Cross- Border Outsourcing

- The engagement of a service provider based in a different jurisdiction exposes the the Company to country risk. To manage such risk, the Company shall closely monitor government policies of the jurisdiction in which the service provider is based and the political, social, economic and legal

conditions on a continuous basis, as well as establish sound procedures for mitigating the country risk. This includes, inter alia, having appropriate contingency and exit strategies. Further, it shall be ensured that availability of records to the Company and the RBI will not be affected even in case of liquidation of the service provider.

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

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

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

12. Exit Strategy

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

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

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

The Company shall adopt the following requirements for storage, computing and movement of data in cloud environments:

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

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

- In adoption of cloud services, the Company shall take into account the cloud service specific factors, viz., multi-tenancy, multi-location storing/ processing of data, etc., and attendant risks, while establishing appropriate risk management framework. Cloud security is a shared responsibility between the Company and the Cloud Service Provider (CSP). The Company may refer to some of the cloud security best practices, for implementing necessary controls, as per applicability of the shared responsibility model in the adoption of cloud services.

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

- **Cloud Service Providers (CSP)**
  Considerations for selection of CSP: The Company shall ensure that the selection of the CSP is based on a comprehensive risk assessment of the CSP. BCPL shall enter into a contract only with CSPs subject to

  jurisdictions that uphold enforceability of agreements and the rights available thereunder to the Company, including those relating to aspects such as data storage, data protection and confidentiality.

- **Cloud Services Management and Security Considerations**

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

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

  c. **Security Controls:** BCPL shall ensure that the implementation of security controls in the cloud-based application achieves similar or higher degree of control objectives than those achieved in/ by an on-premise application. This includes ensuring - secure connection through appropriate deployment of network security resources and their configurations; appropriate and

secure configurations, monitoring of the cloud assets utilised by the Company; necessary procedures to authorise changes to cloud applications and related resources.

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

i. CSP maintains an information security policy framework commensurate with its exposures to vulnerabilities and threats;
ii. CSP is able to maintain its information/ cyber security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment;
iii. nature and frequency of testing of controls by the CSP in respect of the outsourced services is commensurate with the materiality of the services being outsourced by the Company and the threat environment; and
iv. CSP has mechanisms in place to assess the sub-contractors with regards to confidentiality, integrity and availability of the data being shared with the sub-contractors, where applicable.

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

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

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

- **Disaster Recovery & Cyber Resilience**

a. The Company's business continuity framework shall ensure that, in the event of a disaster affecting its cloud services or failure of the CSP, the Company can continue its critical operations with minimal disruption of services while ensuring integrity and security.

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

- **The following points may be evaluated while developing an exit strategy**

a. the exit strategy and service level stipulations in the SLA shall factor in, *inter alia*,
i) agreed processes and turnaround times for returning the Company's service collaterals and data held by the CSP;
ii) data completeness and portability;
iii) secure purge of the Company's information from the CSP's environment;

iv) smooth transition of services; and
v) unambiguous definition of liabilities, damages, penalties and indemnities.

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

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

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

- **Audit and Assurance**
  The audit/ periodic review/ third-party certifications should cover, as per applicability and cloud usage, *inter alia*, aspects such as roles and responsibilities of both BCPL 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.

14. Outsourcing of Security Operations Centre (SOC)

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

a. unambiguously identify the owner of assets used in providing the services (systems, software, source code, processes, concepts, etc.);
b. ensure that the Company has adequate oversight and ownership over the rule definition, customisation and related data/ logs, meta-data and analytics (specific to the Company);
c. assess SOC functioning, including all physical facilities involved in service delivery, such as the SOC and areas where client data is stored / processed periodically;
d. integrate the outsourced SOC reporting and escalation process with the RE's incident response process; and
e. review the process of handling of the alerts / events.

15. Services not considered under Outsourcing of IT Services

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

a. Corporate Internet Banking services obtained by the Company as corporate customers/ sub members of another regulated entity
b. External audit such as Vulnerability Assessment/ Penetration Testing (VA/PT),
c. Information Systems Audit, security review
d. SMS gateways (Bulk SMS service providers)
e. Procurement of IT hardware/ appliances

f. Acquisition of IT software/ product/ application (like CBS, database, security solutions, etc.,) on a licence or subscription basis and any enhancements made to such licensed third-party application by its vendor (as upgrades) or on specific change request made by the Company.
g. Any maintenance service (including security patches, bug fixes) for IT Infra or licensed products, provided by the Original Equipment Manufacturer (OEM) themselves, in order to ensure continued usage of the same by the RE.
h. Applications provided by financial sector regulators or institutions like CCIL, NSE, BSE, etc.
i. Platforms provided by entities like Reuters, Bloomberg, SWIFT, etc.
j. 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
k. Services obtained by the Copmpany as a sub-member of a Centralised Payment Systems (CPS) from another Company
l. Business Correspondent (BC) services, payroll processing, statement printing

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

a. Vendors providing business services using IT. Example – BCs
b. 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
c. Partnership based Fintech firms such as those providing co-branded applications, service, products (would be considered under outsourcing of financial services)
d. Services of Fintech firms for data retrieval, data validation and verification services such as (list is not exhaustive):
   i) Bank statement analysis
   ii) GST returns analysis
   iii) Fetching of vehicle information
   iv) Digital document execution
   v) Data entry and Call centre services
e. Telecom Service Providers from whom leased lines or other similar kind of infrastructure are availed and used for transmission of the data
f. 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.

Appendix

Sr. No.	Abbreviation	Full Form
1	BCPL	Blacksoil Capital Private Limited
2	RE	Regulated Entity
3	DMA	Direct Marketing Agent
4	DOC	Document
5	DSA	Direct Sales Agent
6	DSRA	Debt Service Reserve Account
7	ISRA	Information Security Risk Assessment
8	NBFC	Non-Banking Finance Company
9	ND	Non-Deposit taking
10	RBI	Reserve Bank of India

11	SEBI	Securities Exchange Board of India
12	SI	Systemically Important
13	ACB	Audit Committee of the Board
14	FIU	Financial Intelligence Unit
15	TPSP	Third- Party Service Provider
15	BCP	Business Continuity Plan
16	DR	Disaster Recovery
17	DRP	Disaster Recovery Plan
18	SLA	Service-Level Agreement
19	CSP	Cloud Service Provider
20	SOC	Security Operations Centre
21	MSSP	Managed Security Service Provider