BFSL IT Outsourcing Management Policy

(Approved by Board in meeting held on
_____ 2023 Agenda Item No_____)

Policy Name:	Policy for IT Outsourcing Services
Policy Owner	BOB Financial Solutions Limited
Document Version No.	1.0
Document Version Date	31.10.2023
Policy Custodian	IT
Approved By	Board
Effective Date	

SUMMARY:

Version	Prepared by	Description and Reason for Change	Effective Date
1.0	Milind Kadam	As per new RBI guidelines	1-OCT-2023

IT Outsourcing Policy has been prepared by adhering the Circular issued by RBI: **RBI /2023-24 /102 DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 dated: April 10, 2023**
Points covered in the instant Policy adhering the guidelines of the above-mentioned circular, are mentioned below:

Contents

Table of Contents

Introduction:

This policy addresses the assessment and management of risks associated with IT business process outsourcing. Outsourcing involves transferring responsibility for carrying out an activity (previously carried on internally) to an outsourcing provider (also known as an outsourcer) for an agreed charge. Many commercial benefits can be ascribed to outsourcing, including: reducing organizational costs; greater focus on core business by outsourcing non-core functions; access to world-class expertise and resources; and greater ability to address evolving business needs.

Scope/Applicability:

This policy applies to:

- 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) .
- Services and operations related to Data Centres.
- Cloud Computing Services.
- Managed Security Services.
- Management of IT infrastructure and technology services associated with payment system ecosystem.
- FMS

Post Board Approval over this policy BFSL-IT department will follow below steps as per Circular DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 issued by RBI for the purpose of implementing the same for,

1) IT Outsourced contract prior 1-OCT-2023, will have this policy as addendum in agreement/contract.

2) Will be applicable for IT Outsourced Contract post 1-OCT-2023.

3) Also, contract expiring on 1-OCT-2023 will be comply with clause of agreement from date of renewal.

Definitions:

Outsourcing:

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

II. Service Provider: The term "Service Provider" means the provider of IT enabled services. Service Provider includes, but is not limited to, the vendors, agencies, consultants and / or representatives of the third parties.

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

1. Either significantly impact the BFSL's

(a) Business operations, reputation, strategic plans or profitability; or

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

Or

2. In the event of any unauthorised access, loss or theft of customer information may have material impact on the BFSL's customers.

ROLE IN OUTSOURCING OF IT SERVICES- REGULATORY AND SUPERVISORY REQUIREMENTS:

a) The BFSL will 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.

b) Outsourcing of any activity of the BFSL will not diminish its obligations, including its Board and Senior Management, who will be ultimately responsible for the outsourced activity. The BFSL will 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 BFSL if the same activity was not outsourced. Accordingly, the BFSL will not engage an IT service provider that would result in reputation of the BFSL being compromised or weakened.

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

d) The BFSL will ensure that the service provider will neither impede/ interfere with the ability of the BFSL to effectively oversee and manage its activities nor

impede the supervising authority in carrying out the supervisory functions and objectives.

e) The BFSL will ensure that the service provider, if not a group BFSL, will not be owned or controlled by any Director, or Key Managerial Personnel, or approver of the outsourcing arrangement of the BFSL, or their relatives. The terms 'Control', 'Director', 'Key Managerial Personnel', and 'Relative' have the same meaning as assigned under the Companies Act, 2013 and the Rules framed there under 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.

GOVERNANCE FRAMEWORK:

1. IT Governance is not an isolated activity, but instead occurs within the context of the corporate governance of the organization and it is usually the responsibility of the Board and senior executives of the BFSL. It consists of the leadership and organizational structures and processes that ensure that the enterprise's IT sustains and extends its strategies and objectives. The purpose of IT Governance is to direct IT endeavours to ensure that IT's performance meet the following objectives:

- Alignment of IT with the enterprise and realization of the promised benefits;
- Use of IT to enable the enterprise by exploiting opportunities and maximizing benefits;
- Responsible use of IT resources; and
- Appropriate management of IT-related risks;

Thus, conceptualization of IT Outsourcing Governance is to focus on identifying objectives that must be achieved through the outsourcing arrangement.

2. Key factors for IT outsourced vendor selection strategy:

Following are the key factor of effective IT outsourced vendor selection to meet the objectives within the organization's digital transformation agenda and reduce IT costs;

- The IT vendor should have ability to execute the vision/value proposition.
- There should be Effective Cost/Price analysis.
- Financial stability of the vendor.
- Service and support in terms of maintenance hours, response time, resolution time, security, disaster planning, and other service levels from the vendor.
- Range of Services: It is important that the outsourcing vendor is specialized in providing a range of services.
- Value for money: It is important that the outsourcing vendor provides the services at a reasonable price. The quality of services needs to be at par with

the cost that BFSL is paying for them. The services need to bear the value for money.

ROLE OF THE BOARD: The Board shall be responsible, inter alia, for:

- Approving a framework to evaluate the risks and materiality of all existing and prospective IT
- Outsourcing arrangements as also policies that apply to such arrangements;

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

- Setting up suitable administrative framework of Senior Management for the purpose of these directions.

ROLE OF THE SENIOR MANAGEMENT: The Senior Management 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 and in line with the enterprise-wide risk management of the organization approved by the Board and its implementation;
- Prior evaluation of prospective IT outsourcing arrangements and periodic evaluation of the existing Outsourcing arrangements covering 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 on 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;

ROLE OF IT FUNCTION: The responsibilities of the IT Function will, inter alia, include:

- Assisting the Senior Management in identifying, measuring, 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 standard and provide uninterrupted services, and 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

EVALUATION AND ENGAGEMENT OF SERVICE PROVIDERS:

1. In considering or renewing an Outsourced IT Services arrangement, appropriate due diligence will be performed to assess the capability of the service provider to comply with obligations in the outsourcing agreement on an ongoing basis. Due diligence will take into consideration qualitative, quantitative, financial, operational, legal and reputational factors. The BFSL will also consider, while evaluating the capability of the service provider, risks arising from concentration of outsourcing arrangements with a single/ few service provider/s. Where possible, the BFSL will obtain independent reviews and market feedback on the service provider to supplement its own assessment.
2. A risk-based approach will be adopted in conducting such due diligence activities.
3. Due diligence will 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 comply with the regulatory and legal requirements of the Outsourcing of IT Services arrangement.
    h. Security risk assessment, including of the technology assets administered by the service provider.
    i. Ensuring that appropriate controls, assurance requirements and possible contractual arrangements are in place to establish data ownership.
    j. Ability to enforce agreements and the rights available there under including those relating to aspects such as data storage, data protection and confidentiality.

OUTSOURCING SCOPE:

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

a. Effective access by the BFSL to all data, books, records, information, logs, alerts and business premises relevant to the outsourced activity, available with the service provider;
b. Continuous monitoring and assessment of the service provider by the BFSL, so that any necessary corrective measure can be taken immediately; including termination clause and minimum period to execute such provision, if deemed necessary;
c. Type of material adverse events (e.g., data breaches, denial of service, service unavailability etc.) and incident reporting requirements to the BFSL to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines;
d. Compliance with the provisions of IT Act, other applicable legal requirements and standards to protect the customer data;
e. The deliverables, including Service-Level Agreements ("SLAs") formalizing performance criteria to measure the quality and quantity of service levels;
f. Storage of data only in India as per extant regulatory requirements;
g. Clauses requiring the service provider to provide details of data (related to the BFSL and its customers) captured, processed and stored;
h. Controls for maintaining confidentiality of data of the BFSL and its customers', and incorporating service provider's liability towards the BFSL in the event of security breach and leakage of such information;
i. Types of data/ information that the service provider (vendor) is permitted to share with the BFSL's customer and / or any other party;
j. Specifying the resolution process, events of default, indemnities, remedies, and recourse available to the respective parties;
k. Contingency plan(s) to ensure business continuity and testing requirements;

Right To Audit:

a. right to conduct audit of the service provider by the BFSL, 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 BFSL;
b. right to seek information from the service provider about the third parties (in the supply chain) engaged by the former;
c. Recognizing the authority of regulators to perform inspection of the service provider. Adding clauses to allow RBI or person(s) authorized by it to access the BFSL's IT infrastructure, applications, data, documents, and other necessary information given to, stored or

processed by the service provider in relation to the outsourcing arrangement;

d. including clauses making the service provider contractually liable for the performance and risk management practices;
e. obligation of the service provider to comply with directions issued by the RBI in relation to the activities of the BFSL outsourced to the service provider through specific contractual terms and conditions specified by the BFSL.
f. Termination rights of the BFSL, including the ability to orderly transfer the proposed IT- outsourcing arrangement to another service provider, if necessary or desirable.
g. provision to consider resources of service provider who provide core services as "essential personnel" so that a limited number of staff necessary to operate critical functions can work on-site during exigencies (including pandemic situations);
h. clause requiring suitable back-to-back arrangements between service providers and the OEMs;
i. clause requiring non-disclosure agreement with respect to information retained by the service provider; and

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

BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY PLAN:

I. The BFSL will 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.
II. In establishing a viable contingency plan, the BFSL will 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.
III. In order to mitigate the risk of unexpected termination of the outsourcing scope or insolvency/liquidation of the service provider, the BFSL will retain an appropriate level of control over its IT-outsourcing arrangement along with right to intervene, with appropriate measures to continue its business operations.
IV. The BFSL will ensure that service providers are able to isolate the BFSL'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

BFSL can be removed from the possession of the service provider in order to continue its business operations, or deleted, destroyed or rendered unusable.

MONITORING AND CONTROL OF OUTSOURCED ACTIVITIES:

- The BFSL will have in place a management structure to monitor and control its Outsourced IT activities. This will include (as applicable to the scope of Outsourcing of IT Services) but not limited to monitoring the performance, uptime of the systems/ resources, service availability, adherence to SLA requirements, incident response mechanism, etc.
- The BFSL will conduct regular audits (as applicable to the scope of Outsourcing of IT Services) of service providers with regard to the activity outsourced by it. Such audits may be conducted either by BFSL's internal auditors or external auditors appointed to act on BFSL's behalf. Such periodic audits will assess the performance of the service provider, adequacy of the risk management practices adopted by the service provider, compliance with laws/regulations etc. The frequency of the audit will be determined based on the nature and extent of risk and impact to the BFSL from the outsourcing arrangements. Reports on the monitoring and control activities will be reviewed periodically by the Senior Management and in case of any adverse development, the same will be put up to the Board for information.
- In the event of termination of the outsourcing agreement for any reason in cases where the service provider deals with the customers of the BFSL, the same will be given due publicity by the BFSL so as to ensure that the customers stop dealing with the concerned service provider.
- The BFSL will 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 BFSL, their auditors, regulators and other relevant Competent Authorities, as authorized under law.

OUTSOURCING WITHIN A GROUP:

- To meet the business need, if in future, BFSL adopt the following activities to support the business growth, then process will be adopted by adhering the latest RBI Guidelines in this regard

ADDITIONAL REQUIREMENTS FOR CROSS-BORDER OUTSOURCING:

- To meet the business need, if in future, BFSL adopt the following activities to support the business growth, then process will be adopted by adhering the latest RBI Guidelines in this regard

EXIT STRATEGY:

1. An exit strategy is necessary to:
   - identify possible risks;
   - define potential losses; and

- ensure service continuity.

It should be a 'front end' activity i.e. considered when developing your commodity/service strategy. The exit strategy should be included in the procurement documents and contractual terms and conditions where possible. This may appear counterintuitive, but the BFSL need a strategy which is consistent with overall sourcing strategy. Otherwise the risk being locked into an unsatisfactory contract.

If an exit strategy is in place at the start of a supplier relationship, The BFSL's needs should be included in the contract itself. This ensures minimum business and customer disruption if the relationship were terminated. Exit strategies should be reviewed annually, or when significant change occurs.

There are several considerations to be made when developing an exit plan, including:

- Continuing Service Requirements;
- Data Security and Privacy;
- Knowledge and Documentation Transfer;
- Costs; and
- Personnel

Below suggest some factors for consideration in exit strategy. This is not conclusive: each contract / supplier relationship should be considered on its own merits.

a. Continuing Service Requirements:

An exit strategy should set the service requirements when the parties are transitioning out of the relationship. These requirements may include:

- An obligation on the supplier to continue service performance during the transition period.
- During transition these services must stay at the same quality level and continue to comply with all contract obligations.
- The provision of parallel services for a certain period. This term can be extended as necessary to resolve issues before the final changeover.
- A supplier obligation to maintain the same supplier team during the transition period.
- Confidentiality on any communications regarding the termination of the relationship.

b. Data Security and Privacy:

Data privacy and security are critical. The Exit Strategy should consider provision for:

- The vendor should transfer all data belonging to the BFSL, including any customer information;
- An acceptable method for the supplier to destroy and remove the BFSL's proprietary information; and
- The supplier destroying and removing sensitive information from all media. The supplier must ensure no information is disclosed to other individuals or other entities.

c. Knowledge and Documentation Transfer:

Strict documentation and knowledge transfer contract requirements will be advantageous.

Following points need to be considered in this regard:

- Clearly state responsibilities i.e. which party owns the work performed by the supplier and which party is responsible for the transfer of ownership.
- Fully document the service description for any transition period additional services. These are services required from the supplier e.g. employee training, training new supplier personnel.
- Require the supplier to provide the BFSL with copies of information copies of data, procedures, access logs, error logs, documentation and other information generated as a part of providing the contract services. The supplier should also grant the right to provide this information to potential successor suppliers.

d. Costs:

Transition, termination and timing are a key part of the financial aspects of an exit strategy. Be sure the contract:

- Specifies when compensation should be paid and how much. This includes compensation for any continuing base services and transition activities.
- Specifies the return of any pre-paid fees for services which have not been supplied.

e. Personnel:

An exit strategy should cover personnel issues, such as:

- Will not penalize the BFSL for an early exit. This is especially if the termination is due to the supplier's failure to perform the contract.
- Ensuring supplier personnel and key resources remain on the project and committed during the transition. This ensures relevant knowledge and expertise is retained during transition.
- Defining the exit-strategy team and its roles.

2. The BFSL will 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 will be legally obliged to cooperate fully with both the BFSL and new service provider(s) to ensure there is smooth transition and to agree to not to erase, purge, revoke, alter or change any data during the transition period, unless specifically advised by the regulator/ concerned BFSL.

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

STORAGE, COMPUTING AND MOVEMENT OF DATA IN CLOUD ENVIRONMENTS- USAGE OF CLOUD COMPUTING SERVICES:

To meet the business need, if in future, BFSL adopt the following activities to support the business growth, then process will be adopted by adhering the latest RBI Guidelines in this regard.

Disaster recovery & cyber resilience:

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

b) The BFSL will 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 BFSL's service collaterals
and data held by the CSP;

ii) data completeness and portability;

iii) secure purge of BOB Financial Solution Limited 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 BFSL'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 the BFSL 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.

OUTSOURCING OF SECURITY OPERATIONS CENTER ("SOC"):

To meet the business need, if in future, BFSL adopt the following activities to support the business growth, then process will be adopted by adhering the latest RBI Guidelines in this regard

PEREODICAL REVIEW: The instant Policy will be reviewed in 03 (Three) Years and / or basis of the regulatory changes