JANASEVA SAHAKARI BANK LTD., HADAPSAR, PUNE

जनसामान्यांची असामान्य बँक, जनसेवेसाठी वचनबद्ध!

Document ID JNSBL/ITOUTSOU/23-24	Title IT Outsourcing Policy	Print Date 11.01.2024
Version 1.1	Prepared By IT Team	Date of Preparation 10.01.2024
Board Resolution Date 28.05.2024	Date of Review	Next Review Date
Board Resolution Number 3/1/3	Classification Confidential & Internal use only	

Version Control Information:

Version No	Date Issue	Author	Update Information
1.0	10.01.2024	IT Department	First Published Version
1.1	28.05.2024	IT Department	Second Published

Introduction:

As per the RBI Circular **RBI/2023-24/102 DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 April 10, 2023** this policy sets forth the principles, responsibilities, and frameworks that will govern the selection, engagement, and management of third-party IT service providers.

Compliance with Statutory and Regulatory Requirements:

The Bank shall rigorously adhere to and maintain compliance with all pertinent laws, regulations, rules, and directives applicable to IT outsourcing. This includes, but is not limited to, those related to data protection, cybersecurity, customer privacy, and financial reporting. In conducting due diligence and oversight of IT services outsourcing, the Bank will:

Ensure all service providers are vetted for compliance with relevant statutory and regulatory frameworks before engagement and throughout the contract term.

Require service providers to promptly implement any changes in law or regulation into their operations and services.

Conduct regular compliance assessments to verify that outsourcing operations adhere to evolving legal and regulatory landscapes.

Grievance Redressal Mechanism:

In all IT outsourcing agreements, the Bank will ensure that the rights of customers are preserved and that a clear mechanism for grievance redressal is in place. This includes:

Provisions within outsourcing contracts that uphold the customer's right to seek redress in accordance with applicable laws.

The establishment of a transparent process that allows customers to submit complaints regarding services affected by outsourcing.

Regular review and update of grievance procedures to ensure effectiveness and compliance with customer protection laws.

Inventory of Outsourced Services:

The Bank will maintain a comprehensive inventory of all outsourced IT services, which will be reviewed and updated periodically to reflect current engagements. This inventory will:

Include detailed information on all services provided by third parties, as well as key entities in their supply chains.

Map the Bank's dependencies on outsourced services to identify critical functions and assess associated risks.

Establish a process for regular evaluation of service provider performance, ensuring alignment with the Bank's objectives and service standards.

Material Outsourcing:

"Material Outsourcing of IT Services" are those which:

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

b) May have material impact on the Bank customers in the event of any unauthorised access, loss or theft of customer information.

- The level of importance of the c-operative bank of the activity being outsourced as well as the significance of the risk posed by the same.
- The potential impact of the outsourcing on the bank, on various parameters such as earnings, solvency, liquidity, funding's capital and risk profile.
- The likely impact on the bank reputation and brand value and ability to achieve its business objectives, strategy and plans should the service provider fail to perform the service.
- The cost of outsourcing is a proportion of the total operating cost of the bank.
- The aggregate exposure to that particular service provider, in cases where the bank outsources various functions to the same service provider.
- The significance of the activities outsourced in the context of customer service and protection.
- The purpose of the outsourcing is use of external service provider to effectively deliver IT- enabled business process, application service and infrastructure solutions for business outcomes.

Responsibility of Board:

1) Oversight and Accountability

The Board of the Bank shall ensure continuous oversight of IT outsourcing risks and ensure that the management establishes a process for periodic review and evaluation of the outsourcing arrangements to ensure they remain consistent with the goals and objectives of the bank.

2) Due Diligence and Risk Assessment

The Board of the Bank shall ensure that proper due diligence is performed before entering into any outsourcing arrangements and that comprehensive risk assessments are conducted periodically on all outsourcing vendors to safeguard the interests of the bank and its stakeholders.

3) Regulatory Compliance and Reporting

The Board of the Bank shall be responsible for ensuring that all IT outsourcing activities are in compliance with relevant laws, regulations, and guidelines, and that there is a mechanism for regular reporting on the status and compliance of outsourcing arrangements.

4) Vendor Management and Performance Monitoring

The Board of the Bank shall oversee the development and implementation of a vendor management program that includes criteria for selection, performance monitoring, contract management, and contingency planning for all IT outsourcing vendors.

5) Information Security and Confidentiality

The Board of the Bank shall ensure that policies are in place to maintain the confidentiality, integrity, and availability of information processed by outsourcing vendors, and that these policies are in line with industry best practices and standards.

6) Outsourcing Strategy and Objectives

The Board of the Bank shall define the strategic objectives and boundaries for IT outsourcing, ensuring that any outsourcing arrangements align with the overall business strategy and do not compromise the operational control of the Bank.

7) Audit and Control

The Board of the Bank shall ensure that there are appropriate mechanisms for the internal and external audit of IT outsourcing arrangements, and that there are sufficient controls to manage risks associated with these arrangements.

8) Business Continuity and Disaster Recovery

The Board of the Bank shall ensure that the Bank has robust business continuity and disaster recovery plans that include outsourced IT functions, ensuring that these plans are tested regularly and updated as necessary.

Role of Senior Management:

1) Policy Development and Implementation

Senior Management shall be responsible for implementing this IT outsourcing policy that aligns with the Bank's strategic goals and regulatory requirements, and for ensuring that this policy is communicated effectively to all relevant stakeholders.

2) Due Diligence and Service Provider Selection

Senior Management shall conduct thorough due diligence for all potential IT service providers and make decisions based on a comprehensive assessment of the providers' capabilities, reliability, and adherence to industry standards.

3) Contractual Agreements and SLAs

Senior Management shall negotiate and enforce contractual agreements with IT service providers, ensuring that all contracts include detailed service level agreements, confidentiality clauses, and clearly defined performance metrics.

4) Risk Management and Compliance

Senior Management shall establish a risk management process for IT outsourcing that includes regular risk assessments, compliance checks, and alignment with the Bank's risk appetite and regulatory obligations.

5) Information Security and Data Governance

Senior Management shall ensure the protection of sensitive data and the Bank's information assets managed by third-party providers, in compliance with data protection regulations and best practices in cybersecurity.

6) Incident Response and Reporting Procedures

Senior Management shall develop and maintain an incident response plan that includes outsourced IT services, ensuring prompt action and reporting of incidents to relevant authorities and stakeholders.

7) Monitoring and Performance Review

Senior Management shall set up a continuous monitoring program to assess the performance of IT service providers against contractual SLAs and to implement corrective measures as needed.

8) Regulatory Adherence and Liaison

Senior Management shall maintain a clear understanding of the regulatory landscape related to IT outsourcing and act as the primary liaison with regulatory bodies for all matters concerning outsourcing.

9) Transition Management and Exit Strategies

Senior Management shall ensure that there are effective transition management processes and exit strategies in place for all IT outsourcing agreements to mitigate risks associated with contract termination or provider switch.

10) Capacity and Resource Management

Senior Management shall provide adequate internal resources and capabilities to manage the outsourcing relationships effectively, including specialized staff for oversight and management of outsourced functions.

Role of IT Functions:

1) Risk Management Support

The IT Function of the bank shall assist Senior Management in the continuous process of identifying, measuring, monitoring, mitigating, and managing the levels of IT outsourcing risk, ensuring alignment with the bank's overall risk management strategy.

2) Outsourcing Arrangements Database

The IT Function of the bank shall maintain a centralized, up-to-date database of all IT outsourcing arrangements. This database will be accessible to the Board, Senior Management, Auditors, and Supervisors to facilitate oversight and review.

3) Performance Monitoring and Reporting

The IT Function of the bank shall rigorously monitor and supervise outsourced IT activities to As per established performance standards and service continuity. It shall regularly report performance outcomes and any concerns to Senior Management and coordinate periodic due diligence exercises.

4) Documentation and Compliance

The IT Function of the bank shall be responsible for developing and managing all necessary documentation for IT outsourcing contracts, including defining service level agreements, ongoing monitoring of vendor operations, and maintaining key risk indicators. It will also classify vendors according to assessed risks and As per all contractual obligations.

5) Vendor Relationship Management

The IT Function of the bank shall oversee the relationships with IT service providers, ensuring that vendors meet contractual obligations and service level agreements, and act as the liaison between the service providers and the bank for all contractual matters.

6) Regulatory Compliance and Audit Readiness

The IT Function of the bank shall ensure that IT outsourcing activities comply with applicable regulatory requirements and are prepared for internal and external audits, facilitating any necessary information requests or audit processes.

7) Strategic Alignment

The IT Function of the bank shall align IT outsourcing initiatives with the bank's strategic objectives, ensuring that outsourced activities support the bank's long-term goals and service delivery expectations.

8) Incident and Change Management

The IT Function of the bank shall implement and manage an incident response and change management process for outsourced IT functions, ensuring rapid response to incidents and smooth transition for any changes in service provision.

9) Knowledge Management

The IT Function of the bank shall ensure knowledge transfer and maintain documentation regarding outsourced IT functions, so that the bank retains critical knowledge and is not overly dependent on external providers.

10) Innovation and Continuous Improvement

The IT Function of the bank shall encourage and work with IT service providers to foster innovation and continuous improvement in service delivery that can provide competitive advantages to the bank.

Other clauses:

1) Management Oversight

Banks must establish a robust management structure to oversee outsourced IT functions, ensuring performance metrics, system uptime, service availability, adherence to service level agreements (SLAs), and an effective incident response mechanism are in place and operational.

2) Audit Procedures

Banks are required to perform regular and thorough audits of all IT service providers, including subcontractors, to evaluate the quality and security of the outsourced activities. These audits may be carried out by the bank's internal audit team or by external auditors appointed for this purpose.

3) Collaborative Audits

When multiple banks outsource IT services to the same provider, they may opt for pooled audits to streamline the process. Each bank, however, retains the responsibility to ensure that audits meet their individual contractual needs and regulatory obligations.

4) Performance and Compliance Auditing

The audit process must evaluate the service provider's performance, risk management practices, and legal compliance. The frequency of audits will be contingent upon the associated risks and the potential impact on the bank. Findings from these audits will be reviewed by Senior Management and escalated to the Board as necessary.

5) Third-Party Certifications

Banks may consider third-party certifications when assessing service providers' controls, but this does not diminish the bank's obligation to independently verify that data security and system availability meet the bank's stringent requirements.

6) Financial and Operational Review

Banks shall periodically assess the financial stability and operational competence of their IT service providers to ensure ongoing compliance with outsourcing obligations. These risk-based evaluations will identify any decline in service standards or breaches in confidentiality, security, and operational resilience.

7) Access to Information

Banks must ensure they, and their auditors, have unfettered access to all data related to outsourced activities and can visit service provider sites, in accordance with appropriate security protocols, for effective oversight as permitted by law.

8) Outsourcing Strategy and Policy Review

Banks shall review and update their IT outsourcing strategy and policy periodically to reflect changes in the bank's strategic direction, technological advancements, and evolving industry standards.

9) Service Provider Relationship Management

Banks shall establish clear procedures for managing relationships with IT service providers, including regular communication, performance reviews, and contract renegotiation protocols.

10) Incident and Problem Management

Banks shall define and implement clear processes for incident and problem management related to outsource IT services, ensuring swift resolution and minimal impact on bank operations and clients.

Exit Strategy:

1) Exit Triggers: The strategy will be activated under various conditions, including contractual term completion, mutual agreement for early termination, service provider default, or bank's strategic realignment.

2) Notice Period: A clearly defined notice period will be mandated to initiate the exit process, allowing for an orderly transition without service disruption.

3) Transition Planning: Detailed transition plans will specify the procedural steps, resource allocation, and timelines to ensure service continuity.

4) Alternative Arrangements: The bank will identify and qualify alternative service providers or in-house capabilities to assume the outsourced IT functions when necessary.

5) Stakeholder Communication: A communication plan will be executed to inform all stakeholders, including customers and employees, about changes in service provision.

Based on the image provided, here are clauses that could be included in an IT Outsourcing Policy for a bank's Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP):

Business Continuity Plan and Disaster Recovery Plan:

1) BCP/DRP Development and Testing

Service providers engaged in IT outsourcing must develop, maintain, and routinely test a comprehensive BCP and DRP in alignment with the bank's risk profile and the scale of outsourced operations. These plans must adhere to the regulatory guidelines set forth by the Reserve Bank of India (RBI), with updates to reflect any changes in the RBI's instructions on BCP/DRP requirements.

2) Contingency Planning

The bank shall ensure the establishment of a viable contingency plan that considers the rapid engagement of alternative service providers or the reintegration of outsourced activities in-house during a crisis. The plan will detail the associated costs, timelines, and resource allocations necessary for such a transition.

3) Information and Asset Isolation

IT service providers must demonstrate their capability to segregate and safeguard the bank's information, documents, and records effectively. In the event of adverse conditions, service termination, or contract dissolution, the bank must ensure mechanisms are in place to retrieve or secure all such information. Providers must ensure that the bank's data and documents can be expeditiously removed from their systems, or be permanently deleted, destroyed, or rendered unusable, to protect the bank's interests.

4) Audit and Compliance

Regular audits will be conducted to verify the adequacy and effectiveness of the service provider's BCP and DRP. Compliance with the bank's policy and RBI guidelines will be assessed, and discrepancies will be addressed promptly to ensure no lapse in continuity capabilities.

5) Training and Awareness

The bank will provide ongoing training and awareness programs for relevant staff to ensure they are prepared to execute the BCP and DRP effectively. This includes familiarizing them with the procedures for activating contingency plans and transitioning activities either to an alternate provider or back in-house.

6) Review and Update Cycle

The BCP and DRP will be reviewed and updated on a regular basis, or when significant changes in the bank's operations or IT outsourcing arrangements occur. This ensures that the plans remain current with the evolving nature of threats and the regulatory environment.

Risk Management Framework:

A) Framework Establishment

The bank shall implement a Risk Management Framework specifically designed for the Outsourcing of IT Services to the Service Provider. This framework will detail the processes for identifying, measuring, mitigating, managing, and reporting the risks associated with outsourcing IT service arrangements.

B) Documentation and Approvals

All risk assessments conducted by the bank must be thoroughly documented, requiring formal approvals in accordance with the governance structure involving the Board of Directors, Senior Management, and IT Department. These documents are to be reviewed for quality on a schedule set by a policy approved by the Board.

C) Data Confidentiality and Integrity

The bank will uphold the confidentiality and integrity of customer data and information that the Service Provider has access to. Procedures will be in place to ensure that all data shared with the Service Provider is handled in a secure manner.

D) Controlled Data Access

The Service Provider's access to the bank's data will be strictly regulated, ensuring that any access to sensitive data is granted on a need-to-know basis with appropriate controls to avoid any unauthorized use or data breaches.

E) Trust and Public Confidence

The bank will take necessary actions to maintain public confidence and customer trust by ensuring that the Service Provider maintains the security and confidentiality of customer information at all times. Staff of the Service Provider will be granted access to customer information exclusively on a need-to-know basis.

F) Multi-vendor Environment Management

In situations involving multiple service providers, the bank retains the obligation to oversee and monitor the control environment across all entities that handle the bank's data, systems, records, or resources.

G) Safeguards against Information Merging

The bank will enforce stringent safeguards to prevent the combination or merging of information, documents, records, and assets when the Service Provider is also working with multiple banks.

H) Control Process Monitoring

The bank will consistently monitor the control processes and security practices of the Service Provider. In case of any security breach or leak of confidential customer information, the bank will immediately inform the regulatory body, RBI, and follow the prescribed incident response and recovery procedures.

I) Concentration Risk Evaluation

The bank will assess the concentration risk that could arise from relying on the same Service Provider for multiple outsourced services or when critical functions are outsourced to a limited number of service providers.

J) Review

This Policy for IT Outsourcing will be review and update annually or as needed based on any changes in technology, regulations, or business practices.

Chief Manager IT

Dy. General Manager IT

General Manager

Chief Executive Officer

28.05.24

Chairman
Executive Committee

Chairman
BOD

संचालक मंडळ
विषय क्र. 3
ठराव क्र. 3/1/3/1
दिनांक 28/5/2024 ने मंजूर