

OUTSOURCING POLICY

OF



Version Number 1.0

Dated 01st May, 2010



<u>Table of contents</u>	<u>Page No.</u>
Introduction	2
Activities that are proposed to be outsourced by the Bank	4
Activities that are already outsourced by the Bank	4
Activities that should not be outsourced	5
Material Outsourcing	5
Bank's role and Regulatory and Supervisory requirements	6
Risk Management practices for outsourced Financial Services	7
Need for an Outsourcing Policy	7
Role of Board and Senior Management	7
Evaluation of the Risks	8
Evaluating the Capability of the Service Provider	9
The Outsourcing Agreement	9
Confidentiality and Security	11
Responsibilities of DSA/DMA/Recovery Agents	11
Business Continuity and Management of Disaster Recovery Plan	12
Monitoring and Control of Outsourced Activities	13
Redressal of Grievances related to Outsourced services	13
Reporting of Transactions to FIU or other competent authorities	14
Centralized list of Outsourced Agents	14
Off-shore outsourcing of Financial Services	14
Outsourcing within a Group/Conglomerate	15
Self Assessment of Existing/Proposed Outsourcing Arrangements	15
Review of the Policy	15
List of Abbreviations	16



1. Introduction.

1.1 The world over, banks are increasingly using outsourcing as a means of both reducing cost and accessing specialist expertise, not available internally and achieving strategic aims. 'Outsourcing' may be defined as a bank's 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 (including agreements for a limited period), that would normally be undertaken by the bank itself, now or in the future.

In keeping with this international trend, banks in India too have been extensively outsourcing various activities. Such outsourcing activities results in banks being exposed to various risks. Further, the outsourcing activities are to be brought within regulatory purview and the interests of the customers have to be protected.

It is against this background, that Reserve Bank of India has put in place a set of guidelines to address the risks that a bank would be exposed to in lieu of growing outsourcing activity and to ensure that the bank concerned and Reserve Bank of India have access to all books, records and information available with the service provider. The guidelines also cover issues relating to safeguarding of customer interests. These guidelines are concerned with managing risks in outsourcing of financial services and are not applicable to technology related issues and activities not related to banking services like usage of courier, catering of staff, housekeeping and janitorial services, security of the premises, movement and archiving of records etc. Moreover, audit-related assignments to Chartered Accountant firms will continue to be governed by the instructions/policy as laid down by the Department of Banking Supervision of RBI. Based on these guidelines this policy is formulated.

Typically, outsourced financial services include application processing (loan origination, credit card), document processing, marketing and

research, supervision of loans, data processing and back office related activities. These activities may include;

- i) Opening, settlement and closing of accounts.
- ii) Issue and processing of Cheques
- iii) Managing of Customer queries (Call Centers)
- iv) Recruitment, Selection and Training of Personnel.
- v) Administration of Payroll and Taxation
- vi) Marketing of bank products
- vii) Maintaining of Computer and other electronic gadgets
- viii) Cross Selling of Bank Products like Insurance and Mutual Funds
- ix) Credit Card and Debit Card customer acquisition / queries
- x) Maintenance of ATMs.

1.2 The Joint Forum, a tripartite body comprising Basel Committee on Banking Supervision, International Organization of Securities Commission and International Association of Insurance Supervisors, had issued guidelines on outsourcing in financial services in February, 2005. Internationally, several countries like USA, UK, Germany, Hong Kong, Australia and Singapore, have put in place, guidelines on outsourcing in financial services. Based on these international best practices, Reserve Bank of India has issued certain guidelines for outsourcing in financial services.

1.3 Outsourcing brings in its wake, several risks like Strategic Risk, Reputation Risk, Compliance Risk, Operational Risk, Legal Risk, Exit Strategy Risk, Counter party Risk, Country Risk, Contractual Risk, Access 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 either the service provider or the outsourcing bank, can lead to financial losses or loss of reputation for the bank and could also lead to systemic risks within the entire banking system in the country. It would therefore be imperative for the bank outsourcing its activities to ensure effective management of these risks.

1.4 The guidelines on managing risks in outsourcing are intended to provide direction and guidance to banks which choose to outsource financial services to adopt sound and responsive risk management practices for effective oversight, due diligence and management of risks arising from such outsourcing activities. The guidelines are applicable to outsourcing arrangements entered into by a bank with a service provider located in India or elsewhere. The service provider may either be a member of the group/conglomerate to which the bank belongs, or an unrelated party.

1.5 The underlying principles behind these guidelines are that the bank should ensure that outsourcing arrangements neither diminish its ability to fulfill its obligations to customers and RBI nor impede effective supervision by RBI. Banks, therefore, have to take steps to ensure that the service provider employs the same high standard of care in performing the services as would be employed by the bank, if the activities were conducted within the bank and not outsourced. Accordingly, banks should not engage in outsourcing that would result in their internal control, business conduct or reputation, being compromised or weakened.

1.6 Banks which desire to outsource financial services do not require prior approval from RBI whether the service provider is located in India or outside India.

1.A. Activities that are proposed to be outsourced by the Bank.

The financial services proposed to be outsourced by our bank include making small value cash transactions (for Social Security benefit payments, NREGA payments, utility bill collections), application processing (deposits as well as loans) through BCs using biometric enabled smart cards, data processing and back office related activities etc.

1.B. Activities that are already outsourced by the Bank.

The following activities are already outsourced by the Bank.

<u>Department</u>	<u>Outsourcing Activities</u>
CIAD	<ul style="list-style-type: none">* Credit Card Back -end operations and Authorization Switch Maintenance• Merchant Acquiring, Back-End Operations and Authorization Switch Maintenance• Credit Card, ACS (Access Control Server) Operations for 3DSecure• Credit Card and Debit Card, Personalization, Encoding, PIN generation
T&ISD	<ul style="list-style-type: none">* SMS alert Server Back End Operations• Providing bandwidth services for the bank.• Disaster Recovery Site Hosting and co location services.

- Branch/ Office Computer Hardware and peripherals maintenance.
- ATM hardware maintenance and support.

The Bank has bought various softwares like Finacle (vendor Infosys) for core banking, e-Funds ATM Switch (vendor e-Funds) for ATMs, DpSecure (vendor CMC Limited) for Depository, Finacle e-Channels (vendor Infosys) for e-Banking, Amlock (vendor 3i Infotech) for KYC / AML, ITMS (vendor Lasersoft) for Treasury Operations, CTS (vendor NCR) for Cheque Truncation, OFSA (vendor Oracle) for TP/PA/RM, People Soft (vendor Oracle) for HRM. The bank has purchased licenses for all these applications. However, the Annual Maintenance Contract for both the bought software and hardware is generally carried out by vendors. All RBI supplied softwares like RTGS family, NDS family etc. are supported by RBI or RBI entities. These softwares and hardwares are however used/operated by Bank.

2 Activities that should not be outsourced.

As per RBI guidelines banks which choose to outsource financial services should however not outsource core management functions including Internal Audit, Compliance Function and decision-making functions like determining compliance with KYC norms for opening deposit accounts, according sanction for loans (including retail loans) and management of investment portfolio.

3 Material Outsourcing.

During Annual Financial Inspections (AFI), RBI will review the implementation of these guidelines to assess the quality of related risk management systems, particularly in respect of material outsourcing. Material outsourcing arrangements are those, which if disrupted, have the potential to significantly impact the business operations, reputation or profitability. Materiality of outsourcing would be based on:

- The level of importance to the bank, of the activity being outsourced.
- The potential impact of the outsourcing on the bank, on various parameters such as, earnings, solvency, liquidity, funding capital and risk profile.
- The likely impact on the bank's 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 the outsourcing as a proportion of total operating costs of the bank.
- The aggregate exposure to that particular service provider, in case where the bank outsource various functions to the same service provider.

4 Bank's role and Regulatory and Supervisory requirements (As per RBI guidelines).

4.1 The outsourcing of any activity by bank does not diminish its obligations, and those of its Board and Senior Management, who have the ultimate responsibility for the outsourced activity. The bank would therefore be responsible for the actions of their service provider including Direct Sales Agents/Direct Marketing Agents and Recovery Agents and the confidentiality of information pertaining to the customers that is available with the service provider. The bank should retain ultimate control of the outsourced activity.

4.2 It is imperative for the bank, when performing its due diligence in relation to outsourcing, to consider all relevant laws, regulations, guidelines and conditions of approval, licensing or registration.

4.3 Outsourcing arrangements should not affect the rights of a customer against the bank, including the ability of the customer to obtain redress as applicable under relevant laws. Since the customers are required to deal with the service providers in the process of dealing with the bank, the bank should incorporate a clause in the product literature/brochures etc., stating that they may use the services of agents in sales/marketing etc. of the products. The role of agents may be indicated in broad terms.

4.4 Outsourcing, whether the service provider is located in India or abroad, should not impede or interfere with the ability of the bank to effectively oversee and manage its activities nor should it impede the Reserve Bank of India in carrying out its supervisory functions and objectives.

4.5 Banks need to have a robust grievance redressal mechanism, which in no way should be compromised on account of outsourcing.

4.6 The service provider, if it is not a subsidiary of the bank, should not be owned or controlled by any director or officer/employee of the bank or their relatives having the same meaning as assigned under Section 6 of the Companies Act, 1956.

5 Risk Management practices for outsourced Financial Services.

5.1 Need for an Outsourcing Policy.

A bank intending to outsource any of its financial activities should 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, parameters for defining material outsourcing based on the broad criteria indicated in **Para 3**, delegation of authority depending on risks and materiality and systems to monitor and review the operations of these activities.

5.2 Role of the Board and Senior Management.

5.2.1. The Board of the Bank, or a Committee of the Board to which powers have been delegated should be responsible, *inter alia*, for:-

- Approving a framework to evaluate the risks and materiality of all existing and prospective outsourcing and the policies that apply to such arrangements.
- Laying down appropriate approval authorities for outsourcing depending on risks and materiality.
- Undertaking regular review of outsourcing strategies and arrangements for their continued relevance, and safety and soundness, and
- Deciding on business activities of a material nature to be outsourced, and approving such arrangements.

5.2.2 The Senior Management of the Bank would be responsible for:-

- 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.
- 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, 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.

5.3 Evaluation of the Risks.

The key risks in outsourcing that need to be evaluated by the bank are:-

- Strategic Risk** - The service provider may conduct business on its behalf, which is inconsistent with the overall strategic goals of the bank.
- Reputation Risk** - Poor service from the service provider, its customer interaction not being consistent with the overall standards of the bank.
- Compliance Risk** - Privacy, consumer and prudential laws not adequately complied with.
- Operational Risk** - Arising due to technology failure, fraud, error, inadequate financial capacity to fulfill obligations and/or provide remedies.
- Legal Risk** – includes, but is not limited to, exposure 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** - This could arise from over-reliance on one firm, the loss of relevant skills in the bank itself preventing it from bringing the activity back in-house and contracts entered into wherein speedy exits would be prohibitively expensive.
- Counter party Risk** - Due to inappropriate underwriting or credit assessments.
- Country Risk** - Due to political, social or legal climate creating added risk.
- Contractual Risk** - arising from whether or not the bank has the ability to enforce the contract.

- j) **Concentration and Systemic Risk** - Due to lack of control of individual banks over a service provider, more so when overall banking industry has considerable exposure to one service provider.

5.4 Evaluating the Capability of the Service Provider.

5.4.1. In considering or renewing an outsourcing arrangement, appropriate due diligence should be performed to assess the capability of the service provider to comply with the obligations in the outsourcing agreement. Due diligence should take into consideration qualitative and quantitative, financial, operational and reputational factors. Bank should 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. Bank should also consider, while evaluating the capability of the service provider, issues relating to undue concentration of outsourcing arrangements with a single service provider. Wherever possible, the bank should obtain independent reviews and market feedback on the service provider to supplement its own findings.

5.4.2. Due Diligence should involve an evaluation of all available information about the service provider, including but not limited to:-

- Past experience and competence to implement and support the proposed activity over the contract period.
- Financial soundness and ability to service commitments even under adverse conditions.
- Business reputation and culture, compliance, complaints and outstanding or potential litigation.
- Security and internal control, audit coverage, reporting and monitoring environment, business continuity management.
- External factors like political, economic, social and legal environment of the jurisdiction in which the service provider operates and other events that may impact service performance.
- Ensuring due diligence by service provider of its employees.

5.5. The Outsourcing Agreement.

5.5.1. The terms and conditions governing the contract between the bank and the service provider should be carefully defined in written agreements and vetted by bank's legal counsel on their legal effect and

enforceability. Every such agreement should address the risks and risk mitigation strategies. The agreement should be sufficiently flexible to allow the bank 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 should also bring out the nature of legal relationship between the parties i.e. whether agent, principal or otherwise. Some of the key provisions of the contract would be:

- The contract should clearly define what activities are going to be outsourced, including appropriate service and performance standards.
- The bank must ensure that it has the ability to access all books, records and information relevant to the outsourced activity available with the service provider.
- The contract should provide for continuous monitoring and assessment by the bank of the service provider, so that any necessary corrective measure can be taken immediately.
- A termination clause and minimum periods to execute a termination provision, if deemed necessary, should 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.
- Contingency plans to ensure business continuity.
- The contract should;
 - Provide for the prior approval/consent by the bank of the use of sub-contractors by the service provider for all or part of an outsourced activity.
 - Provide the bank 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 bank.
- Outsourcing agreements should include clauses to allow the Reserve Bank of India or persons authorized by it to access the bank's documents, records of transactions, and other necessary information given to, stored or processed by the service provider, within a reasonable time.
- Outsourcing agreement should also include clause to recognize the right of the Reserve Bank to cause an inspection to be made of a service provider of a bank and its books and account by one or more of its officers or employees or other persons.

- The outsourcing agreement should also provide that the confidentiality of customer's information should be maintained even after the contract expires or gets terminated.
- The outsourcing agreement should provide for the preservation of documents and data by the service provider in accordance with the legal/regulatory obligation of the bank in this regard.

5.6. Confidentiality and Security.

5.6.1. Public confidence and customer trust in the bank is a prerequisite for the stability and reputation of the bank. Hence the bank should seek to ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the service provider.

5.6.2. Access to customer information by staff of the service provider should be on 'need to know' basis, i.e. limited to those areas where the information is required in order to perform the outsourced function.

5.6.3. The bank should ensure that the service provider is able to isolate and clearly identify the bank'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 banks, care should be taken to build strong safeguards so that there is no commingling of information/documents, records and assets.

5.6.4. The bank should review and monitor the security practices and control processes of the service provider on a regular basis and require the service provider to disclose security breaches.

5.6.5. The bank should immediately notify RBI in the event of any breach of security and leakage of confidential customer related information. In these eventualities, the bank would be liable to its customers for any damage.

5.7. Responsibilities of DSA/DMA/Recovery Agents.

5.7.1. Code of conduct for Direct Sales Agents formulated by the Indian Banks' Association (IBA) could be used in formulating the bank's own codes for Direct Sales Agents/Direct Marketing Agents/Recovery Agents. The Bank shall ensure that the Direct Sales Agents/Direct Marketing Agents/Recovery Agents are properly trained to handle with care and sensitivity, their responsibilities, particularly aspects like soliciting customers, hours of calling, privacy of customer information and conveying the correct terms and conditions of the products on offer etc.

5.7.2. Recovery Agents should adhere to extant instructions on Fair Practice Code for lending (Circular DBOD.Leg.No.BC.104/09.07.007/2002-03 dated 5th May 2003) as also bank's own code for collection of dues. It is essential that the Recovery Agents refrain from action that could damage the integrity and reputation of the bank and that they observe strict customer confidentiality.

5.7.3. The bank and its 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, making threatening and anonymous calls or making false and misleading representations.

5.8. Business Continuity and Management of Disaster Recovery Plan.

5.8.1. The bank should require its service providers to develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures. Bank needs to ensure that the service provider periodically tests the business continuity and recovery plan and may also consider occasional joint testing and recovery exercises with the service provider.

5.8.2. In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, bank shall retain an appropriate level of control over the 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 bank and its services to the customers.

5.8.3. In establishing a viable contingency plan, the bank 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.

5.8.4. Outsourcing often leads to the sharing of facilities operated by the service provider. The bank shall ensure that service providers are able to isolate the bank's information, documents, records and other assets. This is to ensure that in adverse conditions, all documents, records of transactions and information given to the service provider, and assets of the bank, can be removed from the possession of the service provider in order to continue its business operations, or

deleted, destroyed or rendered unusable.

5.9. Monitoring and Control of Outsourced Activities.

5.9.1. The bank 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.

5.9.2. A central record of all material outsourcing that is readily accessible for review by the Board and senior management of the bank shall be maintained. The records shall be updated promptly and half yearly reviews shall be placed before the Board by the respective departments / divisions.

5.9.3. Regular audits by either the internal auditors or external auditors of the bank shall assess the adequacy of the risk management practices adopted in overseeing and managing the outsourcing arrangement, the bank's compliance with its risk management framework and the requirements of these guidelines.

5.9.4. The bank 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 should highlight any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness.

5.9.5. In the event of termination of the agreement for any reason, this shall be publicized so as to ensure that the customers do not continue to entertain the service provider.

5.10. Redressal of Grievances related to Outsourced services.

a) The Grievance Redressal Machinery of the bank shall be widely publicized through electronic and print media. The name and contact number of designated grievance redressal officer of the bank shall be made known and widely published. The designated officer shall ensure that genuine grievances of customers are redressed promptly without involving delay. It shall be clearly indicated that bank's Grievance Redressal Machinery will also deal with the issue relating to services provided by the outsourced agency.

b) Generally, a time limit of 30 days may be given to the customers

for preferring their complaints/grievances. The grievance redressal procedure of the bank and the time frame fixed for responding to the complaints shall be placed on the bank's website.

c) If a complainant does not get satisfactory response from the bank within 60 days from the date of lodging, the complainant will have the option to approach the office of the concerned Banking Ombudsman for redressal of his/her grievance/s.

5.11. Reporting of transactions to FIU or other competent authorities.

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

6. Centralized List of Outsourced Agents.

If a service provider's services are terminated by the bank, IBA will be informed with reasons for termination. IBA would be maintaining a caution list of such service providers for the entire banking industry for sharing among banks.

7. Off-shore outsourcing of Financial Services.

7.1. The engagement of service providers in a foreign country exposes a bank to country risk - economic, social and political conditions and events in a foreign country that may adversely affect the bank. Such conditions and events could prevent the service provider from carrying out the terms of its agreement with the bank. To manage the country risk involved in such outsourcing activities, the bank shall take into account and closely monitor government policies and political, social, economic and legal conditions in countries where the service provider is based, 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.

7.2. 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 the bank in a timely manner.

7.3. The outsourcing related to overseas operations of Indian banks

would be governed by both these guidelines and the host country guidelines. Where there are differences, the more stringent of the two would prevail. However, where there is any conflict, the host country guidelines would prevail.

8. Outsourcing within a Group/Conglomerate.

The risk management practices expected to be adopted by a bank while outsourcing to a related party (ie. party within the Group/Conglomerate) would be identical to those specified in **Para 5** of this guidelines.

9. Self Assessment of Existing/Proposed Outsourcing Arrangements.

The bank shall conduct a self-assessment of its existing outsourcing agreements within a time bound plan and bring them in line with these guidelines expeditiously.

10. Review of the Policy.

The policy will be reviewed at yearly intervals or as and when considered necessary by the Board of Directors of the Bank.

List of Abbreviations

AML	Anti Money Laundering
ATM	Automated Teller Machine
BC	Business Correspondent
CBS	Core Banking Solution
CIAD	Card Issuance & Acquiring Department
CTS	Cheque Truncation System
DMA	Direct Marketing Agent
DSA	Direct Sales Agent
FIU	Financial Intelligence Unit
IBA	Indian Banks' Association
ITMS	Integrated Treasury Management Solution
KYC	Know Your Customer
NDS	Negotiated Dealing System
NREGA	National Rural Employment Guarantee Act
OFSA	Oracle Financial Services Applications
PA	Performance Analyzer
RBI	Reserve Bank of India
RM	Risk Manager
RTGS	Real Time Gross Settlement
T&ISD	Technology & Information Systems Division
TP	Transfer Pricing