## Chapter 4 – IT Services Outsourcing

### *Introduction*

In India, as banks augment growth and expand business, there is an increasing reliance on external service providers as partners in achieving the growth targets and as effective cost alternatives.

'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 that would normally be undertaken by the bank itself, now or in the future. 'Continuing basis' includes agreements for a limited period.

The benefits of outsourcing include efficiencies in operations, increased ability to acquire and support current technology and tide over the risk of obsolescence, increased time availability for management to focus on key management functions, shorter lead time in delivering services to customers, better quality of services, and stronger controls among others.

### *Common areas for Outsourcing*

Outsourcing has been a constant theme in banking technology over at least the past ten years, as banking has become more technology intensive and the required scale of investment has grown exponentially. Many operations have been outsourced to Third party vendors comprising external vendors and specialized subsidiaries. Service providers today may be a technology company or specialist outsourcing manager. This decision to outsource should fit into the institution's overall strategic plan and corporate objectives.

Common areas where Banks have outsourced functions include:

- Technology Operations
    - Technology Infrastructure Management, Maintenance and Support
    - Application Development, Maintenance and Testing
- Banking Operations
    - Sourcing, Leads Generation
    - Cash Management and Collections
    - Customer Service helpdesk / call center services
    - Transaction Processing including payments, loans, deposits
    - Activities such as Debit card printing and dispatch, verifications, etc.
- Marketing and Research
- Fiduciary and Trading activities

### *Role of the Board and Senior Management*

The Board and senior management are ultimately responsible for 'outsourcing operations' and for managing risks inherent in such outsourcing relationships. Whereas an institution may delegate its day-to-day operational duties to a service provider, responsibilities for effective due diligence, oversight and management of outsourcing and accountability for all outsourcing decisions continue to rest with the Bank, Board and senior management. Board and senior management have the responsibility to institute an effective governance mechanism and risk management process for all outsourced operations.

The Board is responsible for:

- Instituting an appropriate governance mechanism for outsourced processes, comprising of risk based policies and procedures, to effectively identify, measure, monitor and control risks associated with outsourcing in an end to end manner
- Defining approval authorities for outsourcing depending on nature of risks in and materiality of outsourcing
- Assessing management competencies to develop sound and responsive outsourcing risk management policies and procedures commensurate with the nature, scope, and complexity of outsourcing arrangements
- Undertaking a periodic review of outsourcing strategies and all existing material outsourcing arrangements

Senior management is responsible for:

- Evaluating the risks and materiality of all prospective outsourcing based on the framework developed by the Board
- Developing sound outsourcing policies and procedures for implementation by Line Managers
- Periodically reviewing the effectiveness of policies and procedures
- Communicating significant risks in outsourcing to the Board on a periodic basis
- Ensuring an independent review and audit in accordance with approved policies and procedures
- Ensuring contingency plans have been developed and tested adequately

***Various components/aspects relating to outsourcing:***

**1. 'Material' Outsourcing**

Banks need to assess the degree of 'materiality' inherent in the outsourced functions. Whether an outsourcing arrangement is 'material' to the business context or not is a qualitative judgment and may be determined on the basis criticality of service, process, or technology to the overall business objectives.

Outsourcing of non-financial processes, such as technology operations, is 'material' and if disrupted has the potential to significantly impact business operations, reputation and stability of the Bank. Where a Bank relies on third party employees to perform key banking functions such as applications processing, verifications, approvals, etc.,on a continuous basis, such outsourcing may also be construed as 'material', whether or not the personnel are located within the premises of the Bank. However, extant RBI guidelines on outsourcing indicate activities which cannot be outsourced and need to be carried out by the bank. These include Internal Audit, Compliance function, and decision making functions like KYC compliance, loans sanctioning, and managing investment portfolio. These need to be kept in view.

Criteria that may be considered in determining the materiality of proposed outsourcing include the following:

- Size and scale of operations which are outsourced
- Potential impact of outsourcing on parameters such as cost of outsourcing as a proportion of total operating costs, earnings, liquidity, solvency, funding capital, risk profile, among others, for the Bank
- Nature of functions outsourced
- Nature and extent of data sharing involved. For e.g., where outsourcing involves sharing of customer data, the engagement may be 'material'

- Degree/extent of control and oversight exercised by the bank on vendor managed processes. For e.g., the ability of bank staff to design and influence day to day operations and decision making, whether bank staff is able to exercise sufficient oversight over the day to day activities performed by outsourced agencies
- Degree of control exercised by banks on outsourced entities, regardless of a conglomerate entity structure
- Impact on data privacy and security. For e.g., whether access to customer data has to be extended to staff of the service provider
- Whether the bank has adequate flexibility to switch service providers, so that the risk of being attached to a single service provider is adequately mitigated, and the aggregate exposure to a single service provider

Banks should undertake a periodic review of their outsourced processes to identify new outsourcing risks as they arise. For e.g. when the service provider has further sub-contracted work to other service providers or has undergone a significant change in processes, infrastructure, or management.

Materiality should be considered both at an institution level and on a consolidated basis i.e. together with the institution's branches and corporations/entities under its control.

### 2. Risk Management in outsourcing arrangements

Risk management is the process of identifying, measuring, monitoring and managing risk. Risks inherent to process outsourcing, include Strategic risk, Reputation risk, Operational risk, Compliance risk, Legal risk, Counter party risk, Country risk, Contractual risk, Access risk, Concentration and systemic risk, and Exit strategy risk. Failure of a service provider in providing a specified service, a breach in security/ confidentiality, or non-compliance with legal and regulatory requirements, among others may lead to reputation / financial losses for the bank and may also result in systemic risks within the banking system in the country. Pervasive use of technology in banking operations further amplifies the risk impact.

#### *(i) Risk Evaluation and Measurement*

Risk evaluation should be performed prior to entering into an outsourcing agreement and reviewed periodically in the light of known and expected changes, as part of the strategic planning or review processes.

The framework for risk evaluation should include the following steps:

- Identification of the role of outsourcing in the overall business strategy and objectives, and inter-linkages with corporate strategic goals
- Comprehensive due diligence on the nature, scope and complexity of the outsourcing to identify the key risks and risk mitigation strategies For e.g. in case of technology outsourcing, state of security practices and controls environment offered by the service provider is a key factor
- Analysis of the impact of such arrangement on the overall risk profile of the bank, and whether adequate internal expertise and resources exist to mitigate the risks identified
- Analysis of risk-return on the potential benefits of outsourcing vis-à-vis the vulnerabilities that may arise

Banks should evaluate vendor managed processes or specific vendor relationships as they relate to information systems and technology. All outsourced information systems and operations may be subject to risk management and security and privacy policies that meet the Bank's own standards.

#### *(ii) Service provider selection*

Management should identify functions to be outsourced along with necessary controls and solicit responses from prospective bidders via an RFP process. Proposals submitted by service providers should be evaluated in the light of the organisation's needs, and any differences in the service provider proposals as compared to the solicitation should be analyzed carefully. Selection of affiliated parties as service providers should be done at arm's length in accordance with this guideline.

***Due Diligence***

In negotiating / renewing an Outsourcing arrangement, due diligence should be performed to assess the capability of the technology service provider to comply with obligations in the outsourcing agreement. Due diligence should involve an evaluation of all information about the service provider including qualitative, quantitative, financial, operational and reputational factors, as follows:

- Past experience and competence to implement and support proposed activities over the contractual period
- Financial soundness and ability to service commitments even under adverse conditions
- Business reputation and culture, compliance, complaints and outstanding or potential litigations
- Security and internal control, audit coverage reporting and monitoring environment, business continuity management
- External factors like political, economic, social and legal environment of jurisdiction in which the service provider operates and other events that may impact service performance
- Business continuity arrangements in case of technology outsourcing
- Due diligence for sub-service providers
- Risk management, framework, alignment to applicable international standards on quality / security / environment, etc., may be considered
- Secure infrastructure facilities
- Employee training, knowledge transfer
- Reliance on and ability to deal with sub-contractors

Extent of due diligence reviews may vary based on risk inherent in the outsourcing arrangements. Due diligence undertaken during the selection process should be documented and re-performed periodically as part of the monitoring and control processes of outsourcing.

***Maintaining Caution lists and scoring for service providers (bureau services)***

Where possible the Bank may obtain independent reviews and market feedback to supplement internal findings. IBA may facilitate requisite data sharing between banks to maintain scoring information for existing / new service providers. Banks should ensure that information used for due diligence is current and not more than 12 months old.

***Reporting to the regulator***

Banks must be required to report to the regulator, where the scale and nature of functions outsourced are significant, or extensive data sharing is involved across geographic locations as part of technology / process outsourcing and when data pertaining to Indian operations are stored/processed abroad.

***Multiple Service provider relationships***

A multiple service provider relationship is one where two or more service providers collaborate to deliver an end to end solution to the financial institution. Multiple contracting scenarios are possible:

- One service provider may be designated as the 'Lead Service Provider', to manage the other service providers
- Bank may independently enter into stand-alone contracts with each service provider

An institution selects from the above or any other contractual relationship, however, remains responsible for understanding and monitoring the control environment of all service providers that have access to the banks systems, records or resources.

***(iii) Contracting***

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.

Banks should ensure that the contract brings out nature of legal relationship between the parties (agent, principal or otherwise), and addresses risks and mitigation strategies identified at the risk evaluation and due diligence stages. Contracts should clearly define the roles and responsibilities of the parties to the contract and include suitable indemnification clauses. Any 'limitation of liability' consideration incorporated by the service provider should be assessed in consultation with the legal department.

Contracts should provide for periodic renewal and re-negotiation to enable the institution to retain an appropriate level of control over the outsourcing and should include the right to intervene with appropriate measure to meet the Banks' legal and regulatory obligations.

Contractual agreements should, in the very least, have provisions for the following:

- *Scope:*Agreements should state the activities that are to be outsourced
- *Performance Standards*:Key performance metrics should be defined for each activity to be outsourced, as part of the overall Service Level Agreement
- *Monitoring and Oversight:*Provide for continuous monitoring and assessment by the bank of the service provider so that any necessary corrective measure can be taken immediately
- *Access to books and records / Audit and Inspection:*This would include :

✓ Ensure that the bank has the ability to access all books, records and information relevant to the outsourced activity available with the service provider. For technology outsourcing, requisite audit trails and logs for administrative activities should be retained and accessible to the Bank based on approved requests

✓ Provide the bank with the right to conduct audits on the service provider whether by its internal or external auditors, or by external specialists 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

✓ 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. This includes information maintained in paper and electronic formats

✓ 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

✓ Where the controlling/Head offices of foreign banks operating in India outsource the activities related to the Indian operations, the Agreement should include clauses to allow

the RBI or persons authorized by it to access the bank's documents, records of transactions and other necessary information given or stored or processed by the service provider within a reasonable time as also clauses to recognize the right of RBI to cause an inspection to be made of a service provider and its books and accounts by one or more of its officers or employees or other persons

- *Include termination clause :*

  - ✓ Contracts should include a termination clause and minimum periods to execute a termination provision, as deemed necessary
  - ✓ Agreements should provide for maintaining confidentiality of customer's information even after the contract expires or is terminated by either party
  - ✓ Contract should include conditions for default termination / early exit option for contracts. This may include circumstances when the service provider undergoes a change in ownership, becomes insolvent or goes under liquidation, received judicial indictment (whether within India or any other location), or when there has been a breach of confidentiality, security, or demonstrable deterioration in quality of services rendered
  - ✓ In all cases of termination (early or otherwise), an appropriate handover process for data and process needs to be agreed with the service provider

- *Confidentiality and security :*

- ✓ Mandate controls to ensure customer data confidentiality and service providers' liability in case of breach of security and leakage of confidential customer related information. For e.g. use of transaction-enabled mobile banking channels necessitates encryption controls to ensure security of data in transmission
- ✓ 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

- *Business Continuity:*The contract should contain clauses for contingency plans and testing thereof, to maintain business continuity.

- *Sub-contracting:*Agreements may include covenants limiting further sub-contracting. Agreements should provide for due prior approval/consent by the bank of the use of subcontractors by the service provider for all or part of an outsourced activity. The bank should retain the ability of similar control and oversight over the sub service provider as the service provider.

- *Dispute resolution:* Agreements should specify the resolution process, the event of default, indemnities involved and the remedies and recourse of the respective parties to the agreement.

- *Applicable laws:* Agreements should include choice of law provisions, based on the regulations as applicable to the bank. An agreement should be tailored to provide for specific risks relating to cross border businesses and operations, data privacy and ownership aspects, among others.

### (iv) Monitoring and Control of outsourced activities

Banks should establish a structure for management and control of outsourcing, based on the nature, scope, complexity and inherent risk of the outsourced activity.

A structure for monitoring and control of outsourced activities should comprise of the following:

- A central record of all material outsourcing, including technology outsourcing and sub service provider relationships, that is readily accessible for review by the Board and senior management of the bank should be maintained. The records should be updated promptly and half yearly reviews should be placed before the Board.
- Banks should 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.
- Banks 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.
- Banks should pro-actively intimate RBI of any adverse developments or non – compliance with legal and regulatory requirements in an outsourcing arrangement.
- In the event of outsourcing of technology operations, the banks should subject the same to enhanced and rigorous change management and monitoring controls since ultimate responsibility and accountability rests with the bank. It may be desirable if banks control the management of user ids created for use of external vendor personnel. As a contingency measure, banks may also endeavor to develop, over a period of time, reasonable level of skills/knowledge in various technology related areas like system administration, database administration, network architecture and administration, etc., to effectively engage with the vendors and also to take over these functions in the event of any contingency.

***Service Level Agreements and performance metrics***

Management should include SLAs in the outsourcing contracts to agree and establish accountability for performance expectations. SLAs must clearly formalize the performance criteria to measure the quality and quantity of service levels. Banks should develop the following towards establishing an effective oversight program:

- Formal policy that defines the SLA program
- SLA monitoring process
- Recourse in case of non-performance
- Escalation process
- Dispute resolution process
- Conditions in which the contract may be terminated by either party

For outsourced technology operations, specific metrics may be defined around the service availability, business continuity and transaction security, in order to measure services rendered by the external vendor organization. Please refer to the paper on '*IT Operations Framework*' for details on the SLA and performance metrics for technology operations.

Performance expectations, under both normal and contingency circumstances, need to be defined. Provisions need to be in place for timely and orderly intervention and rectification in the event of substandard performance by the service provider.

***Control environment offered by the Service Provider***

Banks should evaluate the adequacy of internal controls environment offered by the service provider. Due consideration should be given to the implementation of following by the service provider:

- Information security policies and employee awareness of the same
- Controls for logical access to customer information by service provider staff, so that information may be accessed on a need-to-know basis only
- Physical and environmental security and controls
- Network security and controls
- Formal process for tracking and monitoring program changes and projects
- Process for incident reporting and problem management
- Special control considerations for service providers using cloud computing as part of service
- Control considerations for handling of customer information and personally identifiable information
- Data classification and controls for handling data

***Periodic Risk Assessment, Audit and Reviews***

Outsourcing should not impede or interfere with the ability of the Bank or the Regulator in performing its supervisory functions and objectives.

As a practice, institutions should conduct pre- and post- outsourcing implementation reviews. An institution should also review its outsourcing arrangements periodically to ensure that its outsourcing risk management policies and procedures, and these Guidelines, are effectively complied with.

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

Banks should also periodically commission independent audit and expert assessments on the security and control environment of the service provider. Such assessments and reports on the service provider may be performed and prepared by the institution's internal or external auditors, or by agents appointed by the institution.

Such reviews should take adequate cognizance of historical violations or issue remediation during previous audits and assessments. Copies of previous audits and assessments should be shared during RBI inspections.

***Business Continuity Planning***

Banks should ensure that their business continuity preparedness is not adversely compromised on account of outsourcing. Banks are expected to adopt sound business continuity management practices as issued by RBI and seek proactive assurance that the outsourced service provider maintains readiness and preparedness for business continuity on an ongoing basis.

Banks, while framing the viable contingency plan, need to consider the availability of alternative service providers or the possibility of bringing the outsourced activity back-in-house in an emergency(for example, where number of vendors for a particular service is extremely limited) and the costs, time and resources that would be involved and take suitable preparatory action.

### *(v) Confidentiality and Security*

Public confidence is a cornerstone in the stability and reputability of a bank. Banks should be proactive to identify and specify the minimum security baselines to be adhered to by the service providers to ensure confidentiality and security of data. This is particularly applicable where third party service providers have access to personally identifiable information and critical customer data.

An institution may take the following steps to ensure that risks with respect to confidentiality and security of data are adequately mitigated:

- Address, agree and document specific responsibilities of the respective parties in outsourcing to ensure adequacy and effectiveness of security practices, including identifying obligations and liability in the event of a breach or default
- Discuss and agree on the instances where customer data shall be accessed and the user groups who will have access to the same. Access to a Bank's data should be strictly on a need to know basis
- Ensure that service provider employees are adequately aware and informed on the security and privacy policies

### *(vi)Outsourcing to Foreign Service providers*

The engagement of service providers across multiple geographies exposes the organization to country risk – economic, social and political reasons in the country that may adversely affect the Banks business and operations. Banks should proactively evaluate such risk as part of the due diligence process and develop appropriate mitigating controls and as required, an effective exit strategy.

Outsourcing outside India should be agreed, in a manner that does not obstruct or hinder the ability of the bank or regulatory authorities to perform periodic audits/inspections and assessments, supervise or reconstruct activities of the bank based on books, records and necessary documentation, in a timely manner. Banks should ensure the following:

- Banks should principally enter into arrangements with parties operating in jurisdictions that generally uphold confidentiality clauses and agreements
- Banks may not outsource within jurisdictions where access to books, records and any other information required for audit and review purposes may be impeded due to regulatory or administrative constraints
- Banks should notify the Regulator where the rights of access for the Bank and / or the Regulator are likely to be impeded
- Emerging technologies such as data center hosting, applications as a service, cloud computing have given rise to unique legal jurisdictions for data and cross border regulations. Banks should clarify the jurisdiction for their data and applicable regulations at the outset of an outsourcing arrangement. This information should be reviewed periodically and in case of significant changes performed by the service provider

### *(vii) Outsourcing within a Group*

These guidelines are generally applicable to outsourcing within a group conglomerate, including parent or Head Office, branch or a group company, whether located within or outside India. These requirements may be addressed as part of group wide risk assessment and management procedures.

Due diligence on an intra-group service provider may take the form of evaluating qualitative aspects on the ability of the service provider to address risks specific to the institution, particularly those relating to business continuity management, monitoring and control, and audit and inspection, including confirmation on the right of access to be provided to RBI to retain effective supervision over the institution, and compliance with local regulatory

standards. The respective roles and responsibilities of each office in the outsourcing arrangement should be documented in writing in a formal Service Level Agreement.

***(viii) Handling customer grievances and complaints***

The Board and senior management are responsible for ensuring that quality and availability of banking services to customers are not adversely affected due to the outsourcing arrangements entered into by the Bank. Banks need to institute a robust grievance redressal mechanism, which should not be compromised in any way due to outsourcing.

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

Generally, a time limit of 30 days may be given to the customers for forwarding their complaints / grievances. The grievance redressal procedure of the bank and the time frame fixed for responding to the complaints should be placed on the bank's website. If a complainant does not get satisfactory response from the bank within 60 days from the date of his lodging the complaint, he will have the option to approach the Office of the concerned Banking Ombudsman for redressal of his grievance/s.

**INDUSTRY-WIDE RECOMMENDATIONS:**

1. IBA may facilitate requisite data sharing between banks to maintain scoring information for existing / new service providers and including any fraud or major operational lapses committed by the service providers.

2. Detailed service provider assessment and monitoring frameworks and best practices from a banking context can be explored by IBA in collaboration with institutions like DSCI and IDRBT.

**KEY RECOMMENDATIONS:**

1. The Board and senior management are responsible for outsourced operations and for managing risks inherent in such outsourcing relationships. Whereas an institution may delegate its permitted day-to-day operational duties to a service provider, responsibilities for effective due diligence, oversight and management of outsourcing and accountability for all outsourcing decisions continue to rest with the Bank, Board and senior management. Board and senior management have the responsibility to institute an effective governance mechanism and risk management process for all outsourced operations.

2. Banks need to assess the degree of ‘materiality’ inherent in the outsourced functions. Whether an outsourcing arrangement is ‘material’ to the business context or not is a qualitative judgment and may be determined on the basis of criticality of service, process, or technology to the overall business objectives. Outsourcing of non-financial processes, such as technology operations, is ‘material’ and if disrupted has the potential to significantly impact business operations, reputation and stability of the bank. Where a Bank relies on third party employees to perform key banking functions such as applications processing, etc., on a continuous basis, such outsourcing may also be construed as ‘material’, whether or not the personnel are located within the premises of the Bank.

3. Risk evaluation should be performed prior to entering into an outsourcing agreement and reviewed periodically in the light of known and expected changes, as part of the strategic planning or review processes. Banks should evaluate vendor managed processes or specific vendor relationships as they relate to information systems and technology. All outsourced information systems and operations may be subject to risk management and security and privacy policies that meet the Bank's own standards.

4. When considering negotiating / renewing an Outsourcing arrangement, due diligence should be performed to assess the capability of the technology service provider to comply with obligations in the outsourcing agreement. Due diligence should involve an evaluation of all information about the service provider including qualitative, quantitative, financial, operational and reputational factors.Where possible the Bank may obtain independent reviews and market feedback to supplement internal findings.

5. Banks must be required to report to the regulator, where the scale and nature of functions outsourced are significant, or extensive data sharing is involved across geographic locations as part of technology / process outsourcing.

6. In the event of multiple service provider relationships where two or more service providers collaborate to deliver an end to end solution for the financial institution, a bank, however, remains responsible for understanding and monitoring the control environment of all service providers that have access to the Banks systems, records or resources.

7. 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.

8. Banks should ensure that the contract brings out the nature of the legal relationship between the parties (agent, principal or otherwise), and addresses risks and mitigation strategies identified at the risk evaluation and due diligence stages. Contracts should clearly define the roles and responsibilities of the parties to the contract and include suitable indemnification clauses. Any 'limitation of liability' consideration incorporated by the service provider should be assessed in consultation with the legal department. Various critical aspects that need to be considered have been indicated in the chapter.

9. Banks should establish a structure for management and control of outsourcing, based on the nature, scope, complexity and inherent risk of the outsourced activity.

10. Management should include SLAs in the outsourcing contracts to agree and establish accountability for performance expectations. SLAs must clearly formalize the performance criteria to measure the quality and quantity of service levels.For outsourced technology operations, specific metrics may be defined around the service availability, business continuity and transaction security, in order to measure services rendered by the external vendor organization.

11. Banks should evaluate the adequacy of the internal controls environment offered by the service provider. Due consideration should be given to implementation by the service provider of various aspects like information security policies and employee awareness of the same, logical access controls, physical and environmental security and controls, controls for handling data, etc.

12. Outsourcing should not impede or interfere with the ability of the bank or the regulator in performing its supervisory functions and objectives.As a practice,

institutions should conduct pre- and post- outsourcing implementation reviews. An institution should also review its outsourcing arrangements periodically to ensure that its outsourcing risk management policies and procedures, and these Guidelines, are effectively complied with. An institution should, at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet outsourcing obligations.

13. Banks should also periodically commission independent audit and expert assessments on the security and control environment of the service provider. Such assessments and reports on the service provider may be performed and prepared by the institution's internal or external auditors, or by agents appointed by the institution.

14. Banks should ensure that their business continuity preparedness is not compromised on account of outsourcing. Banks are expected to adopt sound business continuity management practices as issued by RBI and seek proactive assurance that the outsourced service provider maintains readiness and preparedness for business continuity on an ongoing basis.

15. A bank needs to take effective steps to ensure that risks with respect to confidentiality and security of data are adequately mitigated.

16. Banks, while framing the viable contingency plan, need to consider the availability of alternative service providers or the possibility of bringing the outsourced activity back-in-house in an emergency(for example, where number of vendors for a particular service is extremely limited) and the costs, time and resources that would be involved and take suitable action, if warranted.

17. In the event of outsourcing of technology operations, the banks should subject the same to enhanced and rigorous change management and monitoring controls since ultimate responsibility and accountability rests with the bank. It may be desirable that banks control the management of user ids created for use of external vendor personnel. As a contingency measure, banks may also endeavor to develop, over a period of time, reasonable level of skills/knowledge in various technology related areas like system administration, database administration, network architecture and administration, etc., to effectively engage with the vendors or to take over these functions in the event of any contingency.

18. The engagement of service providers across multiple geographies exposes the organisation to country risk – economic, social and political reasons in the country that may adversely affect the Banks business and operations. Banks should proactively evaluate such risk as part of the due diligence process and develop appropriate mitigating controls and as required, an effective exit strategy.

19. Emerging technologies such as data center hosting, applications as a service and cloud computing have given rise to unique legal jurisdictions for data and cross border regulations. Banks should clarify the jurisdiction for their data and applicable regulations at the outset of an outsourcing arrangement. This information should be reviewed periodically and in case of significant changes performed by the service provider.

20. These guidelines are generally applicable to outsourcing within a group conglomerate, including parent or Head Office, branch or a group company, whether located within or outside India. The requirements may be addressed as part of group wide risk assessment and management procedures.

21. Banks should ensure that quality and availability of banking services to customers are not adversely affected due to the outsourcing arrangements entered into by the Bank. Banks need to institute a robust grievance redressal mechanism, which should not be compromised in any way due to outsourcing.

22. IBA may facilitate requisite data sharing between banks to maintain scoring information for existing / new service providers and including any fraud or major operational lapses committed by the service providers.

23. Detailed service provider assessment and monitoring frameworks and best practices from a banking context can be explored by IBA in collaboration with institutions like DSCI and IDRBT.